Security Credential Management System Proof–of–Concept Implementation

EE Requirements and Specifications Supporting SCMS Software Release 1.1

Submitted to the United States Department of Transportation
National Highway Traffic Safety Administration (NHTSA)

May 04, 2016

In Response to Cooperative Agreement Number
DTNH22-14-H-00449/0003

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.

Table of Contents

1 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 (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. These consist of an initial release followed by three maintenance releases that will take place later in the project. This document presents the requirements and specifications for the SCMS POC system that are needed to support the first of the four software releases from the perspective of an end entity (EE). This document is an output of the efforts in Task 4 and was produced to fulfill Task 4, Milestone 2 titled “Completion of POC System Requirements and Specifications (including ASN.1).” This document is a work-in-progress. Future refinements and revisions to the requirements and specifications are anticipated as work in the project continues, new information becomes available, and the lessons learned from system testing can be incorporated into the SCMS design. This document is being provided to mark the progress in Task 4 to date and, potentially, to facilitate the information exchange with other related U.S. Department of Transportation (USDOT) programs and stakeholders.

2 Requirements and Specifications

This page and its subpages contains requirements and specifications of the SCMS PoC protocols and components.

2.1 Common Requirements

2.1.1 SCMS PoC supported V2X Applications

Application	Application category	PSID	SSP notes	Comments	SSP recommendations for PoC
Basic Safety Message	BSM inputs	BSM PSID: 0p20 (= 0x20)		Support multiple V2V safety applications	
Modified Eco-Speed Harmonization /RSE	2 - Speed Harmonization	traveller information and roadside signage PSID: 0p80-03 (0x83)	SSP arrangement may govern region where speed advice applies; may also differentiate between different speed harmonization categories (e.g., eco-, light vehicles, freight, transit, etc.)	PSID owner/manager must specify SSP design within a specific PSID	SSP: 90-FF-FF-01
Modified Eco-Speed Harmonization /TMC	2 - Speed Harmonization	traveller information and roadside signage PSID: 0p80-03 (0x83)	SSP arrangement may govern region where speed advice applies; may also differentiate between different speed harmonization categories (e.g., eco-, light vehicles, freight, transit, etc.)	PSID owner/manager must specify SSP design within a specific PSID	SSP: 90-FF-FF-01

Application	Application category	PSID	SSP notes	Comments	SSP recommendations for PoC
Red Light Violation Warning/RSE	3 - Signal Violation Warning	Intersection Safety and Awareness PSID: 0p80-02 (= 0x82) (SPaT & MAP use message ID to distinguish message type)			SSP: 90-01
Pedestrian in Signalized Crosswalk Warning/RSE	16 - Pedestrian Warnings	Intersection Safety and Awareness PSID: 0p80-02 (= 0x82) (SPaT & MAP use message ID to distinguish message type)	May require a distinct SSP in order to differentiate this application information from SPaT and MAP	PSID owner/manager must specify SSP design within a specific PSID	SSP: 90-01
Vehicle Turning Right in Front of Bus Warning	BSM inputs	BSM PSID: 0p20 (= 0x20)		Assumes specific application in bus to analyze the received BSMs and determine if a warning should be provided to the bus driver	SSP: all
Mobile Accessible Pedestrian Signal System (PED-SIG)	16 - Pedestrian Warnings	Intersection Safety and Awareness PSID: 0p80-02 (= 0x82) (SPaT & MAP use message ID to distinguish message type)	May require a distinct SSP in order to differentiate this application information from SPaT and MAP	PSID owner/manager must specify SSP design within a specific PSID	SSP: 90-01

Application	Application category	PSID	SSP notes	Comments	SSP recommendations for PoC
Curve Speed Warning	8 - Curve Speed Warning	traveller information and roadside signage PSID: 0p80-03 (0x83)	Use of single PSID to provide different messages depends upon either distinct containers within the TIM messages or distinct SSPs for the different messages within the TIM PSID	PSID owner/manager must specify SSP design within a specific PSID	SSP: 90-FF-FF-02
Freight-Specific Dynamic Travel Planning and Performance	17 – Applications Layer Security	IPv6 Routing PSID: 0pEF-FF-FF-FE (= 0x10-20-40-7E)		This assumes that the application uses generic internet access and can connect based upon WSA from RSE. This may change if the detailed application design varies from the current understanding	SSP: all
Reduced Speed/Work Zone Warning/RSE	9 - Temporary Situation Warning	traveller information and roadside signage PSID: 0p80-03 (0x83)	SSP arrangement may govern region where speed advice applies; Use	PSID owner/manager must specify SSP design within	SSP: 90-FF-FF-03

Application	Application category	PSID	SSP notes	Comments	SSP recommendations for PoC
			of single PSID to provide different messages depends upon either distinct containers within the TIM messages or distinct SSPs for the different messages within the TIM PSID	a specific PSID	
Reduced Speed/Work Zone Warning/TMC	9 - Temporary Situation Warning	traveller information and roadside signage PSID: 0p80-03 (0x83)	SSP arrangement may govern region where speed advice applies; Use of single PSID to provide different messages depends upon either distinct containers within the TIM messages or distinct SSPs for the different messages within the TIM PSID	PSID owner/manager must specify SSP design within a specific PSID	SSP: 90-FF-FF-03

Application	Application category	PSID	SSP notes	Comments	SSP recommendations for PoC
Intelligent Traffic Signal System (I-SIG) In-Vehicle Information Potential	Current assumption is BSM inputs only	BSM PSID: 0p20 (= 0x20)	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: all
Forward Collision Warning (FCW)	BSM inputs	BSM PSID: 0p20 (= 0x20)			SSP: all
Emergency Electronic Brake Light (EEBL)	BSM inputs	BSM PSID: 0p20 (= 0x20)			SSP: all
Blind Spot Warning (BSW)	BSM inputs	BSM PSID: 0p20 (= 0x20)			SSP: all
Lane Change Warning/Assist (LCA)	BSM inputs	BSM PSID: 0p20 (= 0x20)			SSP: all
Intersection Movement Assist	BSM inputs	BSM PSID: 0p20 (= 0x20)			SSP: all
Stationary Vehicle Ahead (SVA)	BSM inputs	BSM PSID: 0p20 (= 0x20)			SSP: all
Do Not Pass Warning	BSM inputs	BSM PSID: 0p20 (= 0x20)			SSP: all
Probe Enabled Traffic Monitoring	BSM inputs	BSM PSID: 0p20 (= 0x20)	Detailed application description not available, so both possible approaches to	If the former, then RSE just collects BSMs; if the later; RSE sends WSA with probe	SSP: all
	9 - Temporary Situation Warning	IPv6 Routing PSID: 0pEF-FF-FF-FE (= 0x10-20-40-7E)			SSP: all

Application	Application category	PSID	SSP notes	Comments	SSP recommendations for PoC
			be supported for PoC	request and then vehicle uses IP service to send requested information or establish two-way communications	
Transit Signal Priority/ special vehicles	1 - Signal Pre-emption/Priority	Intersection Safety and Awareness PSID: 0p80-02 (= 0x82) (SPaT & MAP use message ID to distinguish message type)	different SSPs for different levels of pre-emption / priority and related permissions (e.g., different SSPs for police, fire, transit, ambulance, freight pre-emption permissions) / difficult to know the SSP design until the applications design is more complete	PSID owner/manager must specify SSP design within a specific PSID	SSP: 90-FF-FF-01 Transit; 90-FF-FF-02 Police; 90-FF-FF-03 Fire; 90-FF-FF-04 Ambulance; etc.
Spot Specific Weather Warnings/RSE	9 - Temporary Situation Warning	traveller information and roadside signage PSID: 0p80-03 (0x83)	SSP arrangement may govern region where weather warning applies; Use of single	PSID owner/manager must specify SSP design within a specific PSID	SSP: 90-FF-FF-04

Application	Application category	PSID	SSP notes	Comments	SSP recommendations for PoC
			PSID to provide different messages depends upon either distinct containers within the TIM messages or distinct SSPs for the different messages		
Spot Specific Weather Warnings/TMC	9 - Temporary Situation Warning	traveller information and roadside signage PSID: 0p80-03 (0x83)	SSP arrangement may govern region where weather warning applies: Use of single PSID to provide different messages depends upon either distinct containers within the TIM messages or distinct SSPs for the different messages	PSID owner/manager must specify SSP design within a specific PSID	SSP: 90-FF-FF-04
Variable speed limits/RSE	10 - Speed Zone	traveller information and roadside signage PSID: 0p80-03 (0x83)	SSP arrangement may govern region where speed advice applies; Use	PSID owner/manager must specify SSP design within	SSP: 90-FF-FF-05

Application	Application category	PSID	SSP notes	Comments	SSP recommendations for PoC
			of single PSID to provide different messages depends upon either distinct containers within the TIM messages or distinct SSPs for the different messages	a specific PSID	
Variable speed limits/TMC	10 - Speed Zone	traveller information and roadside signage PSID: 0p80-03 (0x83)	SSP arrangement may govern region where speed advice applies; Use of single PSID to provide different messages depends upon either distinct containers within the TIM messages or distinct SSPs for the different messages	PSID owner/manager must specify SSP design within a specific PSID	SSP: 90-FF-FF-05
Speed Harmonization /RSE	2 - Speed Harmonization	traveller information and roadside signage PSID: 0p80-03 (0x83)	SSP arrangement may govern region where speed harmonization	PSID owner/manager must specify SSP design within	SSP: 90-FF-FF-06

Application	Application category	PSID	SSP notes	Comments	SSP recommendations for PoC
			advice applies: Use of single PSID to provide different messages depends upon either distinct containers within the TIM messages or distinct SSPs for the different messages	a specific PSID	
Speed Harmonization /TMC	2 - Speed Harmonization	traveller information and roadside signage PSID: 0p80-03 (0x83)	SSP arrangement may govern region where speed harmonization advice applies: Use of single PSID to provide different messages depends upon either distinct containers within the TIM messages or distinct SSPs for the different messages	PSID owner/manager must specify SSP design within a specific PSID	SSP: 90-FF-FF-06

Application	Application category	PSID	SSP notes	Comments	SSP recommendations for PoC
Work Zone Alerts/RSE	9 - Temporary Situation Warning	traveller information and roadside signage PSID: 0p80-03 (0x83)	SSP arrangement may govern region where work zone alert applies; Use of single PSID to provide different messages depends upon either distinct containers within the TIM messages or distinct SSPs for the different messages	PSID owner/manager must specify SSP design within a specific PSID	SSP: 90-FF-FF-03
Work Zone Alerts/TMC	9 - Temporary Situation Warning	traveller information and roadside signage PSID: 0p80-03 (0x83)	SSP arrangement may govern region where work zone alert applies; Use of single PSID to provide different messages depends upon either distinct containers within the TIM messages or distinct SSPs for the different messages	PSID owner/manager must specify SSP design within a specific PSID	SSP: 90-FF-FF-03

Application	Application category	PSID	SSP notes	Comments	SSP recommendations for PoC
Truck Restrictions/RSE	11 - Special Vehicle Warning	traveller information and roadside signage PSID: 0p80-03 (0x83)	SSP arrangement may govern region where truck restriction information applies; Use of single PSID to provide different messages depends upon either distinct containers within the TIM messages or distinct SSPs for the different messages	PSID owner/manager must specify SSP design within a specific PSID	SSP: 90-FF-FF-07
Truck Restrictions/TMC	11 - Special Vehicle Warning	traveller information and roadside signage PSID: 0p80-03 (0x83)	SSP arrangement may govern region where truck restriction information applies; Use of single PSID to provide different messages depends upon either distinct containers within the TIM messages or	PSID owner/manager must specify SSP design within a specific PSID	SSP: 90-FF-FF-07

Application	Application category	PSID	SSP notes	Comments	SSP recommendations for PoC
			distinct SSPs for the different messages		
Truck Parking	17 – Applications Layer Security	IPv6 Routing PSID: 0pEF-FF-FF-FE (= 0x10-20-40-7E)		RSE sends WSA with IP service availability indicated and then vehicle uses IP service to establish two-way communications with application	SSP: all
Route Guidance	17 – Applications Layer Security	IPv6 Routing PSID: 0pEF-FF-FF-FE (= 0x10-20-40-7E)		RSE sends WSA with IP service availability indicated and then vehicle uses IP service to establish two-way communications with application	SSP: all
Automatic Alerts for First Responders	11 - Special Vehicle Warning	traveller information and roadside signage PSID: 0p80-03 (0x83)	Specific SSPs may need to be designated for messages to special vehicles	Detailed application description not available, so both possible approaches to be supported for PoC	SSP: 90-FF-FF-08
	17 – Applications Layer Security	IPv6 Routing PSID: 0pEF-FF-FF-FE (= 0x10-20-40-7E)			SSP: all

Application	Application category	PSID	SSP notes	Comments	SSP recommendations for PoC
CV-enabled Weather-Responsive Variable Speed Limits	9 - Temporary Situation Warning	traveller information and roadside signage PSID: 0p80-03 (0x83)		Detailed application description not available, so both possible approaches to be supported for PoC	SSP: 90-FF-FF-05
	17 – Applications Layer Security	IPv6 Routing PSID: 0pEF-FF-FF-FE (= 0x10-20-40-7E)			SSP: all
Road Weather Advisories for Trucks and Vehicles	9 - Temporary Situation Warning	traveller information and roadside signage PSID: 0p80-03 (0x83)	different SSPs may be needed to differentiate messages for different categories of vehicles	PSID owner/manager must specify SSP design within a specific PSID	SSP: 90-FF-FF-04
Situational Awareness	17 – Applications Layer Security	IPv6 Routing PSID: 0pEF-FF-FF-FE (= 0x10-20-40-7E)		RSE sends WSA with situational awareness probe request and then vehicle uses IP service to send requested information or establish two-way communications	SSP: all
Advanced Traveler Information System	17 – Applications Layer Security	IPv6 Routing PSID: 0pEF-FF-FF-FE (= 0x10-20-40-7E)		RSE sends WSA with IP service availability indicated and then vehicle uses IP service to	SSP: all

Application	Application category	PSID	SSP notes	Comments	SSP recommendations for PoC
				establish two-way communications with application	
Emergency Communications and Evacuation (EVAC)	9 - Temporary Situation Warning	traveller information and roadside signage PSID: 0p80-03 (0x83)		Application description is unclear, so both possible approaches to be supported for PoC	SSP: 90-FF-FF-09
	17 – Applications Layer Security	IPv6 Routing PSID: 0pEF-FF-FF-FE (= 0x10-20-40-7E)			SSP: all
Differential GPS Corrections, Uncompressed	Support	PSID: 0p80-00 (= 0x80)			SSP: all
Differential GPS Corrections, Compressed	Support	PSID: 0p80-01 (= 0x81)			SSP: all
Certificate Revocation List Application	Support	PSID: 0p80-80 (= 0x01-00)			SSP: all
WAVE Service Advertisement	Support	PSID: 0p80-07 (= 0x87)			SSP: all
Misbehavior Reporting for Common Applications	Support	PSID: 0p26 (= 0x26)			SSP: all
Peer-to-Peer Distribution of Security Management Information	Support	PSID: 0p80-08 (= 0x88)			SSP: all

2.1.2 Certificate Types

The V2X system uses several types of certificates. SCMS components generate these (and in many cases can also be revoked). All certificate lifetimes and renewal periods are listed separately for PoC and CV Pilot. 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. They are defined in cert-profile.asn.

2.1.2.1 OBE

2.1.2.1.1 OBE Enrollment

Enrollment certificate is like a passport for the OBE that it uses to request other certificates: pseudonym and identification certificates. It does not have an encryption key. It is provided to 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 to be made by the SCMS Manager. Enrollment certificates have extremely **long validity** periods expected to cover OBE's full operational lifetime. Revocation of enrollment certificate is done through **internal blacklist** at RA.

2.1.2.1.2 Pseudonym

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

Main features of this certificate and its 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.

2.1.2.1.3 Identification

Identification certificates are used by an OBE primarily for authorization in V2I applications. None of the current V2I applications require encryption by OBE at the application level, however, there might be a need in the future. OBE identification certificates use an optional 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 1** identification certificate valid at a time for a given application. While pseudonymity and tracking is no concern, identity certificates still protect 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 RA. Revocation of identification certificates is done through **CRLs**. There is a one-to-one mapping of (PSID, SSP) combination from enrollment certificates to identification certificates.

2.1.2.2 RSE

2.1.2.2.1 RSE Enrollment

Enrollment certificate is like a passport for the RSE that it uses to request application certificates. It does not have an encryption key. It is provided to 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 extremely **long validity** periods expected to cover RSE's full operational lifetime. Certification process needs to include geographic limits, application classes, etc. Revocation of enrollment certificate is done through **internal blacklist** at RA.

2.1.2.2.2 Application

Application certificates are used by an RSE for authentication and encryption, and therefore unlike all other OBE and RSE certificates, they might have **encryption keys**. As there are no privacy constraints for RSEs, an RSE has **only 1** application certificate valid at a time for a given application. Moreover for continuity reasons, an RSE may be given up to 1 extra application certificate that is valid for the next time period (i.e., say the validity period is 1 day, then an RSE will have only 1 certificate valid for today and up to 1 certificate valid for tomorrow). Revocation of application certificates are dependent on their validity periods: (1) **Short validity periods** (e.g., daily, hourly, etc.) require frequent certificate renewal, and hence **no CRL** except under exceptional circumstances. (2) **Long validity periods** (e.g., monthly, annually, etc.) 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.

2.1.2.3 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, and just like the RSE application certificates, an SCMS component has **only 1** certificate valid at a time. Moreover, for continuity reasons, an SCMS component (except root CA) may be given up to 1 extra application certificate that is valid for the next time period. Revocation of these certificates is done through **CRLs** issued by CRL Generator.

2.1.2.3.1 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 crypto algorithms different from 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, is there only for namesake, as the signature is by the elector itself, and therefore the trust in an elector certificate is established through out-of-band means. Elector certificate does not have an encryption key, as the Electors are mostly offline and do not accept any incoming messages, whether encrypted or not. Elector certificates needs to be made available to everyone in the system. As elector certificates are self-signed, their integrity must be ensured by other means (other than the cryptography used in generating the certificate itself), such as tamper-proof hardware. For the same reason, provisioning and/or update of elector certificates are done through out-of-band means. They can be revoked, and new elector certificates can be added by using the elector model, as explained in Root Management and Revocation Recovery.

2.1.2.3.2 Root CA

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, is there only for namesake, 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 very long lifetime, as changing a root CA certificate is extremely difficult, time consuming, and financially expensive. (4) Only a quorum of Electors can issue root management messages and add them to a CRL to revoke a root CA certificate.

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 root CA certificate must be ensured by other means (other than the cryptography used in generating the certificate itself), such as tamper-proof hardware. For the same reason, provisioning and/or update of root CA certificate is done through out-of-band means. Root CA certificates can be revoked, and new root CA certificates can be added by using the elector model, as explained in Root Management and Revocation Recovery.

2.1.2.3.3 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 ICA certificate.

2.1.2.3.4 ECA

As mentioned above, ECA certificates are of **implicit** 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 do not have encryption keys. To receive encrypted

messages, owner of these certificates can include an ephemeral response encryption key in the request messages. Just like enrollment certificates, ECA certificates have an extremely **long validity** period so that their owner can issue enrollment certificates that have an extremely long validity period. Revocation of ECA certificate is done through **CRLs** issued by CRL Generator.

2.1.2.3.5 PCA

PCA certificates can be used to only issue certificates to end-entities including OBEs and RSEs. These certificates do not have encryption keys. To receive encrypted messages, owner of these certificates can include an ephemeral response encryption key in the request messages. PCA certificates need to have validity periods that are at least as long as the longest validity certificates issued using them. Revocation of PCA certificate is done through **CRLs** issued by CRL Generator.

2.1.2.3.6 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 only by either root CA or ICA), validity period of CRL generator certificates is kept as low as possible. For a given CRACA and CRL series, there is **only 1** valid CRL Generator certificate at any time, except for a short overlap time as defined in PoC Certificate Expiration Timelines respectively CV Pilot Certificate Expiration Timelines.

2.1.2.3.7 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.

2.1.2.3.8 Other

These include LA, MA, and RA certificates. These certificates can**not** be used to issue certificates. These certificates do not have encryption keys. To receive encrypted messages, owner of these certificates can include an ephemeral response encryption key in the request messages. Validity periods are as follows:

2.1.2.3.8.1 LA

Can be small as LAs do not interact with end-entities.

2.1.2.3.8.2 RA

Must be long enough so that end-entities can successfully make a certificate provisioning request after being bootstrapped.

2.1.2.3.8.3 MA

Needs to be long so that end-entities do not need to retrieve these certificates very often.

2.1.2.4 EE certificate type features

The following table provides an overview of the EE certificate types. 'x' describe mandatory features, and '(x)' describe optional features. The table provides a comprehensive overview. We have made the following assumptions for the POC:

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

	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 public-key to RA.	1 per time period, issue longer time periods. RSE generates public/private key pair and provides public-key to RA.
Revocation	RA blacklist	leverage linkage values	add certificate digests of all issued certificates (can be more than one)	RA blacklist	do not renew certificates	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

	OBE Enrollment Certificate	OBE Pseudonym Certificate	OBE Identification Certificate	RSE Enrollment Certificate	RSE Application Certificate	
					RSE with connectivity	RSE without connectivity
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
Non-Traceability		X				
Encryption key			(X) (determined using Butterfly Key mechanism)		X	

2.1.2.5 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1307	Review	Enrollment certificate lifetime	ECA shall issue Enrollment Certificates with a lifetime of 30 years.	For PoC, enrollment certificates use a life span of 30 years to avoid any need to update enrollment certificates.	This is for PoC only	ECA

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1308	SCMS PoC out of Scope	OBE sign misbehavior reports	OBE shall sign a misbehavior report with a currently valid (at time of event observation) pseudonym certificate.	To avoid forged misbehavior reports	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)
SCMS-1310	Review	Mapping PSID/SSP to pseudonym/identification certificates	There shall be a one-to-one mapping of (PSID, SSP) combination from enrollment certificates to pseudonym/ OBE identification certificates.	Otherwise, management is troublesome, in particular revocation.	The PSID/SSP combination of the enrollment certificate is forwarded to all issued pseudonym certificates.	PCA, RA
SCMS-1311	Review	Issue only one OBE identification certificate valid at a time	RA/PCA shall only issue one OBE identification certificate to an OBE valid at a time for a given application.	There is no need for privacy (by definition).		PCA, RA
SCMS-1312	Review	Issue RSE application certificates with optional encryption key	PCA shall issue RSE application certificates with optional	The encryption key is optional.	RSE application certificates always have a signature key and optionally an encryption key.	PCA

Key	Status	Summary	Description	justification	notes	Component/s
			encryption key.			
SCMS-1313	Review	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)	All SCMS component certificates shall be implicit, except for the following, which are explicit: PCA, ICA, Root CA, and elector certificate.	PCA, ICA, Root CA, and elector certificates need to be of explicit type in order to support P2P distribution. All other SCMS component certificates could be either implicit or explicit, and are selected as implicit for performance reasons.		CRL Store, CRLG, DCM, IBLM, ICA, LA, PCA, PG, RA, RCA
SCMS-1315	Review	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		CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, PCA, PG, RA

Key	Status	Summary	Description	justification	notes	Component/s
				complexity low and have maximum control over components, hence allowing exactly one certificate at a given time.		
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-1317	Review	Root CA encryption key	Root CA certificate shall not have an encryption key.	The root CA is not an active component but only used to issue sub-CA certificates.		RCA
SCMS-1318	Review	Root CA certificate validity	The Root CA certificate validity period shall be set to 70 years.	Root CA certificates must have an expiration date. The Root CA certificate must be valid at least as long as the longest issued	Certificate types and expiration periods are defined in the Certificate Types common requirements section (https://wiki.campllc.org/display/SP/Certificate+Types).	RCA

Key	Status	Summary	Description	justification	notes	Component/s
				enrollment certificate.	This is for PoC & CV-Pilot only.	
SCMS-1319	Review	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-1808	Review	Elector encryption key	Elector certificate shall not have an encryption key.	Electors are not active components but only used for management of Root CA certificates.		Elector
SCMS-1809	Review	Elector certificate validity	Elector certificates validity period shall be set to 60 years.	Elector certificates must have an expiration date.	Certificate types and expiration periods are defined in the Certificate Types common requirements section (https://wiki.campllc.org/display/SP/Certificate+Types). The initial 3 elector certificates have an expiration and "in use" time of 20, 40 and 60 years, respectively. Currently, there is only 1 set of Electors for both V2V and V2I. This is for PoC & CV-Pilot only.	Elector

2.1.2.6 CV Pilot Certificate Expiration Timelines

2.1.2.6.1 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 7 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
- 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 sufficiently short to require at least one rollover (renewal) event during the estimated project duration
- PKI hierarchy
  - The V2V-ICA, V2I-ICA, Policy Generator, CRL Generator and MA certificates shall be issued directly by the Root CA.
  - The subtree below V2I-ICA currently has one set of components: V2I-ECA, V2I-PCA, V2I-RA, and V2I-LA. Later on, there might also be a V2I-DCM.
  - The subtree below V2V-ICA is identical to that of the POC, i.e. it has one instance of all components: V2V-ECA, V2V-PCA, DCM, V2V-RA, and V2V-LA.

2.1.2.6.2 Table

	Issuer	Expiration	In Use	Request for Renewal	Start of validity for renewal	Number of concurrently valid certificates	Notes
OBE Enrollment	ECA	Variable, 7 years maximum	Same as expiration	N/A	N/A	1	All OBE Enrollment certificates shall be issued with an expiration at year 7 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)	
OBE Identification	PCA	1 month + 1 hour	1 month	Anytime	1 month	1 + 1 (for just 1 hour)	
RSE Enrollment	ECA	Variable, 7 years maximum	Same as expiration	N/A	N/A	1	All RSE Enrollment certificates shall be issued with an expiration at year 7 regardless of

	Issuer	Expiration	In Use	Request for Renewal	Start of validity for renewal	Number of concurrently valid certificates	Notes
							the date they are issued.
RSE Application	PCA	1 week + 1 hour	1 week	Anytime	1 week	1 + 1 (for just 1 hour)	
DCM	ICA	3 years + 1 week		3 months before end of In-use	3 years	1 + 1 (for just 1 week)	The last renewal/rollover certificate shall have a reduced In-use life. There are 2 DCMs for CV-Pilots: V2V-DCM, V2I-DCM.
ECA	ICA	7 years	3.5 years	3 months before end of In-use	3.5 years	1 + 1	The last renewal/rollover certificate shall have a reduced In-use life (1 month + 1 hour before estimated project duration). There are 2 ECAs for CV-Pilots: V2V-ECA, V2I-ECA.
RA	ICA	3 years + 1 week	3 years	3 months before end of In-use	3 years	1 + 1 (for just 1 week)	The last renewal/rollover certificate shall have a reduced In-use life. There are 2 RAs for CV-Pilots: V2V-RA, V2I-RA.
LA	ICA	3 years + 1 week	3 years	3 months before	3 years	1 + 1 (for just 1 week)	The last renewal/rollover certificate shall

	Issuer	Expiration	In Use	Request for Renewal	Start of validity for renewal	Number of concurrently valid certificates	Notes
				end of In-use			have a reduced In-use life. There are 2 pairs of LAs for CV-Pilots: V2V-LA, V2I-LA.
PCA	ICA	4 years	1 year	3 months before end of In-use	1 year	1 + 3	There are 2 PCAs for CV-Pilots: V2V-PCA, V2I-PCA.
ICA	Root CA	11 years	7 years	3 months before end of In-use	10 years	1	There are 2 ICAs for CV-Pilots: V2V-ICA, V2I-ICA.
MA	Root CA	3 years + 1 week	3 years	3 months before end of In-use	3 years	1 + 1 (for just 1 week)	The last renewal/rollover certificate shall have a reduced In-use life.
CRLG	Root CA	3 years + 1 week	3 years	3 months before end of In-use	3 years	1 + 1 (for just 1 week)	The last renewal/rollover certificate shall have a reduced In-use life. Currently, there is only 1 CRLG for both V2V and V2I.
Policy Generator	Root CA	3 years + 1 week	3 years	3 months before end of In-use	3 years	1 + 1 (for just 1 week)	The last renewal/rollover certificate shall have a reduced In-use life.
Root CA	Self	70 years	20 years	3 months before	20 years	1	Currently, there is only 1 Root CA for both V2V and V2I.

	Issuer	Expiration	In Use	Request for Renewal	Start of validity for renewal	Number of concurrently valid certificates	Notes
				end of In-use			
Elector	Self	60 years	60 years	3 months before end of In-use	60 years	3 (1 per elector)	The initial 3 elector certificates have an expiration and "in use" time of 20, 40 and 60 years, respectively. Currently, there is only 1 set of Electors for both V2V and V2I.

2.1.2.6.3 Requirements

2.1.2.6.3.1 Renewal/Rollover

Key	Summary	Component/s	Description	justification	notes
SCMS-1422	Renewal of component certificate	CRL Store, CRLG, DCM, ECA, ICA, LA, MA, PCA, PG, RA, RCA	A SCMS component shall request rollover 1609 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 1609 certificates prior 3 months to the end of the In-use life	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.

Key	Summary	Component/s	Description	justification	notes
			of the current certificate.		

2.1.2.6.3.2 Expiration, In-use, and Overlap

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, RCA
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-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-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, LA, MA, PG, RA
SCMS-1605	ECA certificate validity	ECA shall request an ECA certificate with a validity of 7 years.	To support issuing of subordinate certificates.	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 a maximum lifetime of 7 years. All EE Enrollment certificates shall be issued with an expiration at year 7 regardless of the date they are issued.	For CV-Pilot, enrollment certificates use a maximum life span of 7 years to avoid any need to update enrollment certificates.	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 3.5 years.	Use 3.5 years for Enrollment SCMS components	Out of scope as this needs to be implemented as operational policy. This is for CV-Pilot only.	ECA
SCMS-1809	Elector certificate validity	Elector certificates validity period shall be set to 60 years.	Elector certificates must have an expiration date.	Certificate types and expiration periods are defined in the Certificate Types common requirements section (https://wiki.camplc.org/display/SP/Certificate+Types) . The initial 3 elector certificates have an expiration and "in use" time of 20, 40 and 60 years, respectively. Currently, there is only 1 set of Electors for both V2V and V2I. This is for PoC & CV-Pilot only.	Elector

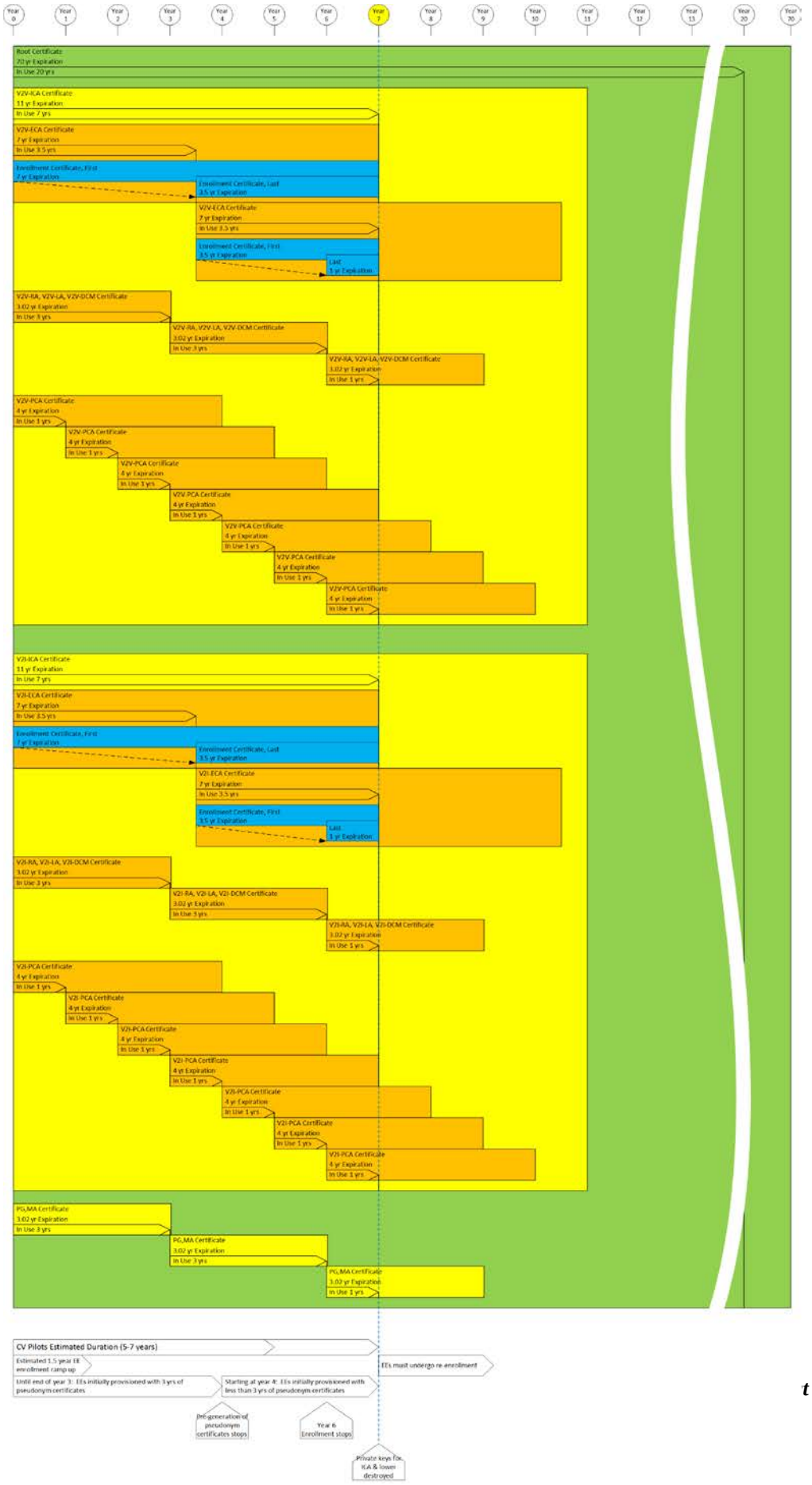
Key	Summary	Description	justification	notes	Component/s
SCMS-1423	Elector Certificate Expiration	The Technical Component of the SCMS Manager (TCotSCMSM) shall issue Elector certificates with an expiration of 60 years.	Component 1609 certificates shall have a defined expiration.	• In the case of the certificate 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 20 years, another one a certificate expiration of 40 years, to prevent multiple elector certificates from expiring at the same time. • These durations are for the SCMS PoC & CV-Pilot only. For other SCMS instances, this duration should be reevaluated.	• Elector

Key	Summary	Description	justification	notes	Component/s
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-1604	ICA certificate in-use period	ICA shall use its ICA certificate for an in-use period of 7 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 CV-Pilot only.	ICA
SCMS-1603	ICA certificate validity	ICA shall request an ICA certificate with a validity of 11 years.	To support issuing of subordinate certificates.	This is for CV-Pilot only.	ICA
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 & 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
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

Key	Summary	Description	justification	notes	Component/s
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
SCMS-526	Certificate Overlap:	RA shall request PCA to generate	The original value for $t_{overlap}$	This is for POC & CV-Pilot only.	RA

Key	Summary	Description	justification	notes	Component/s
	OBE Pseudonym Certificates	OBE pseudonym certificates with an overlap $t_{overlap}$ of one hour.	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.		
SCMS-1332	Root CA certificate overlap	Root CA certificates shall have an overlap of 50 years (an in-use period of 20 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 70 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 (https://wiki.camplc.org/display/SP/Certificate+Types). This is for PoC & CV-Pilot only.	RCA

2.1.2.6.4 Diagrams


Year 0
Year 1
Year 2
Year 3
Year 4
Year 5
Year 6
Year 7
Year 8
Year 9
Year 10
Year 11
Year 12
Year 13
Year 20
Root Certificate
20 yr Expiration
In Use 20 yrs
V2V-ICA Certificate
11 yr Expiration
In Use 7 yrs
V2V-ECA Certificate
7 yr Expiration
In Use 3.5 yrs
Enrollment Certificate, First
7 yr Expiration
Enrollment Certificate, Last
3.5 yr Expiration
V2V-ECA Certificate
7 yr Expiration
In Use 3.5 yrs
Enrollment Certificate, First
3.5 yr Expiration
Last
3 yr Expiration
V2V-RA, V2V-LA, V2V-DCM Certificate
3.02 yr Expiration
In Use 3 yrs
V2V-RA, V2V-LA, V2V-DCM Certificate
3.02 yr Expiration
In Use 3 yrs
V2V-RA, V2V-LA, V2V-DCM Certificate
3.02 yr Expiration
In Use 1 yrs
V2V-PCA Certificate
4 yr Expiration
In Use 1 yrs
V2V-PCA Certificate
4 yr Expiration
In Use 1 yrs
V2V-PCA Certificate
4 yr Expiration
In Use 1 yrs
V2V-PCA Certificate
4 yr Expiration
In Use 1 yrs
V2V-PCA Certificate
4 yr Expiration
In Use 1 yrs
V2V-PCA Certificate
4 yr Expiration
In Use 1 yrs
V2V-PCA Certificate
4 yr Expiration
In Use 1 yrs
V2I-ICA Certificate
11 yr Expiration
In Use 7 yrs
V2I-ECA Certificate
7 yr Expiration
In Use 3.5 yrs
Enrollment Certificate, First
7 yr Expiration
Enrollment Certificate, Last
3.5 yr Expiration
V2I-ECA Certificate
7 yr Expiration
In Use 3.5 yrs
Enrollment Certificate, First
3.5 yr Expiration
Last
3 yr Expiration
V2I-RA, V2I-LA, V2I-DCM Certificate
3.02 yr Expiration
In Use 3 yrs
V2I-RA, V2I-LA, V2I-DCM Certificate
3.02 yr Expiration
In Use 3 yrs
V2I-RA, V2I-LA, V2I-DCM Certificate
3.02 yr Expiration
In Use 1 yrs
V2I-PCA Certificate
4 yr Expiration
In Use 1 yrs
V2I-PCA Certificate
4 yr Expiration
In Use 1 yrs
V2I-PCA Certificate
4 yr Expiration
In Use 1 yrs
V2I-PCA Certificate
4 yr Expiration
In Use 1 yrs
V2I-PCA Certificate
4 yr Expiration
In Use 1 yrs
V2I-PCA Certificate
4 yr Expiration
In Use 1 yrs
V2I-PCA Certificate
4 yr Expiration
In Use 1 yrs
PG,MA Certificate
3.02 yr Expiration
In Use 3 yrs
PG,MA Certificate
3.02 yr Expiration
In Use 3 yrs
PG,MA Certificate
3.02 yr Expiration
In Use 1 yrs
CV Pilots Estimated Duration (5-7 years)
Estimated 1.5 year EE enrollment ramp up
EEs must undergo re-enrollment
Until end of year 3: EEs initially provisioned with 3 yrs of pseudonym certificates
Starting at year 4: EEs initially provisioned with less than 3 yrs of pseudonym certificates
Pre-generation of pseudonym certificates stops
Year 6 Enrollment stops
Private keys for ICA & lower destroyed

t

2.1.3 Hardware, Software and OS Security

Hardware, Software and OS Security for Pilot Deployment Devices provided by NYC Safety Pilot project.

2.1.3.1 Overview and goals

This document describes hardware, software, and operating system security for systems that run DSRC applications that use cryptographic private keys and certificates in the format specified by IEEE Std 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:

- Different privileged applications can have different sets of keys such that
  - A privileged application is able to sign with its own keys
  - A privileged application is not able to sign with keys reserved for use by a different privileged application
  - Non-privileged applications do not have any access to keys that are reserved for use by privileged applications.
- No application has read access to key material – all key material is execute- or write-only.
- Keys used for verification are protected against unauthorized replacement.
- 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.

2.1.3.2 Architectures

The requirements below cover three architectures.

- **Integrated architecture** (Figure 1): The host processor and the HSM are the same processor.
- **Connected architecture** (Figure 2): The host processor and the HSM are different, but they are physically connected using a connector that connects only those two processors, such that the only way to read or write data flowing between the two processors is by physically tapping into that connector.
- **Networked architecture** (Figure 3): 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 requirement for the host processor and the HSM separately in sections 3 and 4 respectively, and then provides architecture-specific requirements in section 5.

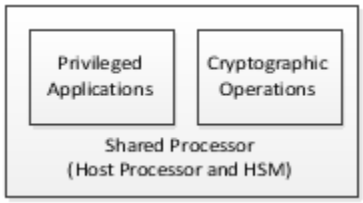


Figure 1 – Integrated architecture

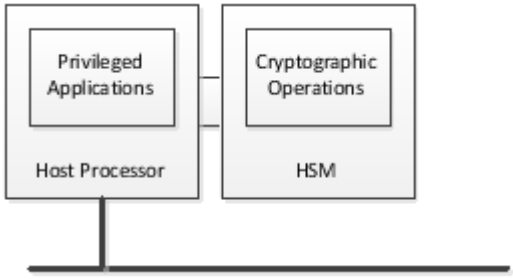


Figure 2 – Connected architecture

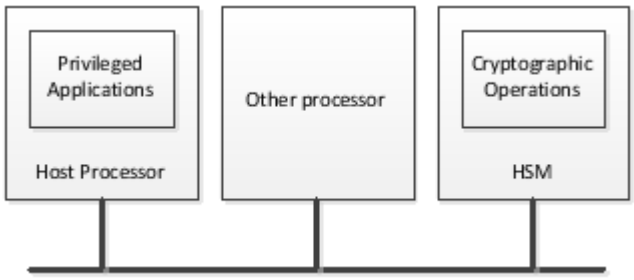


Figure 3 – Networked architecture

2.1.3.3 Host processor

2.1.3.3.1 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.

2.1.3.3.2 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 (TCG)'s 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 request signing 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 such that:

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

2.1.3.3.3 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) the following programs and plaintext data stored 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, for example 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 must also not provide this functionality)

2.1.3.3.4 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 is signed: in other words, 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.

2.1.3.4 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 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 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.

2.1.3.4.1 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.

2.1.3.4.2 Randon number generator

An HSM shall use a random number generator from the list of Approved random number generators in FIPS 140-2 Annex C (2016 draft).

2.1.3.5 Architecture-specific requirements

2.1.3.5.1 Integrated architecture

An integrated processor meets the complete set of requirements identified in sections 3 and 4.

2.1.3.5.2 Connected architecture

Modifications are the following:

- Since it is assumed that the OS on the device manages process separation, the HSM need only maintain two roles:
  - User (which can execute software and firmware, write and delete cryptographic keys, and install signed software and firmware)
  - Security Officer (which can install unsigned software and firmware

The HSM may support additional roles, either corresponding to the different privileged applications, or corresponding to non-privileged applications.

- Activities carried out by the User role do not need to be explicitly authenticated.

2.1.3.5.3 Networked architecture

Modifications are the following:

- All of the Connected architecture requirements above
- In addition, 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.

2.1.3.6 Storage

2.1.3.6.1 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 we refer to as “automotive grade”) to less reliable but cheaper storage (which we refer to as “standard grade”). For example, infotainment systems may use (though we are not sure of this) less-reliable, cheaper storage to allow more storage to be provided.

We assume in this document that automotive-grade storage is so expensive that less than 1 MB will be available. We assume that standard-grade storage will also be available and that it will be

sufficiently cheap to be provided in larger volumes, 100 MB or more. We assume that the executable security and security management code can be provided in a form that does not use the automotive-grade Flash.

2.1.3.6.2 Secure storage

- The OBE needs to store the following, encrypted, in the highly available memory:
  - Its local private keys for signing
  - Local CSR signing key
  - Any symmetric keys used for certificate management, for example 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, so we do not consider that there is a requirement for certificates to be encrypted in place, so 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.
- We assume 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 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.

2.1.3.7 Secure Environment for Device Enrollment

2.1.3.7.1 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 OBU 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 procedure defined in Use Case 2: OBE Bootstrapping.

2.1.3.7.2 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

2.1.3.7.2.1 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 section D (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 104-2 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 the section above. 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 the section above.
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.

2.1.3.7.2.2 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 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.

2.1.3.7.2.3 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 documented procedures.

2.1.3.7.2.4 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:

- Each enrollment location shall maintain a log that records the results of the steps defined in the 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.
- 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.

2.1.4 Root Management and Revocation Recovery

2.1.4.1 Root Management Background

When managing Public-Key Infrastructure (PKI) Credentials, which is the central purpose of the Security Credential Management System (SCMS), the roots of trust for the system, which are the eventual stopping point for trust chains, are a crucial component. The roots of trust chains, or *Trust Anchors*, are a set of certificates or public keys for which signatures will be implicitly trusted by the system. The implicitly trusted entity (*Trust Anchor*) certificates are stored in tamper-evident storage usually referred to as a *Trust Store*. A signature on a certificate from an entity above is what allows a trust chain validator to climb up a link of the chain, and if the last signature of the chain is verified, and that entity is implicitly trusted (a trust anchor), then the whole chain is accepted and trust flows down to the entity at the bottom of the chain. This concept is called chain-validation of certificates, and is the fundamental concept of a PKI. If these trust anchors are not secure, then neither is the system as a whole. If trust anchors cannot be managed as the system evolves, then the system will likely become incapable of producing trusted credentials for the End Entities (EEs) which rely on it. This is because, if a root of trust is compromised and there is no way to revoke and replace it, then the system will not be able to recover. Here an EE is either On-Board Equipment (OBE) or Road-Side Equipment (RSE).

2.1.4.2 High-Level Goals

The high-level goals for Root Management and Revocation Recovery are to provide the system with the means to heal itself from single compromises of even the highest-level components. It must be possible to bring the system into a state where it can again endure another singleton compromise. This recovery should occur while keeping the EEs operational whenever possible - that is, capable of sending, receiving and validating BSMs from non-compromised components - and be able to heal the system hierarchy without requiring physical access to EEs.

2.1.4.3 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, is the approach that has been selected for SCMS root management. In this scheme there are at least three Electors (there can be more, but the minimum of three has been selected for the initial deployment). These Electors have the capability to *vote* to endorse or revoke a Root CA or another Elector. When a *quorum* of valid Elector votes are attached to a message, it can be trusted by any component in the SCMS.

The resulting system may have multiple self-signed Root CAs, each of which operates as the top of the trust chain in a conventional PKI. Each Root CA's certificate is *endorsed* (i.e., certificates themselves are self-signed and the endorser provides a signature on the self-signed certificates) by at least a *quorum* of votes from non-revoked Electors. Only the Electors' certificates need tamper-evident storage, even though both Root CAs' and Electors' certificates are self-signed (although for efficiency EEs may choose to cache validated Root CA certificates or certificate hashes in secure memory as discussed below). The devices need to verify the trust chain up to Root CA, at which point they must verify that a *quorum* of non-revoked Electors have endorsed that Root CA.

2.1.4.3.1 Trust Management Messages

Electors operate by signing Trust Management Messages to be consumed by other SCMS components, including EEs. These Trust Management Messages include this basic set:

Add:

- Add Root CA Certificate
- Add Elector Certificate

Revoke:

- Revoke Root CA Certificate
- Revoke Elector Certificate

These trust management messages each contain a signature of an Elector. Such a signed trust management message is herein called a *Vote*. These votes can be either in favor of a new component (an *Endorsement*) or against an old component (a *Revocation*). Components (including EEs) know the number of such votes from non-revoked Electors that together will

authorize the action contained in the messages. These messages contain a period for the operation to occur. Re-provisioning an entities certificate is often described as Certificate Rollover. Certificate Rollover for a component can be implemented by first adding the new certificate and then revoking the old certificate sometime afterwards. For this rollover, the Add and Revoke messages could be delivered together, so it is beneficial to have a message, which contains a sequence of trust management actions. The SCMS Manager will coordinate the production of these Trust Management Messages.

2.1.4.3.2 Structure of Ballots

Elector votes could be distinct, but, in order to simplify the requirements on the EE and other components processing them, all Elector votes will instead be placed into one ASN.1 structure, referred to as a *Ballot*, which is the record of votes, in this case from multiple Electors. The ballot will contain:

- A Sequence of Root Management **Actions** (Currently Add or Revoke), each containing:
  - The Certificate of the **Object** of the Action (i.e. the self-signed certificate of the root to be added or revoked, or the self-signed certificate of an elector to be added or revoked)
  - The **Time** for the Action to take effect. The effective time for the action to be taken must be specified in the message. Electors shall not sign and (components should not accept as valid) an action with an effective time that occurs prior to the generation time of the elector signature generation time. When building a root management message, the SCMS Manager must choose an effective that allows for any time delay in accessing the Electors to generate their signatures. This has the benefit that a "stale" message (perhaps with less than *quorum* votes already signed) cannot be presented to an elector at some point in the future for a signature. Once the effective time has passed, no new elector votes can be added to the message.
- A sequence of Elector Signatures. A ballot consists of a sequence of independent signatures from each elector. The data to be signed by each elector is the root management action described in item 1 above and the current time (i.e. the current time when the elector signature is generated which is always included in 1609.2 signatures in the *generationTime* field of the *headerInfo* component).

Time is important in root management actions in order to support a managed rollover. It is anticipated that the distribution of a new root certificate ballot and the generation of new device certificates will require some time. This can be accommodated by setting the activation time of a new root CA certificate and the corresponding revocation of a previous root CA certificate to a time in the future. A managed sequence will not be possible in the case of a root compromise where the activation time for the old root revocation may be distributed prior to the creation of a new Root CA, resulting in a period of service disruption while new device certificates are signed by the new root and distributed.

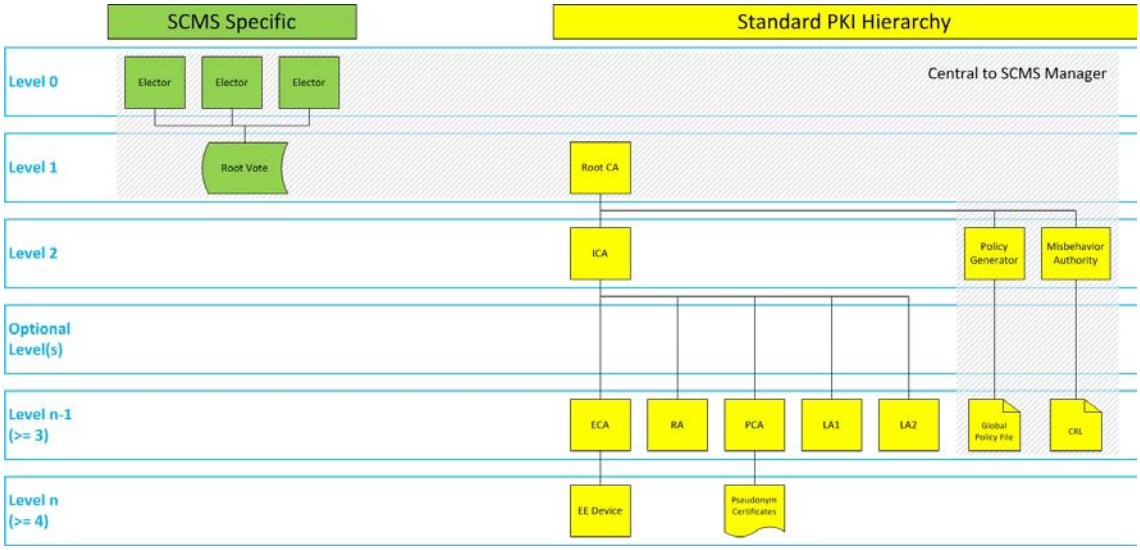
Note that due to the very long time spans over which an elector may be valid, the device may not be able to maintain a trusted source of time during its entire useful life. It will therefore be necessary for the operational policies and procedures on operating electors to provide a trusted source of the current time when they are asked to sign a ballot. While not specified here, policy

may enforce a limit on the span of time allowed in a root management message. For example, policy may declare that no root management message shall be created with an effective date that is more than 1 year in the future.

2.1.4.3.3 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 1609.2 certificates without modification. A significant advantage of the Elector based scheme is that, as new Electors are added at level 1, an existing Root CA can receive new endorsements from an Elector without having to change their certificates.

Figure 1 Endorsement Method details



2.1.4.3.4 Revocation/Addition Impact on EEs

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

Operation	Elector Model Implementation
Revoking an Elector	Revoking one Elector does not stop EE operation, the remaining Elector endorsements of the Root CA certificate would still verify. As long as there are at least three Electors with a quorum of two, then one Elector may be removed without impacting operation. A replacement elector may then be added back to the system to return to a state with three valid electors. For national deployment, a larger number of Electors may be used to improve the system's resilience to compromise or failure of these top-level trust anchors.

Operation	Elector Model Implementation
Revoking a Root CA	Revoking a Root CA would stop EE operation for all certificates chaining up to the revoked Root CA. All impacted EEs could get updates over the air (over the DSRC channel or through an OEM proprietary connection) with a new LCCF, which would include a new Root CA endorsed by a quorum of Electors, and new component certificates that chain up to the new Root CA. Note: Some EEs may need to replace their enrollment certificate after a Root CA has been replaced. A method for remote secure re-enrollment will be included in a future release of the SCMS documentation.
Adding an Elector	A new self-signed Elector certificate that is endorsed by a *quorum* of Electors can be trusted by EEs and other SCMS components without the need of returning them to a secure environment. The ballot that adds the new elector shall be distributed to EEs through an updated LCCF. In addition, this new Elector can endorse existing Root CA certificates without the need for any updates of the existing valid certificates, including EE's pseudonym certificates.
Adding a Root CA	A new self-signed Root CA certificate can be distributed to EEs as a message in the LCCF, signed by at least a quorum of valid Electors. Once this message is received and validated, EEs may begin to trust messages that chain up to the new Root CA.

2.1.4.3.5 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 1609.2 certificates.

2.1.4.3.6 Logical Separation of Electors and Roots, Possible Operational Merging

Setting up a Root CA is an expensive, complex task, and commissioning higher-level components, such as Electors, will be similarly complicated and costly, involving physical and organizational protection, policy development and the secure implementation thereof. For this reason, even though entities with Trust Management authority (e.g. Electors) may be kept distinct from those with PKI authority (e.g. Root CAs), they may also be merged operationally, if the efficiency to be gained is attractive and the increased risk acceptable. To keep logical separation, the certificates of Electors and Root CAs distinct, even if they are operated from the same physical entity.

2.1.4.4 Elector Model Design Details

- **Revocation**: How can a Root CA or Elector be revoked?
  Solution: Any Root CA or Elector certificate can only be revoked by a special revocation message that is signed by a *quorum* of Electors.
  Centralized components will not be provisioned with certificates through an ICA, but directly

from a Root CA, which being operational very infrequently will be much harder to compromise. Each Root CA will delegate revocation authority over its sub-components using the CRL series mechanism defined in 1609.2. Because the composite CRL is frequently distributed to EEs, the revocation of Electors or Root CAs will be included in CRLs as Elector signed revocation messages.

- **Renewal**: How is a new Root CA added to the SCMS, communicated and trusted by the other components and EEs?
  Solution: A new self-signed Root CA certificate must be endorsed by a quorum of Electors. The SCMS Manager will orchestrate this endorsement process and inform the SCMS components by means of the Global Certificate Chain File (GCCF) updates; RA will inform EEs through a local version of the GCCF - the LCCF.

- **RA**: When an RA chains up to a compromised component, the EE still must be able to obtain information on the updated SCMS. How is this done?
  Solution: An EE can download and validate any Elector based endorsements contained in a fresh copy of the LCCF (or GCCF if a local copy is not available) without needing to validate or trust the RA. This file can be downloaded from any RA (even if the RA certificate is no longer trusted, the EE can download and validate the root management commands in the certificate chain file) or it may be pushed down to EEs through alternative, proprietary communications channels.

- **Enrollment Certificates**: The SCMS identifies devices only by their enrollment certificates. How can a device securely identify itself in order to obtain new credentials, if these enrollment certificates chain up to a compromised component?
  Solution: For the PoC, the only mechanism for replacing enrollment certificates is manual re-enrollment of the EE. This will require physical access to the EE (or an authorized proprietary channel for performing re-enrollment). In future releases of the SCMS, a local ICA manager will have the ability to use SCMS messages to restore trust to un-revoked EEs under certain conditions even after a higher-level component has been revoked. When this re-enrollment process occurs, the EE will be required to generate a new key pair such that the new enrollment certificate contains a distinct public key, different from the one in the old enrollment certificate.

- **Policy**: When the top-level authorities issue information, what rules are used to evaluate them, and how in turn is this collection of rules secured?
  Solution: For the PoC, all EEs and SCMS components will use a fixed value of two for the *quorum* of electors that must endorse a valid root management message. In a future release of the SCMS, an elector-signed segment of the GPF will list the current value of *quorum*, enabling changes to this value to be endorsed through Elector votes. By separating this small segment of the GPF (and subsequently the LPF) from other policy information, the electors only need to be accessed when the *quorum* value is to be changed. The Policy Generator (PG) will sign all other global policy information and the local RA will sign local policies.

- **Pseudonym Certificates**: When a Root CA has been revoked, how are EEs kept operational if their entire pseudonym certificates chain to that single Root CA?
  Solution: For the PoC, an EE's pseudonym certificates will rely on a single Root CA such that revocation of that Root CA will require that the EE first get a new LCCF with a valid Root CA endorsement of a new root. The EE will then switch to an RA that validates up to the new root and request new pseudonym certificates. The EE will be temporarily unable to sign BSMs until this process is complete. However, the update can be carried out without recalling or re-enrolling the EE. For national deployment of the SCMS, we recommend that each EE receive a mix of pseudonym certificates that chain up to at least two different Root CAs. This would allow for a more graceful degradation of service even after revocation of a Root CA.

2.1.4.5 PoC Deployment Model

The PoC will implement the Elector based scheme described here. For the PoC, a 2/3 Elector scheme will be tested, with a single active Root CA. The PoC will not deploy the redundancy of multiple Root CAs, but it will be considered for post-PoC implementation.

2.1.4.6 Impact on EE Storage

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 1609.2 Self-Signed Certificates. In the PoC, three Electors will be operational. Storage for four at least for 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.

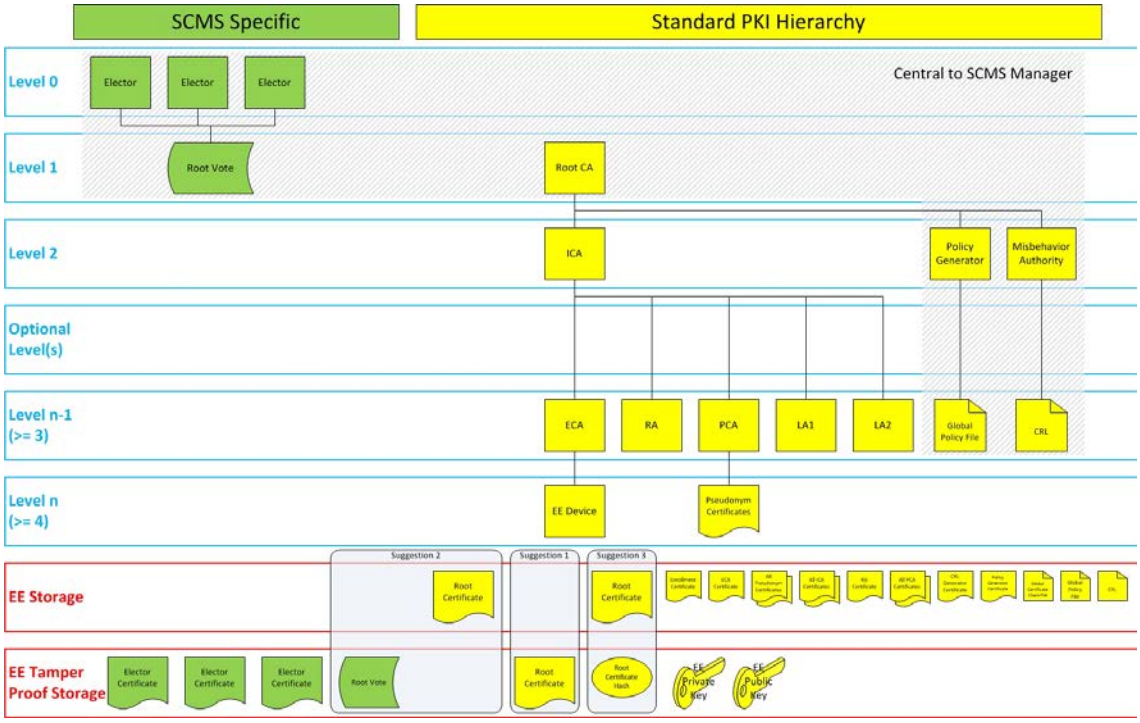
3. EEs must have secure software used to update the Trust Store through the correct processing of ballots. This also involves protection for basic parameters under which votes are acted upon, the *quorum*, which is assumed some number less than ten.

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:

1. Suggestion 1: Store the Root CA certificate directly in tamper-evident storage. This approach allows the EE to access quickly the Root CA certificate with no further validation (EE must validate it only once before it is placed in secure storage).
2. Suggestion 2: The EE may store the endorsement message signed by the Electors in secure storage.
3. 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 2 EE Storage Requirements



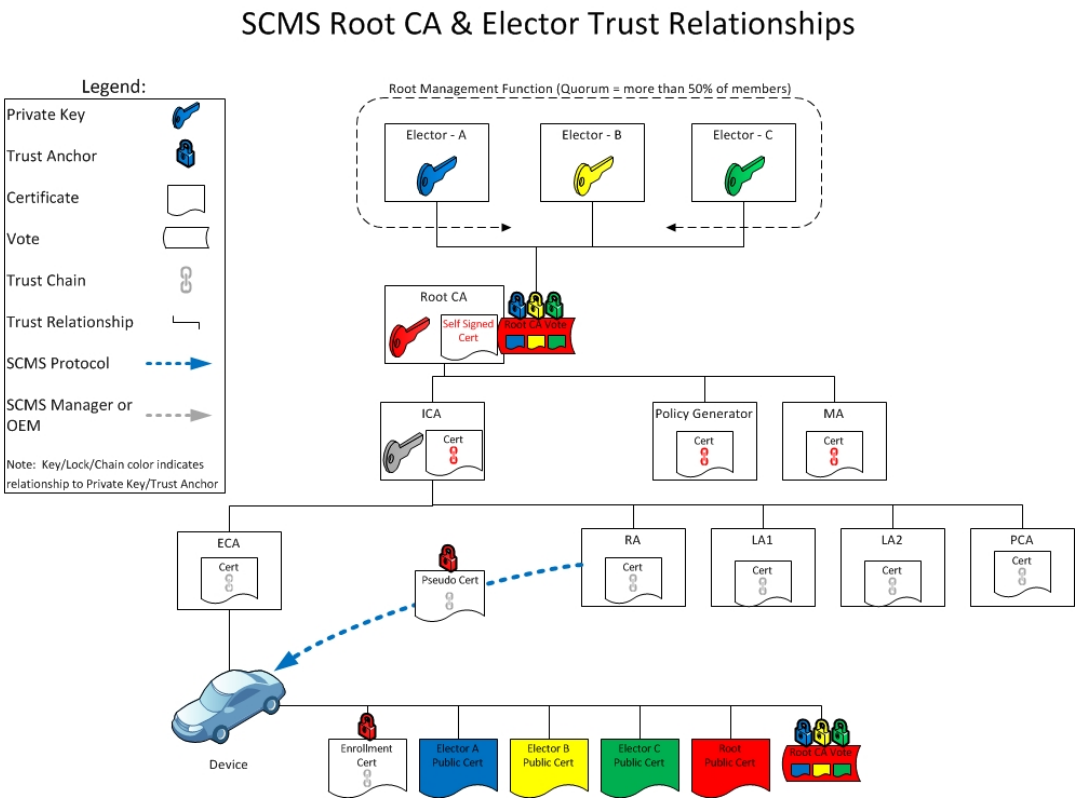
2.1.4.7 Root Management and Disaster Recovery in Action

This section aims to show Root Management and Disaster Recovery in action. To this end, the revocation and replacement of an Elector is described below:

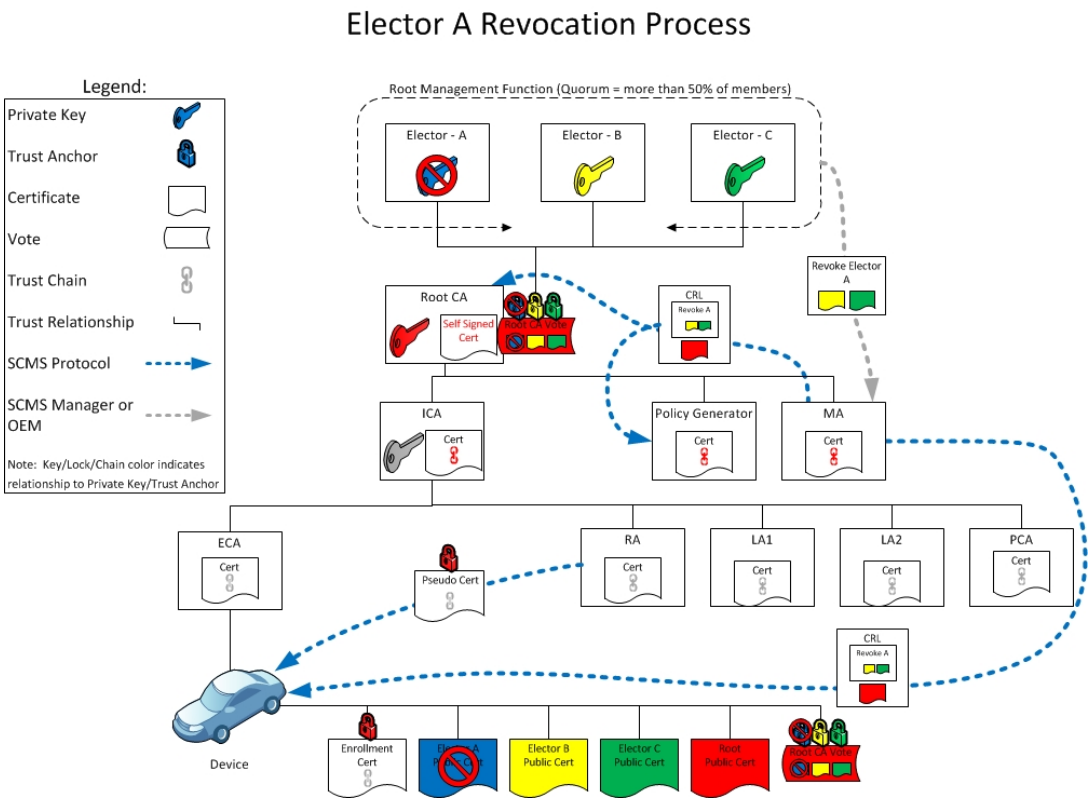
1. Day 1: Typical SCMS Operations
2. Day 2: Revoking an Elector
3. Day 3: SCMS Operating with 2 Electors Only
4. Day 4: Replacing a Elector
5. Day 5: SCMS Returning to Typical Operation

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

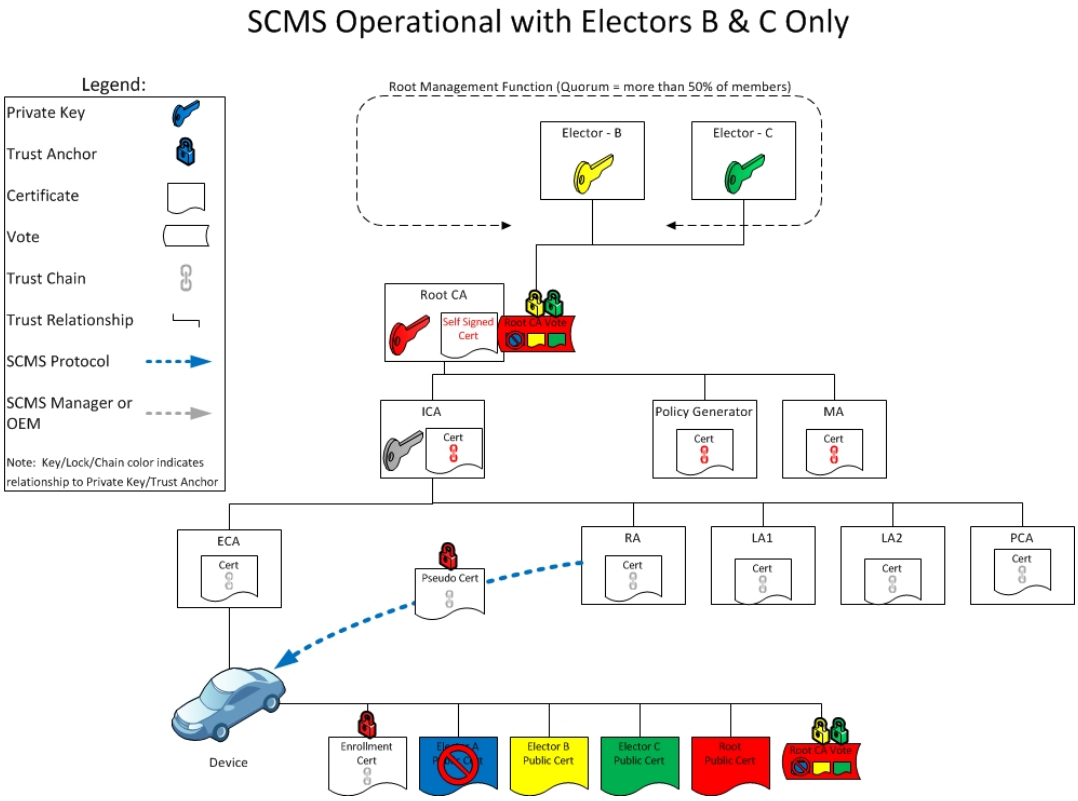


Day 2: Revoking an Elector



In 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.

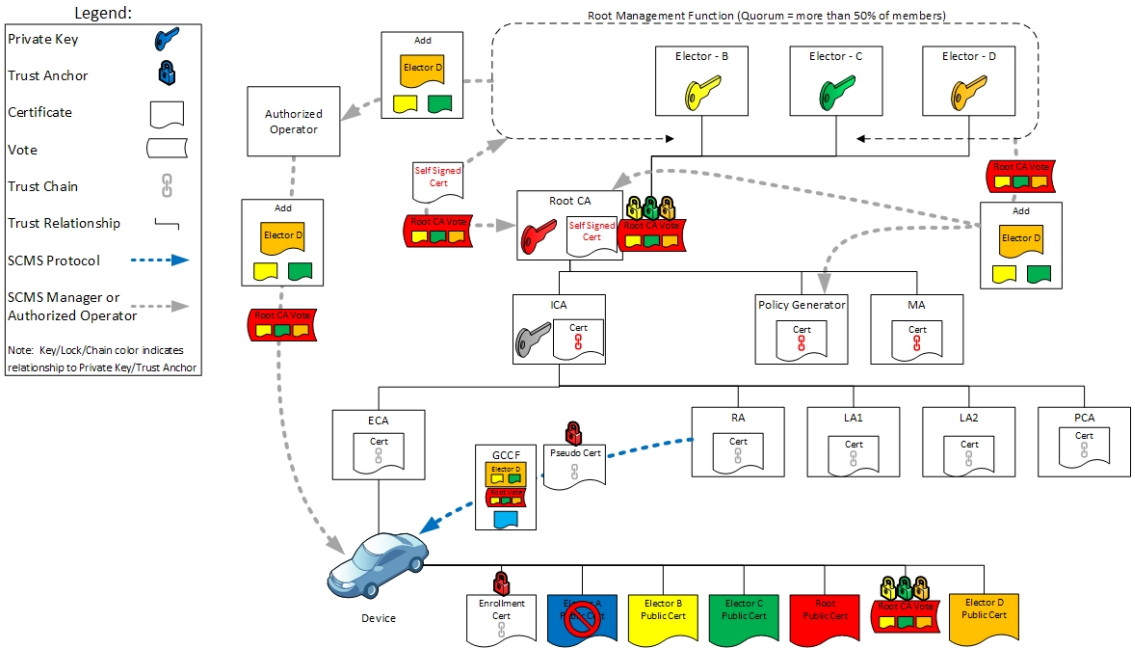
Day 3: SCMS operating with two Electors only



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

Day 4: Replacing an Elector

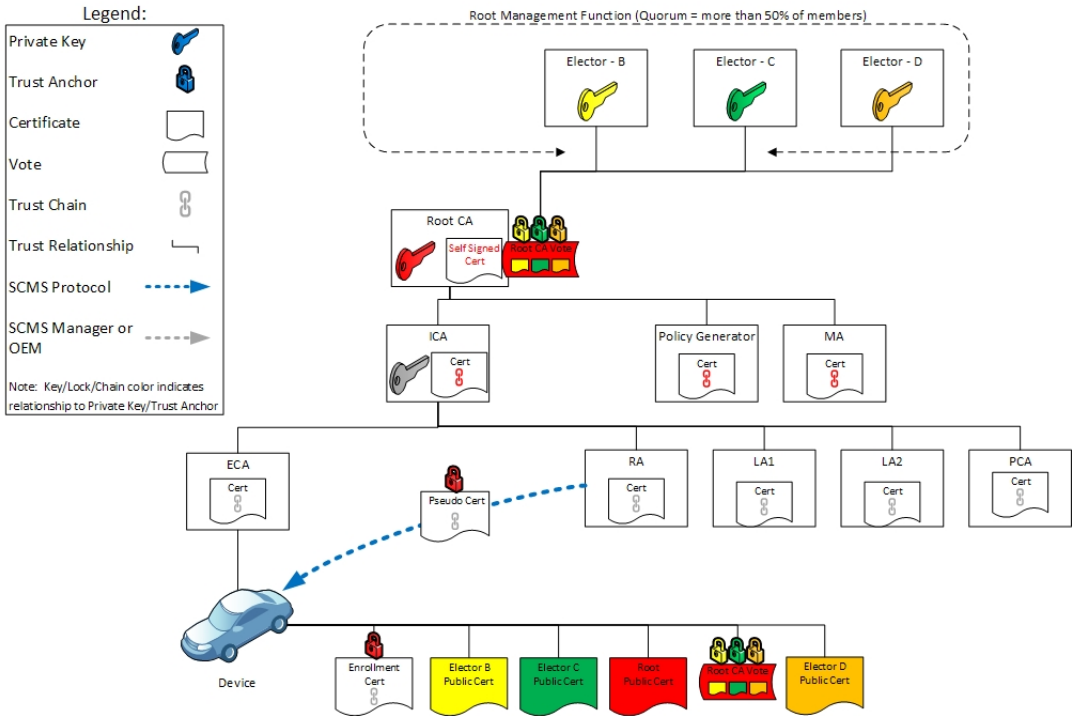
Introduce Elector D



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 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:

SCMS Trust Relationships with Elector D

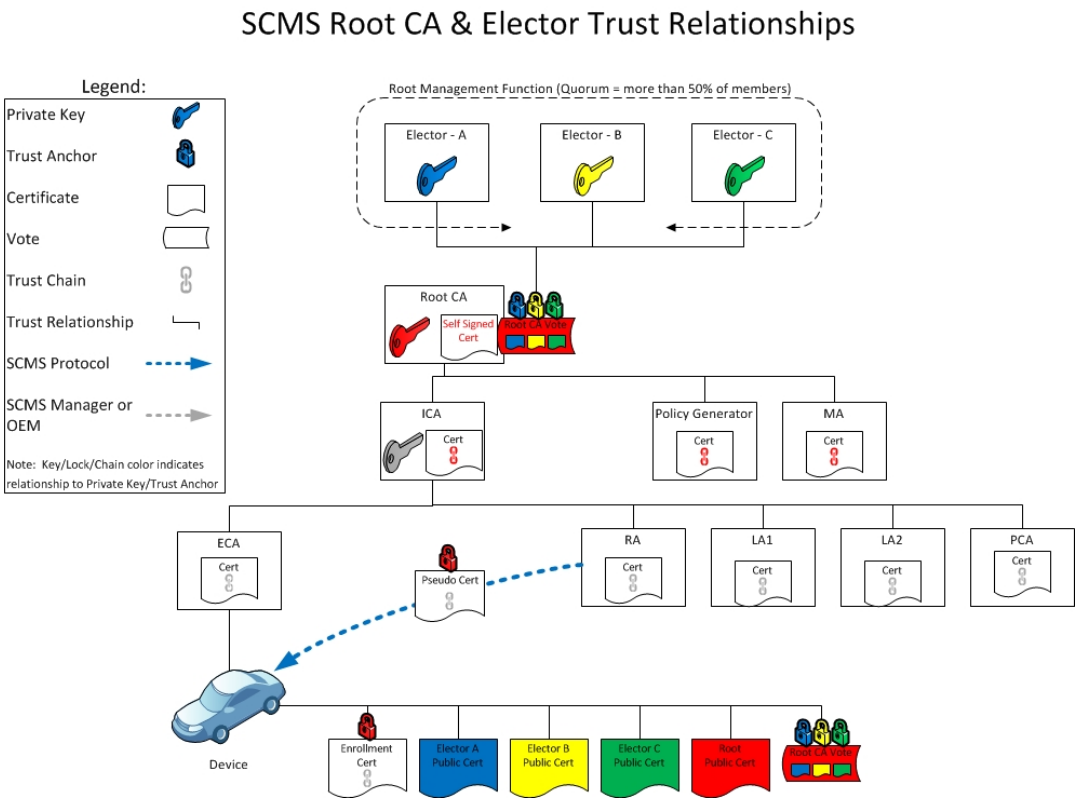


In Day 5, the SCMS has been returned to an equivalent of the Initial State of Day 1, with a replacement Elector.

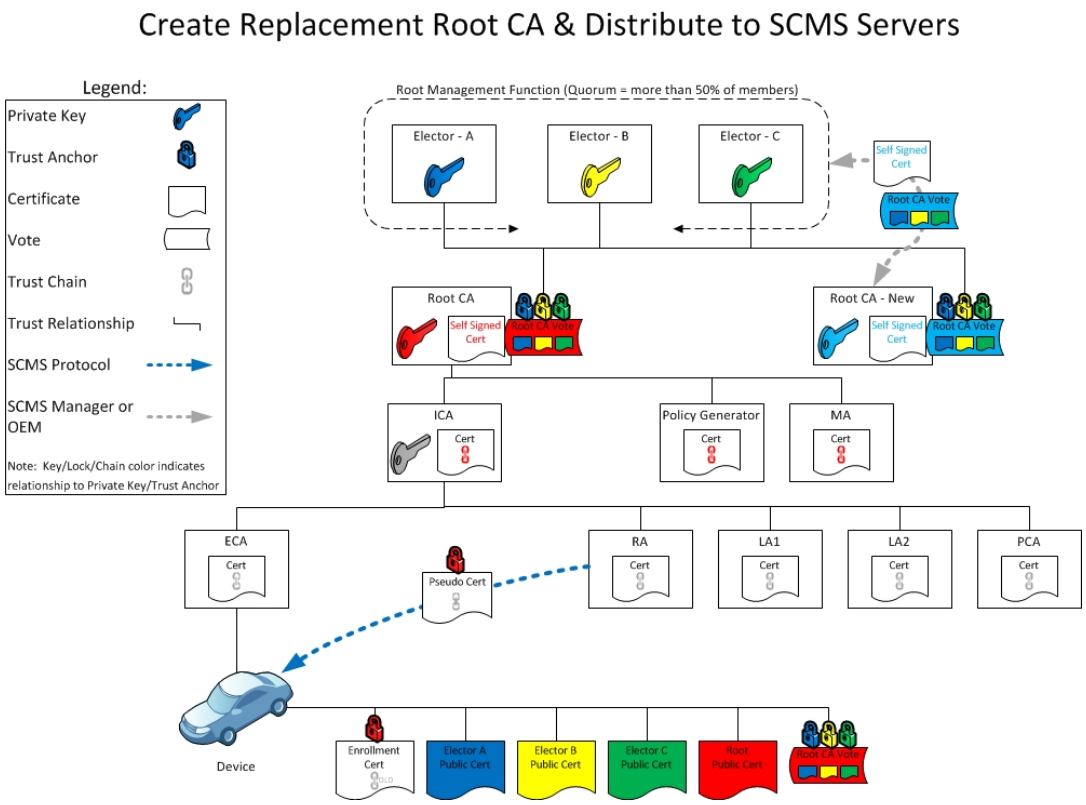
The following describes the revocation and replacement of a Root CA:

- Day 1: Typical SCMS Operations
- Day 2: Standing up a New Root CA
- Day 3: Putting the SCMS Backend Trust Relationships in place for the New Root CA
- Day 4: Revoking the Old and Adding the New Root CA
- Day 5: Revoked Root CA, System Non-functional
- Day 6: System Functionality Restored

Day 1: Typical SCMS Operations:



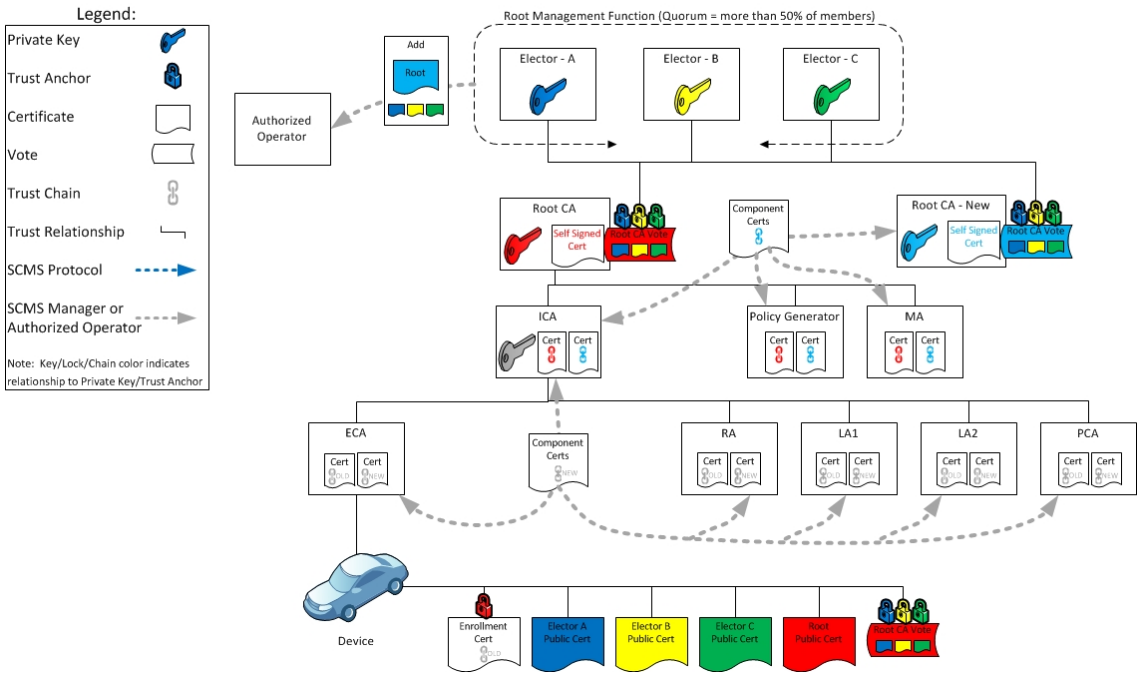
Day 2: Standing up a New Root CA



In Day 2, the new Root CA is stood up and Endorsed, but is not used by SCMS.

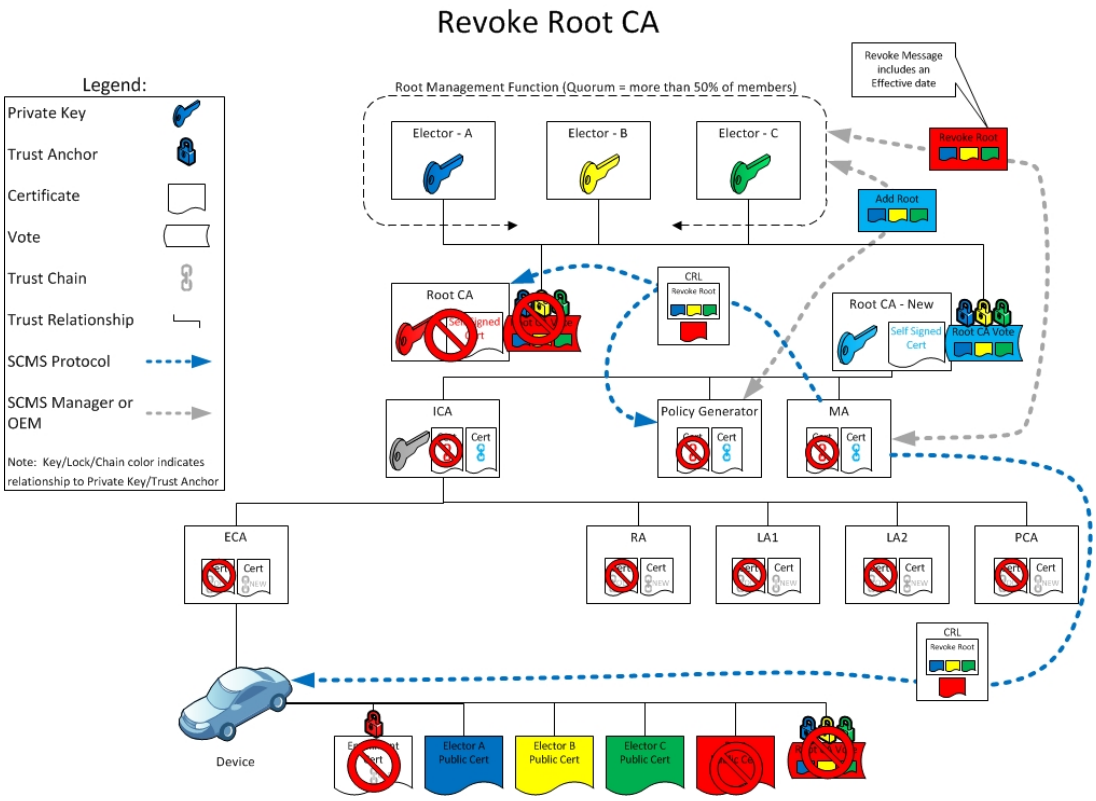
Day 3: Putting the SCMS Backend Trust Relationships in place for the New Root CA

Introduce Replacement Root CA Before Revoking Current Root CA



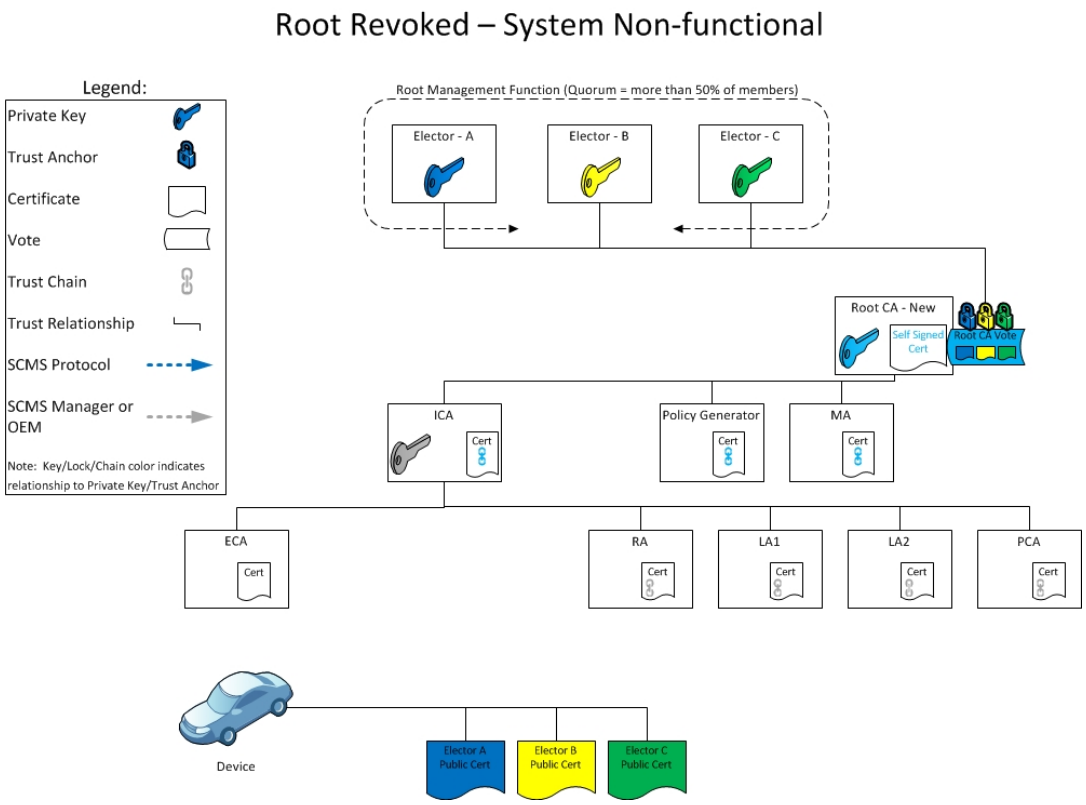
On Day 3, all of the background tasks of generating new certificates for SCMS components is performed, but these are not made active. The new Root Management operation: "Add Root CA" is distributed to all the Authorized Operators to prepare them for distribution.

Day 4: Revoking the Old and Adding the New Root CA



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.

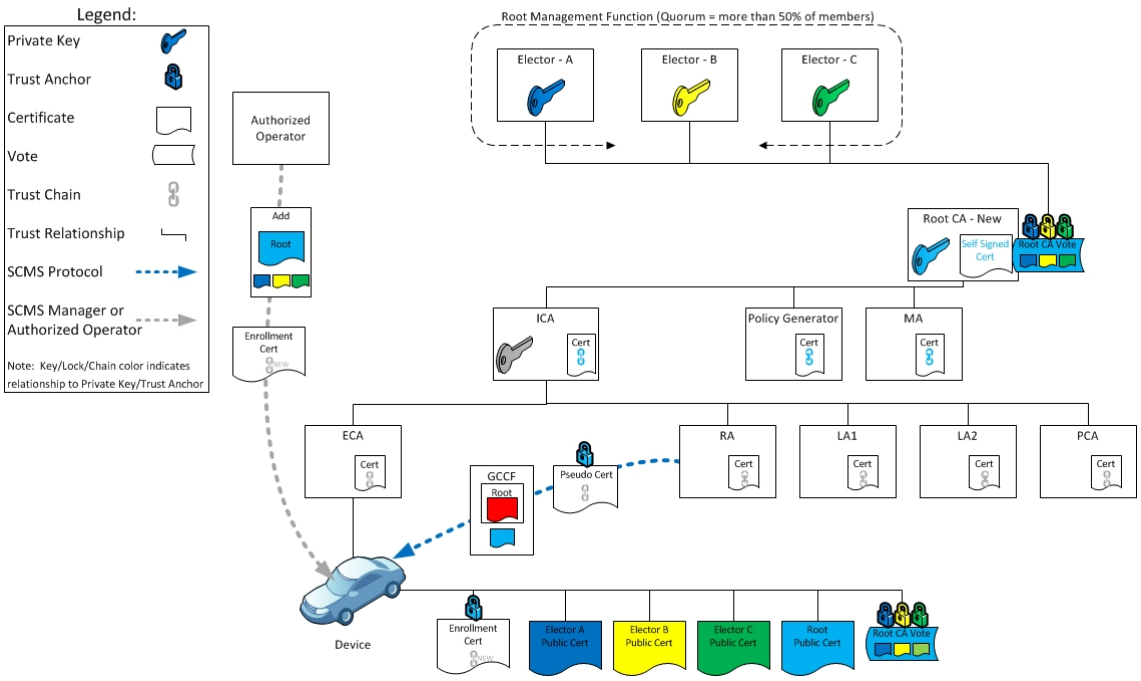
Day 5: Revoked Root CA, System Non-functional



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

Update EEs with new certificates



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 specify the mechanism used to provide new enrollment certificates to EEs, yet; 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 once more.

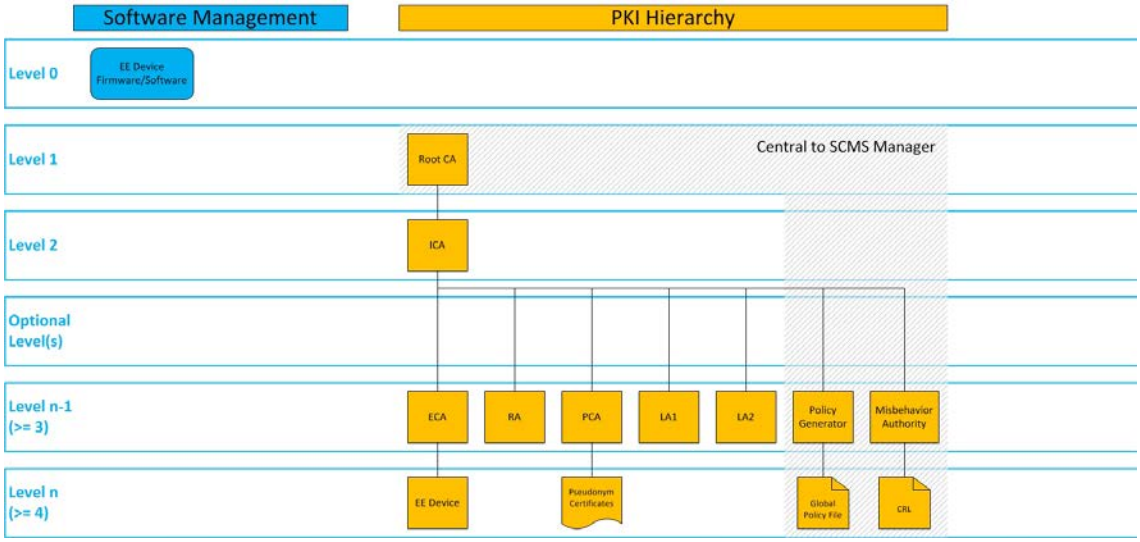
2.1.4.8 Analysis and Comparison of Solutions

2.1.4.8.1 Software Update for Root Management

In many modern PKI-based systems, software updates perform the top-level root management, which includes updating root certificates in a client's *Trust Store*. Validation of a software update is often accomplished via public-key signatures on the updates, which makes security of the software update similar to the managed PKI system. Therefore, protection of the software update's public key must be equal or better than the protection of trust anchors in the client's trust store. This results in a hierarchical scheme in which the software update employs a public key (or certificate) at a higher level than the PKI trust anchors, since the software update can update the PKI trust store. The SCMS structure described in the "Vehicle Safety Communication Security Studies – Final Report" is also a traditional PKI hierarchy, with a Root Certificate Authority (Root CA), intermediate CAs (ICAs), and Registration Authority (RA). The diagram below shows the Pseudonym CA (PCA) as well as other non-traditional components of the SCMS.

The diagram attaches numbers to levels in the hierarchy, with Level 0 being the topmost level, which has administrative control of the End Entity (EE). Level 1 being at the level of the PKI Trust Anchor, and other components at levels below:

Figure 3 Authorization Hierarchy



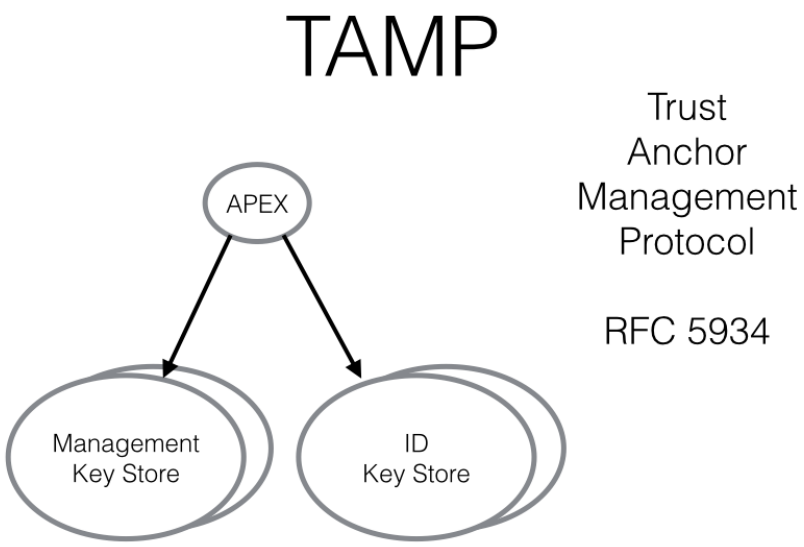
While the software update approach to top level PKI management is commonly used today, this model was deemed unacceptable for use in the SCMS. The key weakness of this approach is that it relies on a separate root of trust that itself faces the unresolved challenge of securely managing that higher-level root. In addition, in the fully deployed SCMS system, OEMs will each choose different methods for updating software in their vehicles. The security design of the SCMS should be independent of individual decisions made by each manufacturer. Rather than forcing all OEMs to adopt a short list of "approved" software update schemes, an alternative design was chosen that separates root management from the software update process.

2.1.4.8.2 TAMP Model

Hierarchical schemes, like the software update scheme above, use higher-level authorities to authorize lower-level entities. The SCMS has a PKI hierarchy already, where the Root CA authorizes ICAs. This Root CA could be used to authorize the addition of new ICAs and the revocation of old ones, creating a basic scheme for trust management. Because of its importance, a Root CA is typically protected with additional security measures, such as being offline, employing highly secure hardware, located in a highly secure facility, etc. In this scheme the Root CA is a single point of failure; if it is compromised, the system fails.

An Internet Engineering Task Force (IETF) scheme targeting Trust Management, RFC 5934 Trust Anchor Management Protocol (TAMP), is also a hierarchical scheme. It aims to replace proprietary trust management via software update, and is referenced as a model by systems needing trust management. It employs multiple keys above the PKI hierarchy to control the addition and subtraction of trust anchors from trust stores, and has some other interesting

technology such as backup public top-level keys, which are held encrypted until they are needed, a technique aiming to reduce exposure of the keys at the top of the hierarchy. It also introduces admin keys at the top level, which are used for such management actions as software update.



The common feature of these hierarchical systems is that they employ a trusted entity, which is above and manages the trust anchors. A single hierarchy, like the ones described above, may not be sufficiently flexible to grow, as new authorities appear. That is a distinct possibility in a scheme such as the SCMS, which eventually may be deployed multi-nationally. Most importantly, these schemes have a single point of failure. For these reasons, the TAMP model was not selected for the SCMS.

2.1.4.8.3 Triple-Signature Model

In the Triple-Signature model, three independent Root CAs replace the single Root CA at the top level of the PKI hierarchy. A minimum of two out of these three roots must all sign the public certificate of a new Top-level ICA (or T-ICA) in order for it to be trusted. This is very similar to the Elector based model that was ultimately selected for the SCMS and described in detail in the Root Management and Revocation Recovery section. The comparison in the following section evaluates the key differences between these two approaches.

2.1.4.8.4 Triple-Signature vs. Endorsement (Elector model)

The VSC5 Consortium has considered many Root Management schemes for the purpose of Recovery from Root CA compromise. Two methods (Triple-Signature and the Elector model)

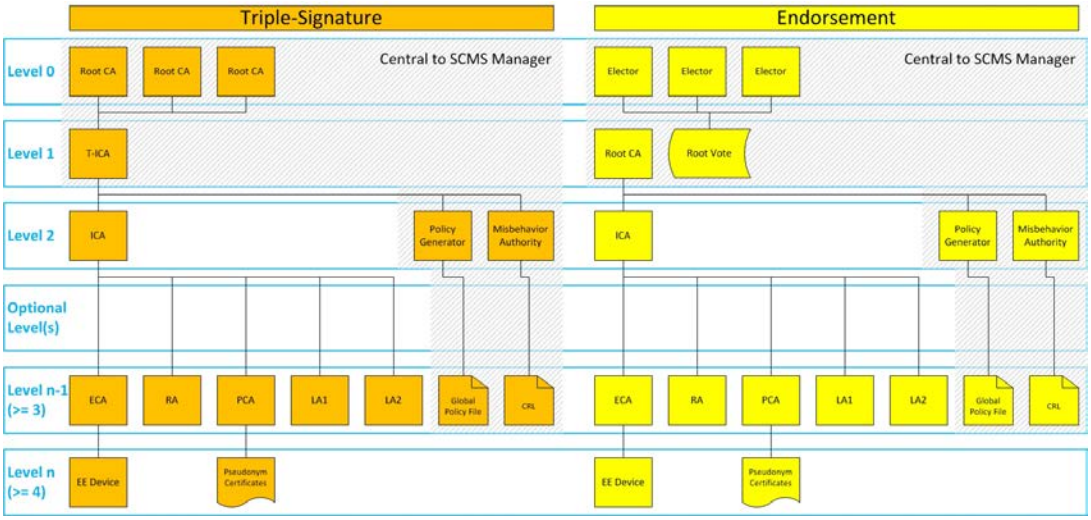
were the only ones that addressed the majority of the original design goals. To compare these two models, the section below describes sub-problems.

- Problem 1: **Revocation**: How can a Root CA, a Top Level ICA (T-ICA), Misbehavior Authority (MA), Policy Generator (PG) or Certificate Revocation List Generator (CRLG) be revoked? Note that if these were to be revoked via a CRL, then compromising a CRLG (or Root CA, T-ICA) could allow an attacker to disrupt severely the SCMS.
  Solution 1: Any Elector, or Root CA (or T-ICA in schemes that have them) certificates can only be revoked by a special revocation message that is signed by multiple top-level entities. Centralized components will not be provisioned certificates through an ICA, but directly from a Root CA, which being operational very infrequently will be much harder to compromise. Because the CRL is most frequently distributed to EEs, the revocation of Electors or Root CAs or centralized components should be included in CRLs.

- Problem 2: **Renewal**: How is a new Root CA added to the SCMS, communicated and trusted by the other components and EEs?
  Solution 2: A new Root CA certificate has to be authenticated by multiple top-level entities. The SCMS Manager will orchestrate this authentication and inform the SCMS components by means of the Global Certificate Chain File (GCCF) updates; the EEs will be informed through a local version of the GCCF - the LCCF.

- Problem 3: **Running**: When a Root CA (end of the trust chain) is compromised and revoked, how are EEs kept running for safety purposes, without the need to return vehicles to secure locations or replace their hardware? Note that the compromise of any component below Root CA in the PKI hierarchy can be handled by commissioning new components whose certificates chain to the trusted Root CA.
  Solution 3: There are two proposed solutions described in diagrams below along with a discussion of pros/cons:

Figure 4 Comparison of proposed solutions



- **Triple-Signature**: In this proposal, there are three Root CAs that also act as electors and multiple Top-Level ICAs (T-ICA); but the rest of the SCMS remains unchanged. A T-ICA is issued a certificate that is *triple-signed,* i.e. one certificate signed by all the three Root CAs and the devices are instructed to trust a certificate that chains back to a quorum of non-revoked Root CAs. Each Root CA certificate requires tamper-proof storage. In this scheme, the electors are also at the top of the PKI hierarchy (the *PKI apex*).
- **Endorsement**: In this proposal there are three Electors (there can be more, but this is set to three to compare with the Triple-Signature), multiple Root CAs each of which form independent trust anchors, but the rest of the SCMS stays as it was. Each of the Root CA's certificate is *endorsed* (i.e., certificates themselves are self-signed and the endorser provides a signature on the self-signed certificates) by at least a quorum of votes from the non-revoked Electors. Only the Electors' certificates need tamper-proof storage, even though both Root CAs' and Electors' certificates are self-signed. The devices need to verify the trust chain up to Root CA, at which point they must verify that a quorum of non-revoked Electors have endorsed that Root CA. Such calculations can be cached securely.

Below is a comparison of the two proposed solutions.

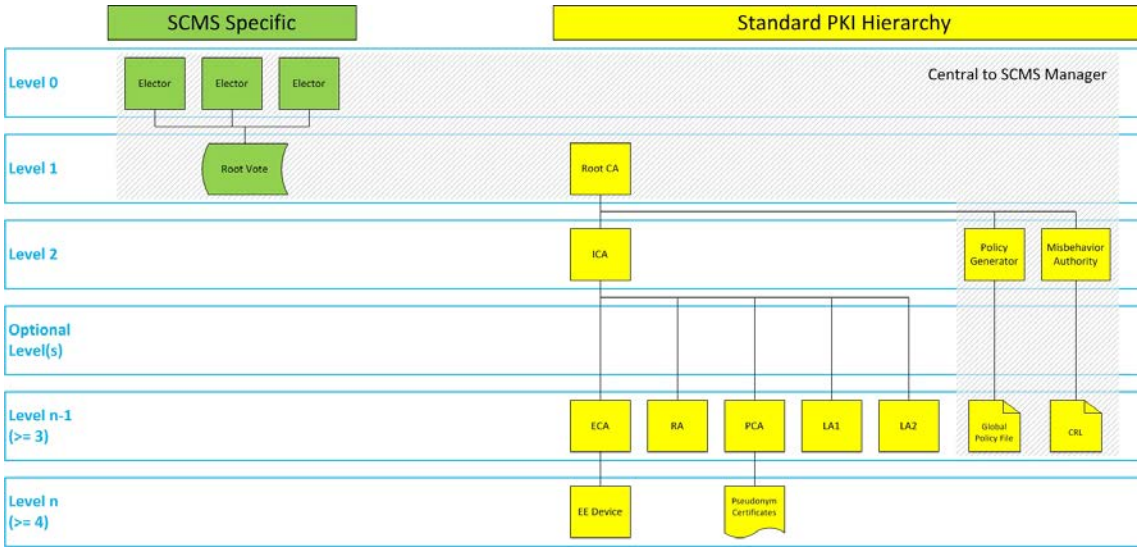
	Triple-Signature	Endorsement
Revoking a top-level Entity	Revoking a Root CA does not stop end-entity (EE) operation, since all currently valid certificates would still verify.	Revoking an Elector does not stop EE operation, since two of the votes on the Root CA certificate would still verify.
Revoking highest singleton of the PKI hierarchy	Revoking a Root CA does not stop EE operation. This is not a fair comparison perhaps, since revoking the T-ICA just below it would stop EE operation. In the Triple-Signature, the T-ICA is the highest singleton in the PKI hierarchy, the point at which a single revocation causes operation to stop.	Revoking a Root CA would stop EE operation for those chaining up to that Root CA (see * below table).
Adding a top-level entity	A new Root CA certificate that is endorsed by a quorum of Root CAs can be trusted by EEs and other SCMS components without the need returning them to a secure environment. However, if a T-ICA switches to a new certificate that is triple-signed by new Root CA, everything below the T-ICA, including EE pseudonym certificates, need to be updated (see * below table).	A new Elector certificate that is endorsed by a quorum of Electors can be trusted by EEs and other SCMS components without the need of returning them to a secure environment. In addition, this new Elector can endorse Root CA certificates without the need for any updates of the existing valid certificates, including EE's pseudonym certificates.

	Triple-Signature	Endorsement
Impact on 1609.2	Triple-signatures require 1609.2 changes.	Votes are defined at the SCMS level, and do not need 1609.2 changes.

*These EEs could however get updates over the air on the DSRC channel, and so would not need to be returned for update, assuming solutions to Problems 4 & 5 below are deployed. RSEs will have frequent connectivity in order to receive updates.

The main advantage of the Endorsement scheme is that, as new top-level entities are added (in the Voting scheme, these are Electors) level-1 entities can receive votes from the new Elector without having to change their certificates. This is a significant advantage. Otherwise, the two schemes are essentially equivalent regarding Problem 3, except in the way they affect 1609.2 standardization. The Voting scheme is illustrated below:

Figure 5 Endorsement Method details



- Problem 4: **RA**: When an RA chains up to a compromised component, the EE still must be able to obtain information on the updated SCMS. How is this done?
  Solution 4: In addition to RA - Retrieve Registration Authority Certificate, Authorized Operator (e.g. OEM, Road Operator, After-market device supplier, etc.) proprietary channels are relied on to update the EE on the new Root CA authenticating the RA, which allows the EE to trust it. Roadside Equipment (RSEs) is assumed to have frequent online connectivity to get new certificates as well as software updates.

- Problem 5: **Enrollment Certificates**: Devices are only identified to the SCMS by their enrollment certificates. If these enrollment certificates chain up to a compromised component, how can a device securely identify itself in order to obtain new credentials?
  Solution 5: Authorized Operator's will keep track of the enrollment certificates, or at least the public keys contained in them. Using the address of the old RA to communicate, or

proprietary channels, EE's will request re-certification of these public keys, using new certificate requests, and will be provided with new Enrollment Certificates, chaining up to non-revoked trust anchors. The Authorized Operator's will investigate which EEs may have been compromised, and ensure that new enrollment certificates are issued only to non-compromised EEs. In addition to Certificate Revocation Lists (CRLs), the SCMS backend components maintain blacklists of components, which they designate as invalid, but which need not be placed on a CRL for EE consumption, keeping the CRL space requirements lower. The internal blacklist will be used to indicate which enrollment certificates have been revoked. The re-issued enrollment certificates will duplicate permissions and other characteristics of the original enrollment certificates, so that this process cannot be used in a privilege escalation attack.

- Problem 6: **Policy**: When the top-level authorities issue information, what rules are used to evaluate them, and how in turn is this collection of rules secured?
  Solution 6: The EEs and SCMS Components are provided with two fixed quantities: the number of top-level entities, which form a quorum, and the total number top-level entities that can exist. These might be 2/3, 3/5, 4/7 or a similar choice. Consideration was made to place these quantities into the Global Policy File (GPF), but that is not suitable, since the only protection for the GPF is the signature of the Policy Generator, not the multiple signatures of Electors. The Policy Generator is a centralized component, which signs Policy Files and the Global Certificate Chain File (GCCF). Bringing Electors operational to update the GPF was considered, but this would mean the Electors would be operational too frequently.

- Problem 7: **Operation**: When the top of PKI hierarchy (Level 1 in the Authorization Hierarchy) has been revoked, how are EEs kept operational?
  Solution 7: There should be multiple components at the apex of the PKI hierarchy. The reasoning for this derives from the fact that 1609.2 certificates refer to the superior certificate by a hash of the complete superior certificate: if any 1609.2 certificate in a chain requires change, then all the certificates below it must also be changed. This means that a change to a higher-level component in the PKI hierarchy cannot be made without replacing all the certificates below it. In Triple-Signature, if the T-ICA for an EE's certificates is compromised, then operation stops for that EE. In the Voting scheme, if the Root CA of an EE's certificates is compromised, then similarly, operation stops for that EE. Having pseudo-certificates from multiple T-ICA's or Root CAs, respectively, allows EEs to continue operation but with fewer certificates: a graceful degradation. Similarly, having more components that are redundant at lower layers can allow lower layer compromise with graceful degradation; if certificates are provided that climb redundant chain validation pathways up to PKI apexes. If there are multiple PKI apex components, then these should all provide certificates to the components just beneath them in the PKI hierarchy. This is redundancy at the top of the PKI hierarchy. Each EE should be provided with pseudonym certificates for each operating period, which derive from multiple PKI apexes. EEs will still operate in the event of a PKI apex revocation, but will do so with fewer certificates (without the ones that chain to the revoked apex). If the redundancy is applied below the apex, then the scheme will be able to keep all EEs operational even with an outage at that lower level as well.

2.1.5 Cryptography

2.1.5.1 Approved Cryptographic Algorithms

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

- Signing
  - ECDSA over NIST p256
- Public key encryption
  - ECIES over NIST p256
- Hash:
  - SHA-256
- Symmetric Encryption
  - AES-CCM with 128-bit keys

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

2.1.5.2 Cryptography Background

2.1.5.2.1 CB1: Cryptographic Services

2.1.5.2.1.1 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.

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

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:

- 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 Std 802.11 and actively supported by service primitives in IEEE Std 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.

2.1.5.2.2 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.

2.1.5.2.2.1 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 Mbyte 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.

2.1.5.2.2.2 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 CA, attests to it by signing Bob's public key. Bob's public key, signed by the CA, 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.

2.1.5.2.2.3 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 below.

2.1.5.2.2.4 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.

2.1.5.2.3 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.

Say 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 Bob is able to verify Alice's certificate using the CA certificate's public key

But this may of course be extended. Bob doesn't 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 don't 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 VSC3 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 VSC3 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 VSC3 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 VSC3 SCMS architecture, even if this migration happens slowly.

2.1.5.2.3.1 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.

2.1.5.2.3.2 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 – the public key only works if the CA was involved in creating it – rather than explicit 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 verifications take about the same time as each other. 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. Note: VIIC is currently directly engaged with lawyers of the company BlackBerry Ltd. in an attempt to develop an agreement that meets the requirements of the automobile manufacturing industry.

2.1.5.2.3.3 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.

2.1.5.2.3.3.1 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: the certificate is looked up, and it is identified 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.

2.1.5.2.3.3.2 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.

2.1.5.2.3.3.3 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: 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.

2.1.5.2.3.3.4 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.

2.1.5.3 Special Cryptographic Primitives in SCMS

This section describes crypto primitives that are used in multiple use cases. In the subsection Crypto Primitives affecting End-Entity, we point out the primitives that also affect EEs. In the following, for a = {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. In addition, unless otherwise noted, la_id1 and la_id2 are 16-bit identifiers of LA1 and LA2, respectively, and i, j, and k are 32-bit strings.

2.1.5.3.1 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.

2.1.5.3.2 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 1 minute, but there are safety concerns with such a small overlap period, so we are extending the overlap period to 1 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 needs to be addressed later.

2.1.5.3.3 Clock Time corresponding to i=0

For 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 Time on Tuesday, January 6, 2015** (i.e., 4023 days and 8 hours or **347,616,000 seconds** since 1609.2 epoch).

2.1.5.3.4 SCP1: Butterfly Keys

2.1.5.3.4.1 Summary

A core principle of PKI implementations is that, if possible, 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 VSC3 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 On-board Equipment (OBE) to the CA are unreliable, there is a risk that certificate requests would not complete successfully within a single communications session.

The CAMP VSC3 design proposed butterfly keys to address both these concerns. Butterfly Keys is a novel cryptographic construction that allows a device to request an arbitrary number of certificates, each with different signing keys and each encrypted with a different encryption key, using only one request that contains one verification public key seed, 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 (reduced to less than 1K bytes), allowing requests to be made when there is only spotty connectivity, and also reduce the computational work to be done by the requester to calculate the keys (it only has to generate two key pairs). The cost is that the download of certificate responses increases in size.

2.1.5.3.4.2 Background

To understand butterfly keys, it is necessary to explain some of the underlying mathematics. 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 (ECDLP) is the statement: Given P and Q = aP, but not a, it is very difficult to work out the value of a.

2.1.5.3.4.3 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 vehicle generates an integer, a, and a description of an expansion function, f(ι). The expansion function maps an integer ι to another

integer in a range from 0 to the maximum value of a, and does it in a way that is cryptographically secure (which roughly means that the output looks random so that given two values of {f(ι), ι}, a third party cannot tell whether the two values were generated by the same version of f(ι) or by different versions). The vehicle stores a and f(ι), and sends A = aG and the description of f(ι) to the SCMS.

In the CAMP VSC3 design, the specific choice of f(ι) was: f(ι) = AES_k(ι right-padded with 0s to 128bit length) || AES_k(ι XORed with a buffer of 16 0xff bytes), where XOR is a bitwise operation, AES_k(x) means "The AES encryption of x with k", and "||" means concatenation. This maps any integer of 128 bits or less to a random 256-bit integer. The "description" of f(ι) is simply the AES key k: to generate f(ι) the vehicle simply generates k, and to send the description of f(ι) the vehicle sends k.

Now the SCMS has the ability to generate an extremely large number of derived points: it can generate $B_ι$ = A + f(ι) * G, with A = aG. The corresponding private key will be $b_ι$ = a + f(ι).

Since the SCMS does not know the original value of a, it cannot know any of the $b_ι$ values, so it can generate an arbitrary number of public keys for which only the vehicle knows the private keys.

Additionally, because the expansion function is cryptographically secure, no one can tell whether two different public keys belong to the same series {$B_ι$} or to a different series without knowing f(ι). This means that the RA can safely use f(ι) 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.

2.1.5.3.4.4 Usage

In the CAMP SCMS PoC, this underlying approach is used as follows. Note: There are three minor technical differences - explained after this - between this description and the CAMP VSC3 approach, which focuses on the core butterfly key operations and omits optimizations that might obscure the explanation:

The vehicle generates two AES keys k_s and k_e, and two "caterpillar" key pairs: (a, A = aG) used for signing, and (h, H = hG) used for encryption

The vehicle sends {k_s, k_e, A, H} to the RA. Note: k_s will define the expansion function for the signing keys and k_e will define the expansion function for the encryption keys.

- The RA uses k_s, to generate {$B_ι$}, the series of "caterpillar" signing public keys for the certificate requests, and k_e to generate {$J_ι$}, the series of caterpillar encryption public keys for encrypting the certificate response, pairs each $B_ι$ with the corresponding $J_ι$, and sends the pairs {$B_ι$, $J_ι$} to the CA.
- The CA does not know which public keys have come from the same vehicle, but the RA knows which public keys are in the requests, so the CA must also change the public keys. For each request, the CA generates a unique random integer c and sets the public key in each certificate to the "butterfly" value to ($B_ι$ + cG).

The CA then uses J_ι to encrypt the response, which contains:

- The certificate based on the public key ($B_\iota + cG$).
- The CA's contribution to the private key, c.

The unencrypted part of the response contains ι, so that the vehicle will know which expanded keys the response corresponds to:

- The RA sends the encrypted message to the vehicle
- The vehicle takes the unencrypted value of ι from the response and uses it to calculate J_ι. It uses J_ι to decrypt the response and recover the certificate based on the public key ($B_\iota + cG$) and the CA's contribution to the private key, c. It then calculates b_ι. The private key for the certificate is then:
- Private key = b_ι (calculated using k_s) + c (provided by CA)

The vehicle 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 vehicle has obtained a set of certificates such that:

- Only the vehicle knows the private keys
- The RA does not know the public keys in the vehicle's certificates
- The CA cannot tell from the requests alone which requests have come from the same vehicle

2.1.5.3.4.5 Notes

- In the CAMP VSC3 design, there are three differences. First, implicit certificates are used, 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. Second, for reasons explained in Section 2.4.2, the series of values is generated with two indices (i, j) rather than a single index ι. Neither of those changes materially affects the principles explained above; in fact, ι is related to (i, j) in a very simple way, for example ι = (8 bytes of 0 || 4-byte representation of i || 4-byte representation of j). Third, 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. It then can decrypt the encrypted response by the CA, view the underlying certificate, and, while responding to the vehicle, encrypt the certificate with the right public key.

- Since the RA knows the public encryption key J_ι, it could create in principle 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.

- The per-certificate value *c* generated by the PCA is vital to keep the identity of 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 PCA 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. The value *c* must therefore be generated with good randomness (see Section 2.2.4 for a discussion).

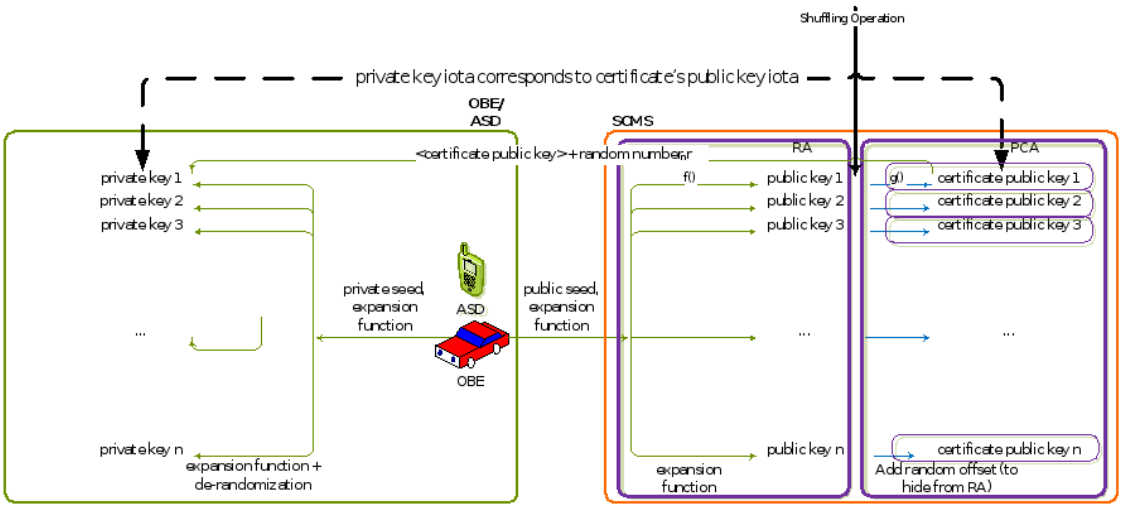


Figure 1: Butterfly Key Mechanism

2.1.5.3.4.6 Modifications

The butterfly expansion function defined in the CAMP VSC3 project and described above does not have the desired randomness properties. In particular, for NISTp256 curve, the outputs of this function has a bias of approximately 2^{-32}, which basically means that by looking at two requests from RA, PCA can tell with a non-negligible probability (close to 2^{-32}) whether the requests are for the same vehicle or different. The problem will get much worse if at some point we decide to switch to Brainpool curves, where the bias is quite high, approximately 1/4. For these reasons, we are modifying the butterfly expansion function as explained below, where the bias is expected to be extremely small (2^{-128}).

- The old butterfly expansion function as explained above can be summarized as:
  - Device picks two random 128-bit AES keys: ck and ek, for certificate keys and encryption keys, respectively, and sends them encrypted to RA.
  - Input x is derived from time period (i, j) as: (0^{64} || i || j).
  - Expansion function $f_k(x)$ with key k and input x: $f_k(x) = f_k^{int}(x) \bmod l$, where l is the order of the elliptic curve and $f_k^{int}(x) = AES_k(x) \,||\, AES_k(x')$ represented as a big-endian integer.
- The **new specification** for the butterfly expansion function:

- Device picks two random 128-bit AES keys: ck and ek, for certificate keys and encryption keys, respectively, and sends them encrypted to RA.
- Input x is derived from time period (i, j) as:
  - **Certificate keys: (0^{32} || i || j || 0^{32})**
  - **Encryption keys: (1^{32} || i || j || 0^{32})**

Note that for every vehicle, there are two sets of butterfly keys: one that go into certificates and the other that are used to encrypt the certificates. The new design with two separate derivations of x based on its usage is inspired in part by NIST SP 800-108.

- Expansion function $f_k(x)$ with key k and input x: $f_k(x) = f_k^{int}(x) \bmod l$, where l is the order of the elliptic curve and **$f_k^{int}(x) = (AES_k(x+1)$ XOR $(x+1))$ || $(AES_k(x+2)$ XOR $(x+2))$ || $(AES_k(x+3)$ XOR $(x+3))$** represented as a big-endian integer. The changes to $f_k^{int}(x)$ are inspired by the standard counter mode of encryption and AES in Davies-Meyer mode.

Note: Test vectors for Butterfly Expansion Function are available at http://stash.campllc.org/projects/SCMS/repos/crypto-test-vectors/browse/bfkeyexp.txt

2.1.5.3.5 SCP2: Linkage Values

2.1.5.3.5.1 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. Note: Group revocation is considered an option besides revocation of single devices. LVs and LAs are used to enable the SCMS to support seven requirements:

1. There should be an efficient way of revoking all the certificates within a device
2. There should be an efficient way of revoking all the certificates within a group of devices
3. Certificates should not be linkable by an eavesdropper unless the owner has been revoked
4. Membership to a group should not be disclosed unless that group has been revoked
5. If a vehicle's security credentials are revoked, the vehicle should be trackable going forward but its movements before it was revoked should not be trackable. Similarly, if a group of vehicles' security credentials is revoked, a device belonging to that group should be identifiable as a member. However, it should not be possible to determine the membership to a group before the group revocation took place.
6. No single entity within the system should be able to determine that two certificates belong to the same device or to the same group. An exception to this rule is the Misbehavior Authority (MA).

7. No single entity within the SCMS should be able to track a vehicle. Once a single LA is introduced, this requirement is not fulfilled any longer. For that reason, two LAs are introduced and the information, which allows for tracking is split between them.

2.1.5.3.5.2 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), 3), and 5). It does not attempt to address 2) and 4), which are relevant to the efficient revocation of groups, and it does not meet requirement 6), 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.

1. The LA starts with an initial linkage seed (ILS), ls(0). (This will be different for each vehicle.)
2. For each time period i > 0, the authority 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)
3. The certificate for each time period i contains the linkage value lv(i) = $AES_{ls(i)}(0)$
4. To revoke a vehicle from time period i onwards, the revocation authority publishes ls(i)
5. To check revocation at time period i' > i, the recipient of a signed message:
6. Hashes ls(i), and then hashes the output of the hash, repeated (i'-i) times to obtain ls(i')
7. Calculates lv(i') = $AES_{ls(i')}(0)$
8. 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 meets the requirements as follows:

1. 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.
2. 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 a secure block cipher, this is not possible.
3. 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 VSC3 SCMS uses two LAs, LA1 and LA2.

In the description above, there is a single chain of LSs and LVs. In the CAMP VSC3 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. Let us now describe the generation process in more detail.

1. LA1 starts with a random ILS, ls1(0)
2. LA2 starts with a random ILS, ls2(0)
3. For each time period i > 0:
4. LA1 sets its LS ls1(i) = H(ls1(i-1)), and LA2 sets its LS ls2(i) = H(ls2(i-1))
5. LA1 sets its PLV, defined as plv1(i) = $AES_{ls1(i)}(0)$ and LA2 sets its plv2(i) = $AES_{ls2(i)}(0)$
6. The CA sets the LV lv(i) = plv1(i) XOR plv2(i) and puts it in the certificate for time period i
7. To revoke a vehicle from time period i onwards, the revocation authority publishes the linkage seeds ls1(i) and ls2(i)
8. To check revocation at time period i' > i, the recipient of a signed message:
9. Iteratively hashes ls1(i) (i'-i) times to obtain ls1(i'); does the same for ls2(i)
10. Calculates PLVs plv1(i') = $AES_{ls1(i')}(0)$ and plv2(i') = $AES_{ls2(i')}(0)$
11. 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.

Three additional refinements in the CAMP VSC3 SCMS are identified here:

- 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 100 days, without this refinement, at key-on the vehicle will have to carry out 100 * 288 hashes for each revocation entry to bring its revocation information up to date (assuming that a vehicle is issued a certificate for every 5-minute period). With this refinement, the vehicle only has to perform one hash per day for each revocation entry. If revocation lists get large, this efficiency gain may be useful.

- To reduce the chance of collisions in the PLVs between two LAs, their identities are also employed during the computation of LSs and PLVs. Let la_id1, la_id2 be unique 16-bit identity strings associated with LA1, LA2, respectively, and for bit-strings x and y, let x || y denote their bit-wise concatenation. 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).

- To reduce the size of certificate revocation list (CRL), which contains the LSs of the revoked vehicles, the LSs are truncated to 16 bytes. For a complete description, see Section 4.2.3.

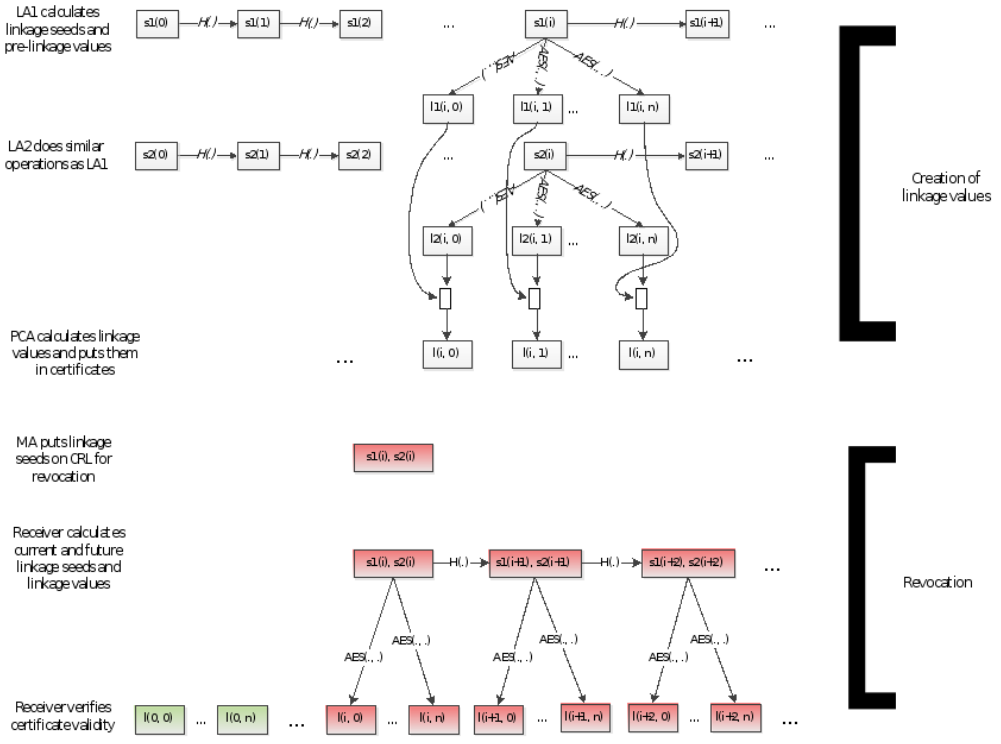


Figure 2: Creation of Individual Linkage Values and Revocation of Individual Device

2.1.5.3.5.3 Modifications

Using AES as a derivation function is not nice from security point of view as AES is a reversible function. Even though we currently do not see a clear attack, there is a possibility that someone can use this structure to attack the system. Instead, we will use a Davies-Meyer type construction, where the input is also XORed into the output of the block cipher. With this construction, being able to reverse the function is like finding a fixed-point in AES, which is presumed to be hard.

We use AES as a derivation function in the following.

1. In the old usage, as explained in above, linkage values are bit strings of size 9 bytes, computed as follows:
   Linkage value for time period (i, j): lv(i, j) = plv1(i, j) XOR plv2(i, j), where

   a. $plv1(i, j) = [AES_{ls1(i)}(la\_id1 \,||\, j \,||\, 0^{80})]_{72}$, where

i. ls1(i) = [SHA-256(la_id1 || ls1(i-1) || 0^{112})]$_{128}$, where

1. ls1(0) is a 128-bit string chosen at random for every device.

b. plv2(i, j) = [$AES_{ls2(i)}$(la_id2 || j || 0^{80})]$_{72}$, where

i. ls2(i) = [SHA-256(la_id2 || ls2(i-1) || 0^{112})]$_{128}$, where

1. ls2(0) is a 128-bit string chosen at random for every device.

2. In the new usage with AES in Davies-Meyer mode as a derivation function, linkage values are computed as follows:
Linkage value for time period (i, j): lv(i, j) = plv1(i, j) XOR plv2(i, j), where

a. plv1(i, j) = [($AES_{ls1(i)}$(la_id1 || j || 0^{80})) **XOR (la_id1 || j || 0^{80})**]$_{72}$, where

i. ls1(i) = [SHA-256(la_id1 || ls1(i-1) || 0^{112})]$_{128}$, where

1. ls1(0) is a 128-bit string chosen at random for every device.

b. plv2(i, j) = [($AES_{ls2(i)}$(la_id2 || j || 0^{80})) **XOR (la_id2 || j || 0^{80})**]$_{72}$, where

i. ls2(i) = [SHA-256(la_id2 || ls2(i-1) || 0^{112})]$_{128}$, where

1. ls2(0) is a 128-bit string chosen at random for every device.

Note: Test vectors for Linkage Values are available at
http://stash.campllc.org/projects/SCMS/repos/crypto-test-vectors/browse/lv.txt

2.1.6 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.

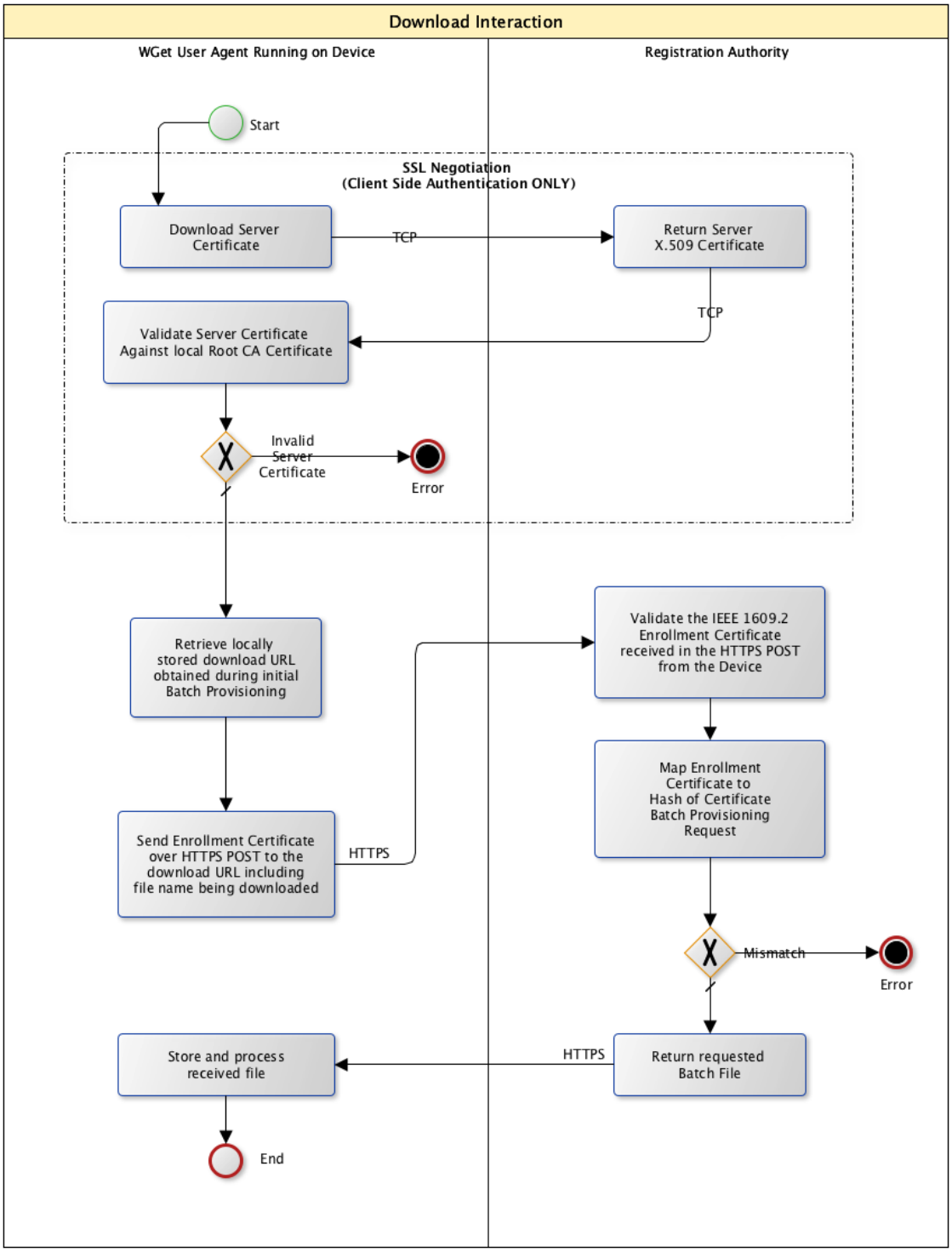
EE initiates all communication between EE and RA. All communications between EE and RA fall into one of two categories: 1) Download Requests 2) SCMS Protocol Messages

2.1.6.1 EE-RA Authentication and RA-EE Authentication

- EE establishes a secure server-authenticated TLS connection with RA (RA authenticates to EE).
- EE then digitally signs the current time of type IEEE 1609.2 Time32 with EE's enrollment certificate
- 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.
- RA validates the enrollment certificate against the internal blacklist, and then verifies the enrollment certificate.
- 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.

- 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.



2.1.6.2 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 though. 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.

2.1.6.3 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 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 named "Batch-Download-Req" is included in the HTTP GET message. The value of this header is Base64 encoded ASN1 serialized SignedAuthenticatedDownloadRequest APDU.
- 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.

2.1.6.4 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.

2.1.6.5 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 named 'Batch-Download-Req' with value equal to an ASN1 serialized Base64 encoded SignedAuthenticatedDownloadRequest request 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.

2.1.7 EE-SCMS Core Communication Requirements

2.1.7.1 Goals

- The goal of the EE-SCMS Core Communication Requirements section if to define all requirements that an EE must follow whenever establishing a connection to the SCMS.
- Specific Use Cases will refer to this page to indicate that the Core Requirements apply to the specific Use Case.
- 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.

2.1.7.2 Background and strategic fit

2.1.7.2.1 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.

2.1.7.2.2 TLS Connection

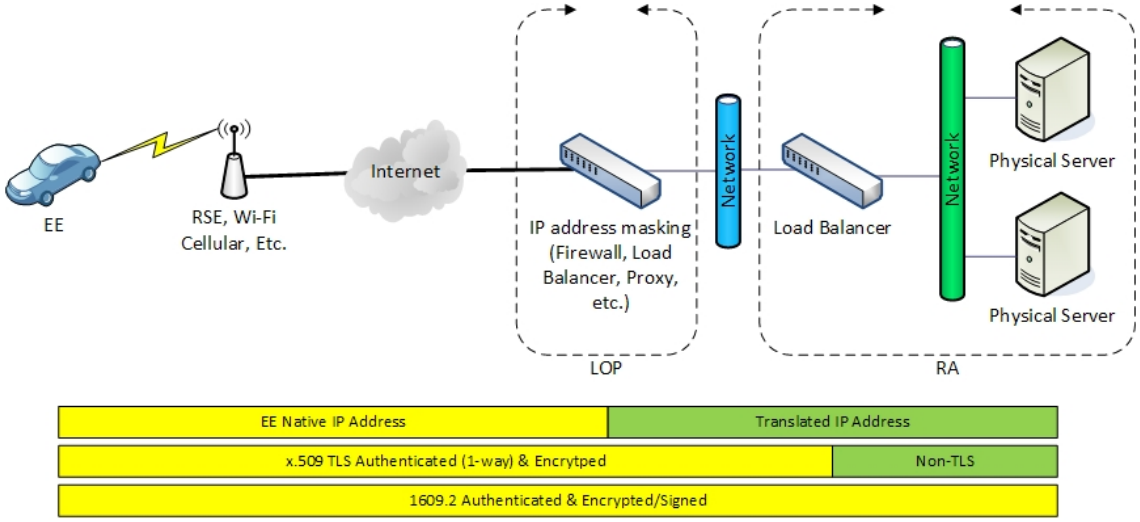
- Provide a means to verify the identity of the SCMS component by using x.509 1-way authentication.
- Encryption is an added privacy preserving enhancement but not a core requirement.

2.1.7.2.3 1609.2 Encrypting and/or Signing

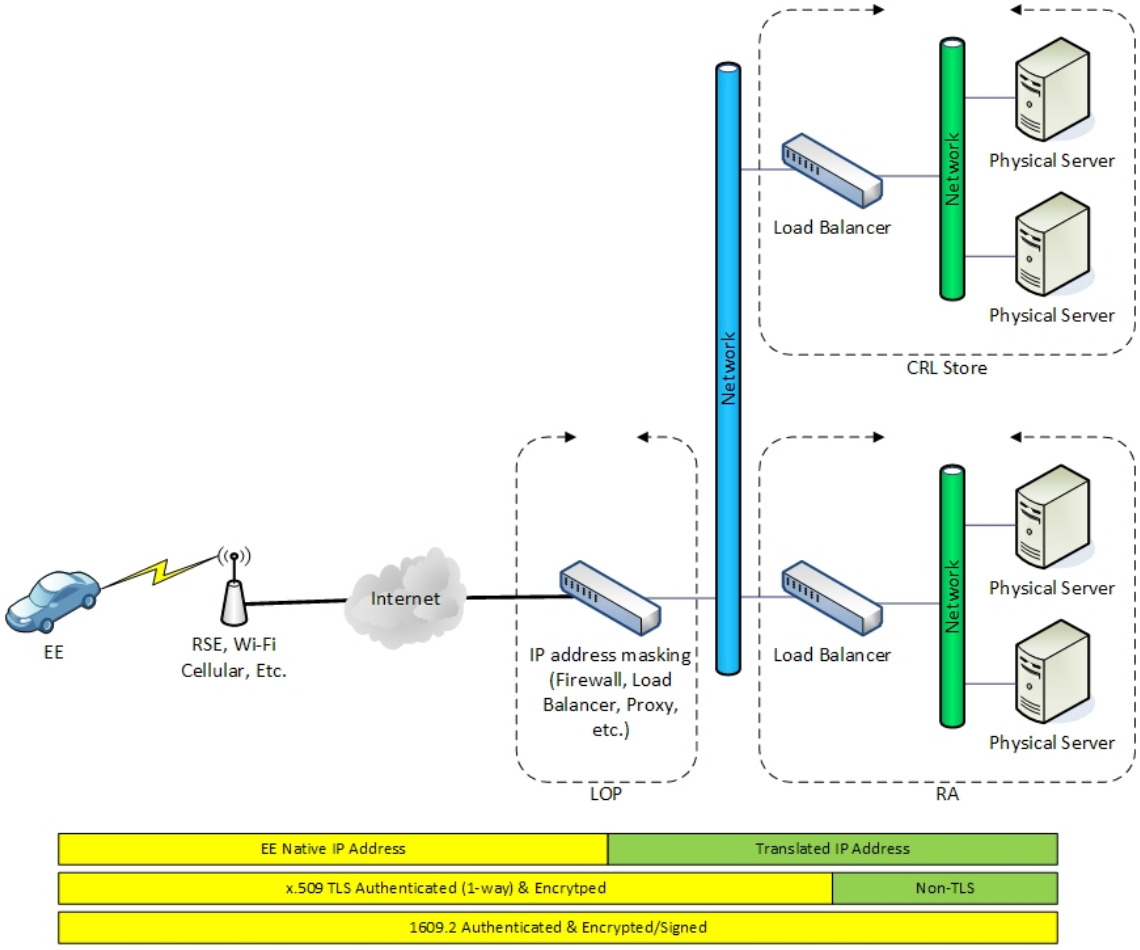
- Provides application layer security and privacy.

2.1.7.3 Diagrams of Communications Methods

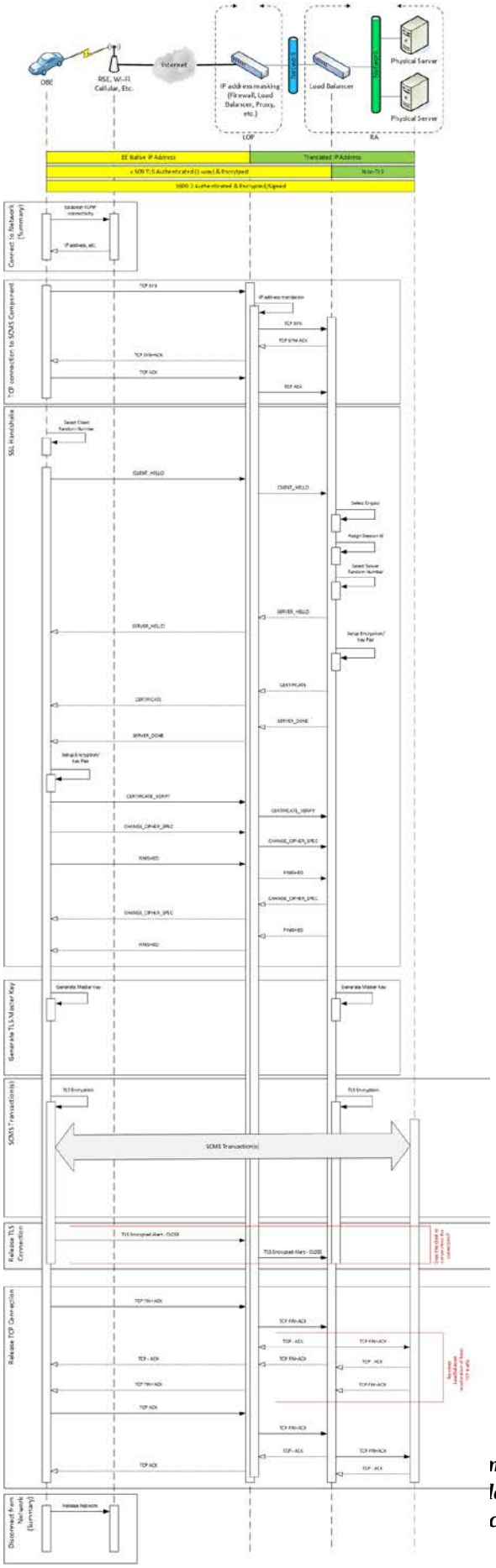
2.1.7.3.1 Overview of Methods



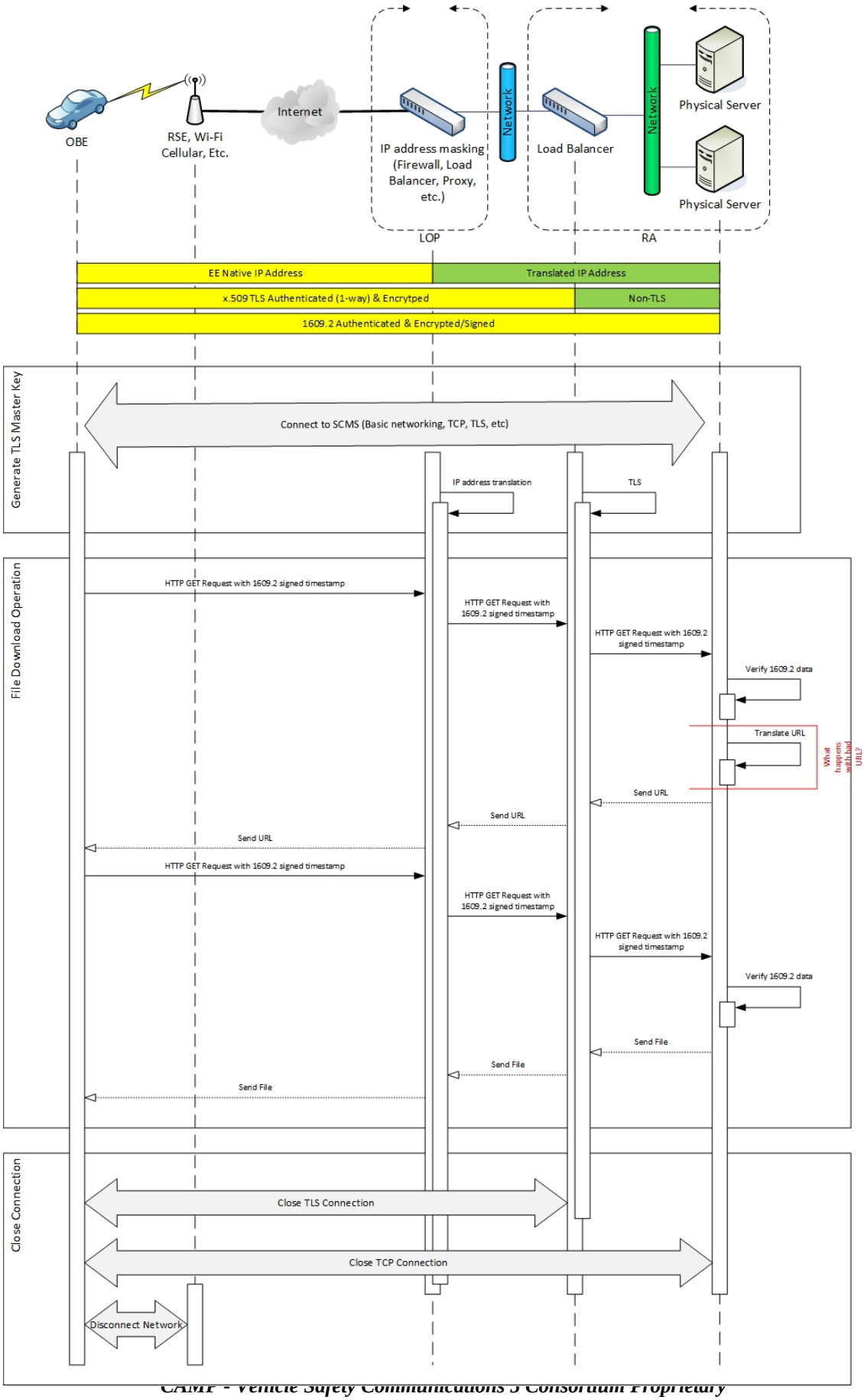
2.1.7.3.2 Overview of Multiple SCMS Components Served by Single LOP



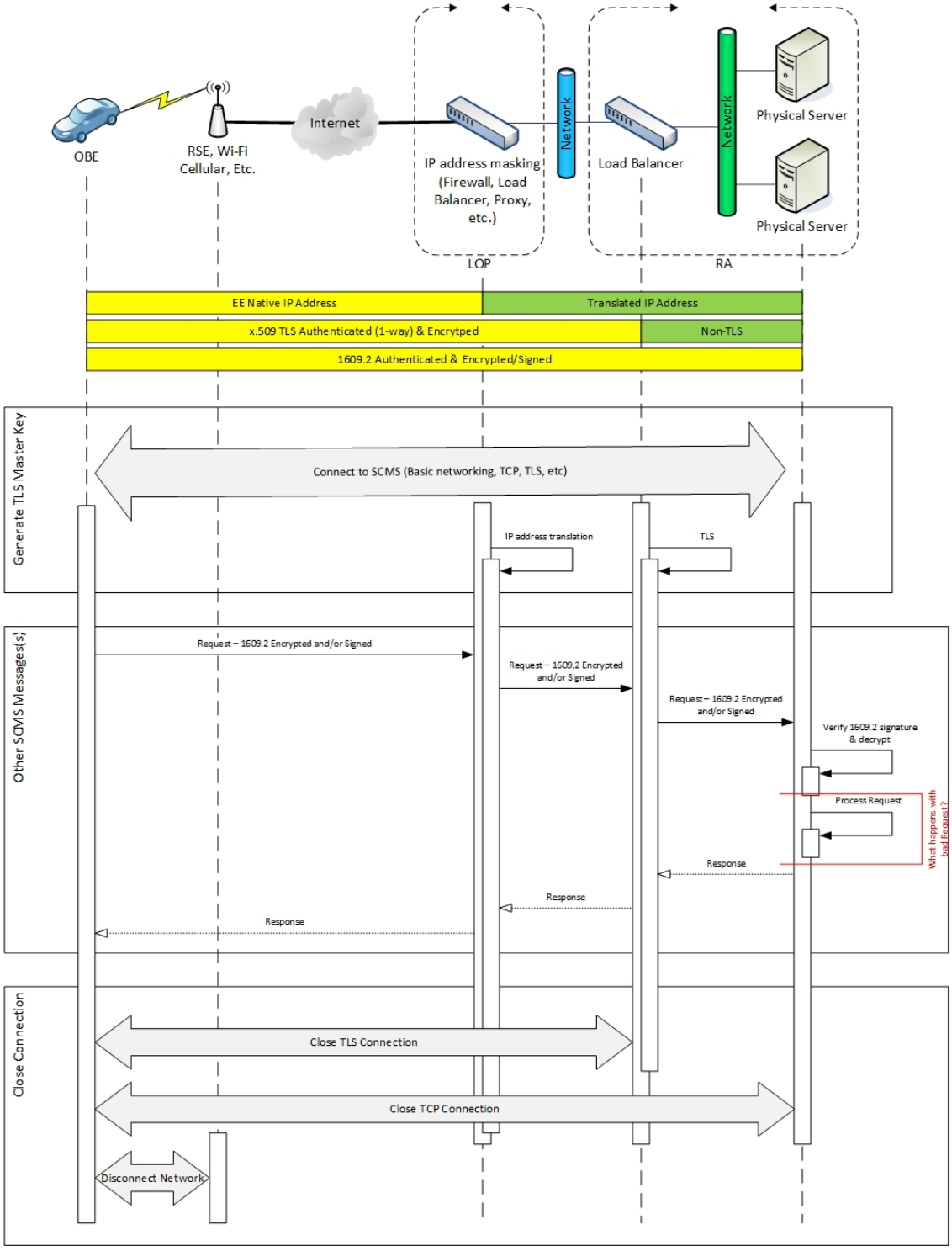
2.1.7.3.3 Universal SCMS Handshake Processes



2.1.7.3.4 Common Process for File Download Operations


OBE
RSE, Wi-Fi
Cellular, Etc.
Internet
IP address masking
(Firewall, Load
Balancer, Proxy,
etc.)
Network
Load Balancer
Network
Physical Server
Physical Server
LOP
RA
EE Native IP Address
Translated IP Address
x.509 TLS Authenticated (1-way) & Encrytped
Non-TLS
1609.2 Authenticated & Encrypted/Signed
Generate TLS Master Key
Connect to SCMS (Basic networking, TCP, TLS, etc)
IP address translation
TLS
File Download Operation
HTTP GET Request with 1609.2 signed timestamp
HTTP GET Request with 1609.2 signed timestamp
HTTP GET Request with 1609.2 signed timestamp
Verify 1609.2 data
Translate URL
What happens with bad URL?
Send URL
Send URL
Send URL
HTTP GET Request with 1609.2 signed timestamp
HTTP GET Request with 1609.2 signed timestamp
HTTP GET Request with 1609.2 signed timestamp
Verify 1609.2 data
Send File
Send File
Send File
Close Connection
Close TLS Connection
Close TCP Connection
Disconnect Network

2.1.7.3.5 Common Process for Sending SCMS Messages



2.1.7.4 Existing JIRA issues with "EE-Handshake" label

Key	Summary	Description	justification	notes	Component/s
SCMS-411	EE Authentication to RA for Request	The EE shall authenticate its requests with its enrollment certificate. These messages shall include a timestamp (which the EE will obtain from its GPS reference) 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.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-416	LOP	All communications from the OBE to the SCMS components (except DCM) shall pass through the LOP	The OBEs location must be obscured.		LOP
SCMS-515	RA requires EE authentication	The RA shall require EE authentication before any other communication process starts.	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	RA

Key	Summary	Description	justification	notes	Component/s
				details of the authentication process are defined E-RA Communications - General Guidance	
SCMS-522	Retry request	If the EE does not receive acknowledgement (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, it shall retry.	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	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	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	On-board Equipment (OBE), RA, Road-side Equipment (RSE)

Key	Summary	Description	justification	notes	Component/s
				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	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 E-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	OCSP stapling - EE	The EE shall use the TLS Certificate Status Request extension (OCSP stapling) to verify	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	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Summary	Description	justification	notes	Component/s
		RA revocation status.		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-958	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-977	TLS error codes	RA shall return standard TLS error codes if TLS errors occur.	in order to enable client side error handling.		RA
SCMS-979	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-1090	Error code: raTcpErrors	RA shall return standard TCP error codes if TCP errors	in order to enable client		RA

Key	Summary	Description	justification	notes	Component/s
		occur and log "Error code: raTcpErrors" and the encountered TCP error.	side error handling.		
SCMS-1201	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-1208	EE securely stores X.509 root certificate	EE shall store the X.509 root certificate in tamper-evident 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-1270	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-1377	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	Error reporting to EE	SCMS Components shall return error code "HTTP 500" to EEs in response to	Specific error codes should be hidden from EEs to prevent useful	• Standard TCP (SCMS-1090) and TLS	CRL Store, RA

Key	Summary	Description	justification	notes	Component/s
		all application level errors.	information from being provided to malicious actors	(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 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	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

2.1.7.5 Existing JIRA issues with OBE or RSE component

Key	Summary	Description	justification	notes
SCMS-335	EE issues a CRL Request	An EE shall issues a HTTP get to the CRL Store to obtain the latest CRL.	EE needs to be provided with current CRL so that the EE can be informed of revoked components.	This is out of scope since it defines EE's behavior.
SCMS-341	EE TLS Cipher Suite	The EE shall at minimum support SSL cipher suite TLS_ECDHE_ECDSA_WITH_AES_128_CCM	This is the requirement for the SSL transport tunnel.	Defined in Study 3 document in section 3.4.3.6 - Certificate Batch Download This is out of scope

Key	Summary	Description	justification	notes
		(as defined in RFC7251) for all communications to SCMS components.		as it defines EE behavior.
SCMS-342	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 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-358	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.
SCMS-411	EE Authentication to RA for Request	The EE shall authenticate its requests with its enrollment certificate. These messages shall include a timestamp (which the EE will	Messages from EEs to an RA must be secure against replay attacks. The signed time stamp from the EE enables the RA to	This is out of scope since it defines EE's behavior.

Key	Summary	Description	justification	notes
		obtain from its GPS reference) to avoid replay attacks on the RA.	validate the freshness of EE requests.	
SCMS-520	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.
SCMS-522	Retry request	If the EE does not receive acknowledgement (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, it shall retry.	to ensure that the request is received by the RA.	This is out of scope as it defines EE behavior.
SCMS-523	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.
SCMS-524	RA certificate	EE shall dynamically acquire RA's SCMS certificate each time it communicates with RA.	so that EE can encrypt the request to the right RA	More information is available at RA - Retrieve Registration Authority Certificate. This is out of scope as it defines EE behavior.
SCMS-537	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 attacker eavesdrops all individually

Key	Summary	Description	justification	notes
			adversary is able to read PCA-encrypted pseudonym certificates.	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	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 E-RA Communications - General Guidance	This is out of scope since it defines EE's behavior.
SCMS-541	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

Key	Summary	Description	justification	notes
				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-557	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 the wiki page on Secure Environment for Device Enrollment for guidelines on physical security for device provisioning. Not software testable, procedural
SCMS-560	Certified Software	EEs shall ensure that during bootstrapping process only certified software is provisioned.	Improper software installation will compromise security of the EEs.	See the wiki page on Secure Environment for Device Enrollment for guidelines on physical security for device provisioning. Not software testable for POC, procedural
SCMS-583	Butterfly keys	The EE shall generate new butterfly keys/expansion functions for the new RA.	Protect privacy of data during transfer by not extracting the keys. This is an optional step at the discretion of the authorized EE operator. See Section Use Case 3.6: Update Pseudonym Certificate Request Parameters for details	

Key	Summary	Description	justification	notes
SCMS-684	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.
SCMS-709	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's behavior.
SCMS-754	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.
SCMS-776	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.
SCMS-864	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.
SCMS-865	EEs obtaining new Enrollment Certificates	EEs shall obtain new Enrollment Certificates from their ECAs, if the Root CA was revoked.	EEs need to obtain new enrollment certificates valid in	The OEMs should keep a record of all Enrollment Certificates issued,

Key	Summary	Description	justification	notes
	upon Root CA revocation	Refreshed Enrollment Certs are encrypted to the old Enrollment Certificate.	the new PKI hierarchy.	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 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	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.
SCMS-949	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.
SCMS-950	Error code: eeInitCRLProvError	EE shall log this error code, if the Initialization process fails at	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.

Key	Summary	Description	justification	notes
		completing the CRL provisioning.		
SCMS-952	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.
SCMS-953	Misbehavior report: eePolicyFileDownloadFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to download the local policy file (e.g. because there is none or it is corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.
SCMS-954	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.
SCMS-955	Misbehavior report: eePolicyVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify the digital signature of the local policy file.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.
SCMS-956	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	This is out of scope since it defines EE's behavior.

Key	Summary	Description	justification	notes
			whenever the EE is not able to read the latest version of that file.	
SCMS-957	Misbehavior report: eePolicyFileParsingFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to parse the successfully downloaded local policy file (e.g. because it is corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.
SCMS-958	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.
SCMS-965	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.
SCMS-966	Misbehavior report: eeCertFileDownloadFailed	EE shall initiate a misbehavior report to MA, if EE is not able to download certificate files (e.g. because there is none or it is corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.
SCMS-967	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's behavior. This is for a single-issue certificate that has been encrypted and digitally signed by PCA.

Key	Summary	Description	justification	notes
SCMS-968	Misbehavior report: eeCertFileVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify the digital signature of an encrypted certificate.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.
SCMS-969	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.
SCMS-970	Misbehavior report: eeCertFileDecryptionFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to decrypt an encrypted certificate.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.
SCMS-971	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.
SCMS-972	Misbehavior report: eeCertVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify a certificate.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.
SCMS-973	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.
SCMS-974	Misbehavior report: eeCertContentFalse	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to parse a certificate, or if the certificate has wrong content.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.
SCMS-979	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

Key	Summary	Description	justification	notes
				defines EE error handling.
SCMS-980	Misbehavior report: eeAuthenticationFailed	EE shall initiate a misbehavior report to MA with the observed error, if RA-to-EE authentication fails.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.
SCMS-984	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's behavior.
SCMS-985	Misbehavior report: eeInfoFileDownloadFailed	OBE shall initiate a misbehavior report to MA with the observed error, if OBE is not able to download the .info file (e.g. because there is none or it is corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.
SCMS-991	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.
SCMS-994	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.
SCMS-995	Error code: eeCRLVerificationFailed	EE shall log "Error code: eeCRLVerificationFailed", if verification of the CRL signature fails.	In order to enable client side error handling and misbehavior reporting.	This is out of scope since it defines EE's behavior. Might be added with MA integration as potential misbehavior.
SCMS-1013	Error code: eeEncryptionFailed	EE shall log this error code, if EE encounters an error when	to enable EE side diagnostics.	This is out of scope since it defines EE's behavior.

Key	Summary	Description	justification	notes
		encrypting a misbehavior report with MA's public key.		
SCMS-1055	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 "Add Root CA" 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 Root CA	This is out of scope as it defines EE behavior.
SCMS-1076	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.
SCMS-1095	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.	
SCMS-1159	EE securely stores Elector certificates	EE shall store the Elector certificates in tamper-evident storage.	The Elector 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 be updated when the proper Root Management authentication mechanisms have been satisfied.	This is out of scope since it defines EE's behavior.

Key	Summary	Description	justification	notes
SCMS-1160	EE securely stores Root CA certificates	EE shall store all Root CA certificates in tamper-evident 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 be updated when the proper Root (Elector) Management authentication mechanisms have been satisfied.	This is out of scope since it defines EE's behavior.
SCMS-1161	Submit certificate request	OBE shall submit a certificate request with change request parameters as defined in Step 3.2: Request for Pseudonym Certificates, whenever it is assigned to a new RA or request parameters changed due to policy change.	so that RA can correctly process the request	Out of scope for SCMS POC as it is an EE requirement.
SCMS-1163	OBE revoked	A revoked OBE shall not attempt to download pseudonym certificate batches/OBE identification certificate files.	To reduce resource usage, since RA will reject request anyways.	This is out of scope since it defines EE's behavior.
SCMS-1164	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	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

Key	Summary	Description	justification	notes
			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).	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 or next time period, the OBE is allowed to make a download attempt at any time.
SCMS-1167	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.
SCMS-1168	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 out of scope since it defines EE's behavior.

Key	Summary	Description	justification	notes
			This is to prevent repeated downloads of the same content.	
SCMS-1170	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
SCMS-1171	EE revoked	EE shall not attempt to download a policy file, if it is revoked.	to avoid unnecessary load at the RA.	This is out of scope since it defines EE's behavior.
SCMS-1174	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.
SCMS-1176	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.
SCMS-1189	Trust Chain Broken - EE	EE shall not attempt to request or download pseudonym certificate batches, OBE identification certificate files, or RSE application certificate files, 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 anyways.	This is out of scope since it defines EE's behavior.
SCMS-1190	RA URL Update	EE shall be able to update RA's URL.	Authorized operators of EEs must have the ability to update the stored RA URL on the device. This is a	

Key	Summary	Description	justification	notes
			device specific method and not a defined SCMS protocol.	
SCMS-1191	TLS Root Update	EE shall be able to receive and store an updated TLS (x.509) Root Certificate.	Authorized operators of EEs must have the ability to update the stored TLS (x.509) Root Certificates stored on the device. This is a device specific method and not a defined SCMS protocol.	
SCMS-1192	Secure Update	All update methods used shall conform to established SCMS security policies.	EE updates shall comply with SCMS Manager policies.	
SCMS-1201	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.
SCMS-1207	EE stores Certificate Revocation List	EE shall store the Certificate Revocation List in tamper-evident 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.
SCMS-1208	EE securely stores X.509 root certificate	EE shall store the X.509 root certificate in tamper-evident 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.
SCMS-1209	EE securely stores Local Certificate Chain File	EE shall store the Local Certificate Chain File in tamper-evident storage.	EE will use Local Certificate Chain File during verification of SCMS certificates	This is out of scope since it defines EE's behavior.

Key	Summary	Description	justification	notes
SCMS-1210	EE Secure Key Storing	EE shall store the following keys in tamper-evident 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
SCMS-1214	OBE downloads .info file	OBE shall download the .info file each time OBE tries to download 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.
SCMS-1215	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 not waste resources by trying to download certificates before they are available.	This is out of scope since it defines EE's 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).
SCMS-1217	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	This is out of scope since it defines OBE's behavior.

Key	Summary	Description	justification	notes
			pseudonym certificate against the revoked linkage value list.	
SCMS-1219	OBE updates linkage value list	OBE shall update the list of revoked linkage values for each i-period. OBE shall either update the linkage value or remove the linkage value.	OBE is able to update the linkage values for each i-period. It is left to the OEM/supplier, when the values are updated. The updated values are needed when a new i-period starts.	Linkage values are updated by hashing the linkage seed value (which is 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	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.
SCMS-1221	EE processes CRL	EE shall process the updated CRL/CRL chunk and update it’s 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.
SCMS-1222	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 is also conform with requirement https://jira.campllc.org/browse/SCMS-1220~~SCMS-1220~~.	This is out of scope since it defines EE's behavior.

Key	Summary	Description	justification	notes
SCMS-1223	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, and comparing it against a CRL entry. Clause 7 contains comprehensive information about CRLs.

Key	Summary	Description	justification	notes
				This is out of scope since it defines EE's behavior.
SCMS-1224	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.
SCMS-1226	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.	
SCMS-1227	EE Timely Limited Configuration Options: POC	For POC, EE shall support the parsing of a timely limited configuration option policy file.	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 is more than one choice, EE will only consider the first choice and assume that this first choice is always valid.
SCMS-1263	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.	
SCMS-1270	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.

Key	Summary	Description	justification	notes
SCMS-1279	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.
SCMS-1280	Error code: eeCertificateNotReadable	EE shall log this error if any certificate is not readable.	To enable error reaction and investigation.	
SCMS-1282	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.
SCMS-1285	EE stops sending: revoked ECA for EE's enrollment certificate	EE shall stop sending over-the-air messages, if it detects (via CRL) that is 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.
SCMS-1286	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.
SCMS-1289	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 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	Expired Certificate Files	The OBE shall only download OBE identification certificate	Only download certificates that are not expired yet.	

Key	Summary	Description	justification	notes
		files for the current and future time periods.		
SCMS-1303	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.
SCMS-1308	OBE sign misbehavior reports	OBE shall sign a misbehavior report with a currently valid (at time of event observation) pseudonym certificate.	To avoid forged misbehavior reports	This is out of scope since it defines EE's behavior.
SCMS-1309	RSE sign misbehavior report	RSE shall sign misbehavior reports with RSE application certificate	To avoid forged misbehavior reports	RSE digitally signs misbehavior reports with an RSE application certificate intended for signing misbehavior reports (i.e., with a determined PSID for such purpose). This is out of scope since it defines EE's behavior.
SCMS-1353	EE request LCCF from RA	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
SCMS-1356	EE uses internal certificate store	EE shall use its internal certificate store to validate received SCMS certificates and respond	EEs need to be able to validate received SCMS certificates based on their certificate chain up to	EE does not need to store all certificate chains, the LCCF provides the minimum set and

Key	Summary	Description	justification	notes
		to P2P certificate requests.	the SCMS Root CA. EEs need to respond to P2P certificate requests to enable receiving EEs to validate the certificate chain.	EEs can learn additional chains via P2P certificate request. This is out of scope as it defines EEs behavior
SCMS-1384	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.
SCMS-1404	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.
SCMS-1410	Misbehavior report: crlgCRLGenerationFailed	The SCMS component shall submit a misbehavior report if there is no CRL available or the current CRL is expired.	Return error & log failure of CRLG	
SCMS-1417	EE download .info file if current file indicates suspended pre-generation	EE shall try to download an updated .info file, if the current .info file contains a timestamp '0', and then EE shall re-try to download pseudonym/OBE identification certificates after the time indicated in the updated .info file.	as a timestamp '0' indicates that RA has suspended pre-generation. After RA suspended pre-generation, RA first needs to start generation of pseudonym/OBE identification certificates. Hence, RA will first update	The process is as follows: 1.) EE tries to download certificates but the folder is empty. 2.) RA recognizes the download attempt, and changes EE's status to 'active'. 3.) RA now

Key	Summary	Description	justification	notes
			the .info file, and then provide certificates at the determined time.	includes EE in the regular pseudo certificate automatic generation process. 4.) RA immediately updates the information in .info to reflect the estimated time of availability. 5.) EE tries to download again, reads the information in .info, and now knows when to download.
SCMS-1421	LCCF validation in EE	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
SCMS-1512	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

Key	Summary	Description	justification	notes
				encryption keys and response encryption keys.
SCMS-1583	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.
SCMS-1587	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, or • in trusting certificate chains chaining to that component's certificate, or • in trusting messages signed using this component's certificate • in sending messages signed with certificates that chain up to this component's certificate See Assumption 1 in Revoke Root CA (Use Case) for a

Key	Summary	Description	justification	notes
				discussion of various scenarios, particularly applicable to ICA and ECA revocation. This is out of scope as it defines EE behavior.
SCMS-1589	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.	
SCMS-1593	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.	
SCMS-1606	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	

Key	Summary	Description	justification	notes
			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	
SCMS-1607	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 chronologically earlier then the stored ValidityPeriod.start value of the previously received valid CRLG Certificate.	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 certificate 3) The CRL Store makes the new valid CRL available for download 4) The attacker	

Key	Summary	Description	justification	notes
			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-1608	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, or • in trusting certificate chains chaining to that component's certificate, or • in trusting messages signed using this component's certificate, or • in sending messages signed with certificates that

Key	Summary	Description	justification	notes
				chain up to this component's certificate See Assumption 1 in Revoke Root CA (Use Case) for a discussion of various scenarios, particularly applicable to ICA and ECA revocation. This is out of scope as it defines EE behavior.
SCMS-1625	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 an specific RA)	as EE needs to know when and where it can go to download certificates.	

<table>
<tr><th>Key</th><th>Summary</th><th>Description</th><th>justification</th><th>notes</th></tr>
<tr><td></td><td></td><td>Case: Certificate Provisioning Request Reject
HTTP 500 error code</td><td></td><td></td></tr>
<tr><td>SCMS-1632</td><td>EE parse LCCF</td><td>EE shall parse the local certificate chain file (LCCF) and adjust its store of trusted certificate chains accordingly.</td><td>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.</td><td>This is out of scope as it defines EE behavior.</td></tr>
<tr><td>SCMS-1639</td><td>Download certificate batches</td><td>OBE shall not attempt to download certificate batches for i-value periods more than max_available_cert_supply in the future</td><td>To reduce resource usage by not attempting to download certificate batches that do not exist.</td><td>This is out of scope as it defines EE behavior.
This is the OBE counterpart of https://jira.campllc.org/browse/SCMS-547~~SCMS-547~~</td></tr>
<tr><td>SCMS-1685</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></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></tr>
</table>

Key	Summary	Description		justification	notes
		overdue_CRL_tolerance	2 weeks		
		(OBE only) i_period	1 week		
		(OBE only) min_certs_per_i_period	20		
		(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		
SCMS-1727	EE to verify RA FQDN matches the RA SCMS certificate ID	EEs shall verify that FQDN specified in the "id" field of the RA's SCMS certificate matches the FQDN used to contact the RA.		SCMS components (server) are only reachable by standard TCP/IP networking methods.	This is out of scope since it defines EE's behavior.

2.1.8 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 in particular 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 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 is 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. 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, 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. Other forms of re-enrollment might be added at a later point. The SCMS will not support re-issuance.

2.2 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 (not part of this documentation, because it is purely about backend operations),
- Step 3.3: Initial Download of Pseudonym Certificates,
- Step 3.4: Schedule Generation of Subsequent Batch of Pseudonym Certificates (not part of this documentation, because it is purely about backend operations), and
- 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.

2.2.1 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 e.g. 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
- Use Case 3: OBE Pseudonym Certificates Provisioning

- Use Case 8: OBE Pseudonym Certificate Revocation
- Use Case 19: OBE Identification Certificate Provisioning

2.2.2 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 e.g. 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
- Use Case 13: RSE Application Certificate Provisioning
- Use Case 16: RSE Application and OBE Identification Certificate Revocation

2.2.3 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

2.2.4 Requirements to be updated / added with next revisions

- CRL Generator / CRL format (with MA integration and Collaborative Distribution projects)
- Re-enrollment of EEs (to support the root management strategy for disaster recovery)
- DNS information for CV pilot SCMS server that are relevant to EEs

2.2.5 Document header and status

All use cases and use case steps have their own header to list authors, reviewers etc. All requirements are listed with all details including their status of implementation (e.g. SCMS-500-Firewall whitelist - Tests failed) and a JIRA link is given for traceability reasons. **There is no additional information essential to EE developers given at the links**. Statuses given are:

- "Review" translates to the requirement is currently under review by the Software Team
- "In Implementation" translates to the requirement is currently in implementation by the Software Team
- "Implemented" translates to the Software Team finished the implementation as well as unit tests
- "Ready for Testing" translates to the 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" translates to all tests of the given requirement were successful within the latest test run
- "Tests failed" translates to one or more tests of the given requirement failed during the latest test run
- "Closed" translates to the requirement is implemented and successfully tested.

- "Manual Process" translates to the requirement is meant to be executed within the PoC software in a manual way and will not be implemented in software
- "SCMS PoC Out Of Scope" translates to this 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.

2.2.6 Use Case 2: OBE Bootstrapping

2.2.6.1 Goals

Bootstrapping encompasses two distinct activities: initialization and enrollment. Initialization is the process by which an OBE receives keys that allow it to trust other SCMS components and credentials to connect to them. Enrollment is the process by which an OBE receives a SCMS long-term certificate, which it can use in interactions with the SCMS.

2.2.6.2 Background and strategic fit

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

- Credentials and information that allow it to communicate with the SCMS:
  - A correctly issued enrollment certificate and the corresponding private key, to allow it to authenticate its pseudonym certificate batch request.
  - The RA certificate and contact information for the RA, to encrypt and know where to route the pseudonym certificate batch request.
- Certificates and information that allow it to send and receive messages securely:
  - The required Root CA certificate(s), optional Intermediate CA and Pseudonym CA certificates to allow it to verify received V2X messages. The OBE can learn unknown PCA and ICA certificates in ongoing operation as defined in IEEE 1609.2.
  - CRL Generator certificates (optional), to allow it to trust received CRLs.
  - Contact information for the CRL store, to allow it to download CRLs.
  - The MA certificate and contact information for the MA, to allow it to submit misbehavior reports.

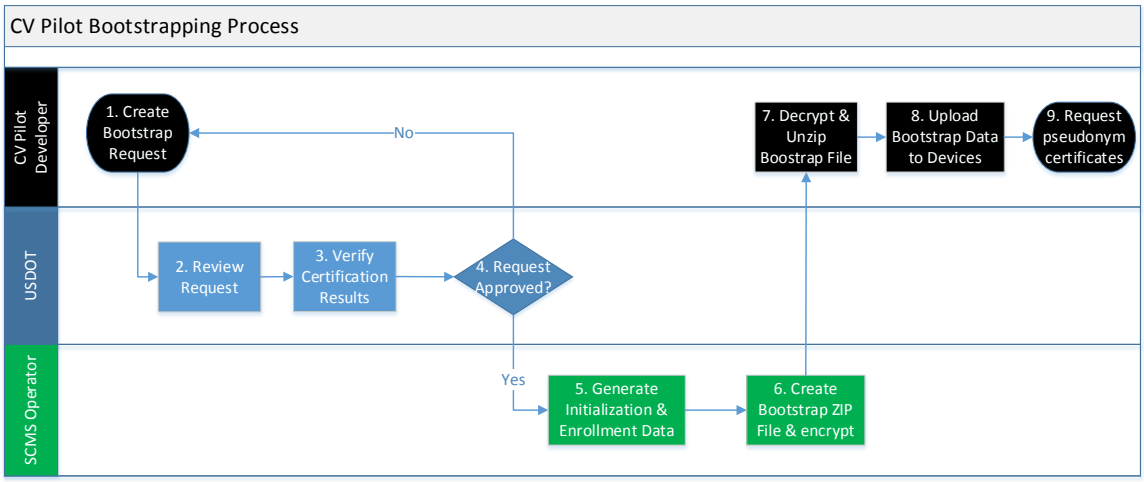
Bootstrapping must protect the OBE from getting incorrect information and the ECA from issuing a certificate to an unauthorized OBE. Any bootstrapping process is acceptable that results in this information being established securely.

There are multiple methods to provision OBEs with enrollment certificates, with these two being most likely:

1. Certificate Request/Response method: The OBE is initialized with firmware, Root CA certificate(s) and essential network information in a secure environment as defined in Secure Environment for Device Enrollment. The OBE subsequently connects to the DCM through a secure channel, performs an Enrollment certificate request, and receives an Enrollment certificate response through the DCM.

2. Certificate Injection method: The OBE enrollment public/private key pair is generated in a secure environment outside of the OBE (for example in the DCM). The DCM then performs an Enrollment certificate request to the ECA and receives an Enrollment certificate on behalf of the OBE. Subsequently, the OBE is initialized with firmware, Root CA certificate(s), essential network information, the enrollment public/private key pair and the Enrollment certificate through secure key injection, as described in Secure Environment for Device Enrollment.

As there are currently no processes, procedures or policies defined that avoids an ECA to issue certificates to unauthorized EEs, the decision is that there will be no automated bootstrapping process for CV pilots, but instead a manual process as shown in the following process flow. Later versions of the SCMS will implement an automated process.



2.2.6.3 Assumptions

- All required certificates are provided upfront to the In-production DCM.
- A "secure environment" as defined in Secure Environment for Device Enrollment ensures that the entirety of the connection between the DCM and the device is under the control of the operator running the bootstrap operation.
- At the start of bootstrap, a device has no certificates and no knowledge of how to contact the SCMS.

2.2.6.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-556	SCMS PoC out of Scope	Secure process	DCM shall use a secure operational process to inject EE firmware, enrollment certificates etc.	Physical and operational security involving EEs is crucial to their security.	See the wiki page on Secure Environment for Device Enrollment for guidelines on physical security for device	DCM

Key	Status	Summary	Description	justification	notes	Component/s
			as defined by the SCMS Manager.		provisioning. Does not apply to POC.	
SCMS-557	SCMS PoC out of Scope	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 the wiki page on 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)
SCMS-559	Manual Process	Certified Devices	DCM shall ensure that only certified EEs are provisioned.	Rogue devices will compromise the security of the EE, and could spread insecurity further than a single device.	See the wiki page on Secure Environment for Device Enrollment for guidelines on physical security for device provisioning. Not software testable for POC, procedural	DCM
SCMS-560	SCMS PoC out of Scope	Certified Software	EEs shall ensure that during bootstrapping process only certified software is provisioned.	Improper software installation will compromise security of the EEs.	See the wiki page on Secure Environment for Device Enrollment for guidelines on physical security for device provisioning. Not software testable for POC, procedural	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1270	SCMS PoC out of Scope	Network connection	EEs shall use TCP/IP to communicate	SCMS components (server) are only reachable by	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side

Key	Status	Summary	Description	justification	notes	Component/s
			with the SCMS.	standard TCP/IP networking methods.		Equipment (RSE)

2.2.6.5 Step 2.1: OBE Initialization

Target release	Release 0.1
Document owner	Biswajit Panja, Virendra Kumar
Reviewer	Benedikt Brecht, Virendra Kumar

2.2.6.5.1 Goals

Initialization is the process by which an OBE receives keys that allow it to trust SCMS components and credentials to connect to them. Therefore the overall goal of the initialization process is:

- Provisioning of SCMS component certificates
- Configuration, e.g. URL for RA, ECA, and MA services
- Current CRL
- Current Local Policy File
- Current Local Certificate Chain File

2.2.6.5.2 Background and strategic fit

(Note: This step-by-step process is also listed in J2945/1 sec. 6.6.1.)

The use case Initialization involves the following components:

- Actively involved:
  - The DCM
  - OBE
- Provide information to the DCM beforehand:
  - URLs for RA, ECA, and CRL store services
  - Local Certificate Chain File (containing Root and Elector "Add messages")
  - Local Policy File

Overview:

The DCM gathers the following current certificates:

- All Electors
- All Root CAs
- The Intermediate CAs and Pseudonym CAs that may issue certificates that the OBE will use to trust received application messages. These certificates can be communicated to the OBE via peer-to-peer protocol as defined in J2945/1 and IEEE 1609.2 or via the Local Certificate Chain File
- The MA
- Policy Generator

- Any CRL Generators that may issue CRLs that the OBE will need to process. These certificates can be communicated to the OBE as part of the CRL itself.

The DCM installs these certificates on the OBE using the Local Certificate Chain File. The Elector and the Root CA certificates have to be installed in a secure environment for the SCMS PoC implementation. Given sufficient Elector votes, the Root CA certificate could also be validated. All other certificates can be installed in a non-secure environment as the OBE now has the certificate of the Root CA to validate whether these certificates are genuine.

The Local Certificate Chain File details are documented in Step 18.5: Generate Global and Local Certificate Chain File.

2.2.6.5.3 Assumptions

- It is assumed that the process takes place in a secure environment as recommended in Secure Environment for Device Enrollment.
- The DCM is only accessible from a secure environment and sets up a secure connection to the SCMS.
- The DCM will be configured with the set of Elector, Root CAs, ICAs, PCAs, ECA and MA certificates to be used for any given OBE.

2.2.6.5.4 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

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-486	Manual Process	DCM shall acquire the current CRL	The In-production 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 In-production DCM will request these from the CRL Store and will provide these to the EE.	DCM
SCMS-562	Tests passed	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	Tests passed	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	Tests passed	MA certificate and FQDN	DCM shall provide the EE with the MA certificate and the FQDN for the MA.	The EE will need to communicate securely with the MA (e.g. in order to download CRLs)		DCM
SCMS-565	Tests passed	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	Tests passed	PCA certificates	DCM shall provide the EE with its own PCA certificate. Optionally, include other	The EE needs its PCA certificate, e.g. to provide this to other EE in peer-to-peer certificate updates.		DCM

Key	Status	Summary	Description	justification	notes	Component/s
			existing PCA certificates.			
SCMS-567	Tests passed	CRL	DCM shall provide the EE with the latest CRL and contact information for the CRL (CRACA certificate is part of the CRL).	The EE will be provided with the current CRL so as to reject communication from invalidated devices.		DCM
SCMS-568	Tests passed	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-946	Tests passed	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 the Misbehavior Authority.		DCM
SCMS-948	In Implementation	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

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-949	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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-1158	Review	Elector certificates	DCM shall provide the device with all Elector certificates.	The Elector certificates will be required to perform any future Root Management operations.		DCM
SCMS-1159	SCMS PoC out of Scope	EE securely stores Elector certificates	EE shall store the Elector certificates in tamper-evident storage.	The Elector 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 be updated when the proper Root Management authentication mechanisms	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
				have been satisfied.		
SCMS-1160	SCMS PoC out of Scope	EE securely stores Root CA certificates	EE shall store all Root CA certificates in tamper-evident 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 be updated when the proper Root (Elector) Management authentication mechanisms have been satisfied.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1174	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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	Tests passed	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	Implemented	Certificate Revocation List Generator certificate	DCM shall provide the OBE with the Certificate Revocation List Generator	The OBE requires this to validate the signature on the CRL.		DCM

Key	Status	Summary	Description	justification	notes	Component/s
			(CRLG) certificate.			
SCMS-1207	SCMS PoC out of Scope	EE stores Certificate Revocation List	EE shall store the Certificate Revocation List in tamper-evident 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)
SCMS-1208	SCMS PoC out of Scope	EE securely stores X.509 root certificate	EE shall store the X.509 root certificate in tamper-evident 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	SCMS PoC out of Scope	EE securely stores Local Certificate Chain File	EE shall store the Local Certificate Chain File in tamper-evident 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)

2.2.6.6 Step 2.2: OBE Enrollment

This specifies only the implementation for POC / Pilot Deployments.

Target release	Core
Document owner	Biswajit Panja
Reviewer	Jeff Hahn

2.2.6.6.1 Goals

Enrollment is the process by which a qualified (as per the certification policies set by SCMS Manager) device receives an enrollment certificate.

Once this process is complete, the OBE has:

- The enrollment certificate

2.2.6.6.2 Description

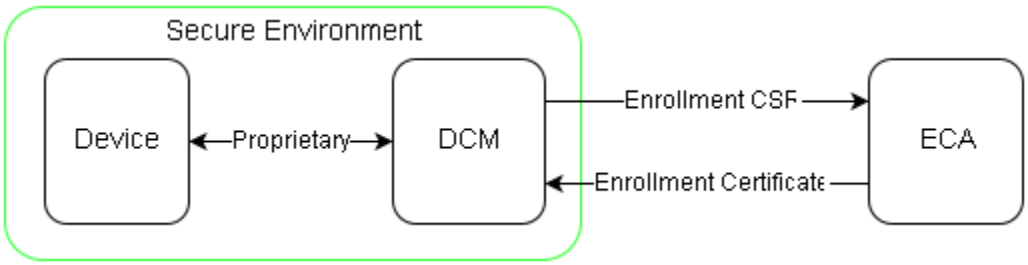
Entities involved

- Actively involved in the use case:
  - Device being enrolled
  - Device Configuration Manager (DCM)
  - Enrollment CA (ECA)
- Provide information before/during the use case:
  - Certification Services
  - Policy Generator

2.2.6.6.3 Prerequisites

- Device has been securely initialized and held within a secure chain of custody since initialization, see Step 2.1: OBE Initialization for details.
  - As a result of initialization the device has the ECA certificate and any necessary certificates to construct a chain back to the root (so it can verify its own enrollment certificate)
- Device is connected with DCM in a secure environment, as defined by SCMS Manager and recommended in Secure Environment for Device Enrollment.
- Enrollment certificate requests come only from a DCM that is authorized by the ECA.
- The ECA and the DCM have current X.509 certificates and access to CRLs or other revocation information to ensure that the certificates are trustworthy.
- DCM and ECA can communicate securely, i.e. with mutual authentication. For Proof of Concept the supported mechanism is a mutually authenticated TLS connection (as specified in SCMS-938, SCMS-938, SCMS-407, SCMS-479, SCMS-405)
- All participants that generate keys or signatures have access to and use an approved random number generator.

2.2.6.6.4 Process



4. The verification key pair (see Public Key Algorithms in CB2: Types of Cryptographic Algorithms for details about key pair) is generated. The private key is used to sign the certificate request and the public key is used as an input to calculating the public value within the implicit certificate that is issued at the end of this process.
   The verification key pair must be generated using any algorithm approved for use within the system (see Approved Cryptographic Algorithms). The enrollment certificate request does not use butterfly key expansion.
   Best practice is that the verification key material is generated inside the device, but key

generation off the device followed by secure key injection, as defined in Secure Environment for Device Enrollment, is permitted in the system.

5. A certificate signing request (CSR) is generated. This is a signed structure specified in eca-ee.asn. The CSR indicates:
    a. The verification public key to be used to create the certificate
    b. The permissions (PSIDs, SSPs, Geographic Region) and lifetime that are being requested for the enrollment certificate
        i. Requested lifetime is stated in the certificate request but may be overridden by the global policy for the particular PSID/SSP combination. See definition of global policy in scms-policy.asn and definition of requirements for global policy in this wiki.
    c. The SCMS PoC supports two options for signing the CSR:
        i. The private key is generated on the OBE and the CSR is signed by this key
        ii. The private key is generated by the DCM, the DCM signs the CSR with the generated key, and subsequently the key is injected to the OBE in step 5.

    There is a strong recommendation to implement the first option. The signed CSR is specified in scms-protocol.asn. This provides proof of possession of the signing key.

6. The DCM sends the CSR to the ECA.
    The proof that the DCM is entitled to authorize such a request is provided by the fact that the DCM and the ECA have a secure connection.
7. The ECA generates an enrollment certificate and returns it to the DCM. The response format is specified in eca-ee.asn. If the DCM doesn't receive the response within a configurable time it resends the request up to a configurable number of times. If the DCM receives a "rejected" response it does not resend the request. The response is sent over a reliable transport mechanism (HTTPs over TCP/IP) so there is no need for an acknowledge message at the application level. The response from the ECA is not encrypted at the application level, so it is visible to the DCM.
8. Verification of the enrollment certificate:
    - If the DCM generated the verification key pair:
        - DCM checks that the certificate corresponds to the private key and that the certificate correctly verifies (see CB3: Public Key Infrastructure for details about certificates and their verification), including building a chain back to the root.
        - If this check succeeds, it securely injects the enrollment certificate and the reconstructed private key in the OBE.
        - The DCM securely deletes the private key.
    - If the OBE generated the verification key pair:

- The DCM provides the enrollment certificate to the device.
- The OBE checks that the certificate corresponds to the private key and that the certificate correctly verifies, including building a chain back to the root.

2.2.6.6.5 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
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	SCMS PoC out of Scope	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-1210	SCMS PoC out of Scope	EE Secure Key Storing	EE shall store the following keys in tamper-evident storage: • Private enrollment key • Butterfly key	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	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
			parameters (seed + expansion function parameter) • All private keys (e.g. of OBE application certificates and private keys calculated from the Butterfly key parameters)		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	
SCMS-1305	Review	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	ECA shall not issue more than one enrollment certificate associated with a	A clear mapping is required for proper administration.	In cases where an enrollment certificate has more than one PSID, the correspond	ECA

Key	Status	Summary	Description	justification	notes	Component/s
		PSID/SSP combination	particular (PSID, SSP) combination per requested public key.		ing 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.	
SCMS-1307	Review	Enrollment certificate lifetime	ECA shall issue Enrollment Certificates with a lifetime of 30 years.	For PoC, enrollment certificates use a life span of 30 years to avoid any need to update enrollment certificates.	This is for PoC only	ECA
SCMS-1411	SCMS PoC out of Scope	CV pilots: DCM keep track of generated enrollment certificates	For the CV pilot deployment the Single Point of Contact (SPOC) of the DCMs shall keep track of all issued enrollment certificates.	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	Review	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	Review	Enrollment certificate lifetime	ECA shall issue Enrollment Certificates with a maximum lifetime of 7 years. All EE Enrollment certificates shall be issued with an expiration	For CV-Pilot, enrollment certificates use a maximum life span of 7 years to avoid any need to update enrollment certificates.	This is for CV-Pilot only.	ECA

Key	Status	Summary	Description	justification	notes	Component/s
			at year 7 regardless of the date they are issued.			
SCMS-1906	Review	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.		DCM, On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1907	Review	Enrollment certificate verification	The enrollment key-pair generator (OBE, RSE, or DCM) shall check that the enrollment certificate certificate correctly verifies, including building a chain back to the root.	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	SCMS PoC out of	Verification key pair generatio	EE shall shall generate the verification key pair	because only those algorithms will be supported by the SCMS.	See Approved Cryptographic Algorithm	On-board Equipment (OBE), Road-side

Key	Status	Summary	Description	justification	notes	Component/s
	Scope	n algorithm	using an algorithm approved for use within the SCMS.		s This is out of scope as it defines EE behavior.	Equipment (RSE)

2.2.7 Use Case 3: OBE Pseudonym Certificates Provisioning

Target release	Release 0.1
Document owner	Virendra Kumar
Reviewer	Roger Motz, Benedikt Brecht

2.2.7.1 Goals

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

2.2.7.2 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, as from this point onwards 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 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 3 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.

For an explanation of time periods i and j, please refer to Cryptographic Primitives.

2.2.7.3 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.

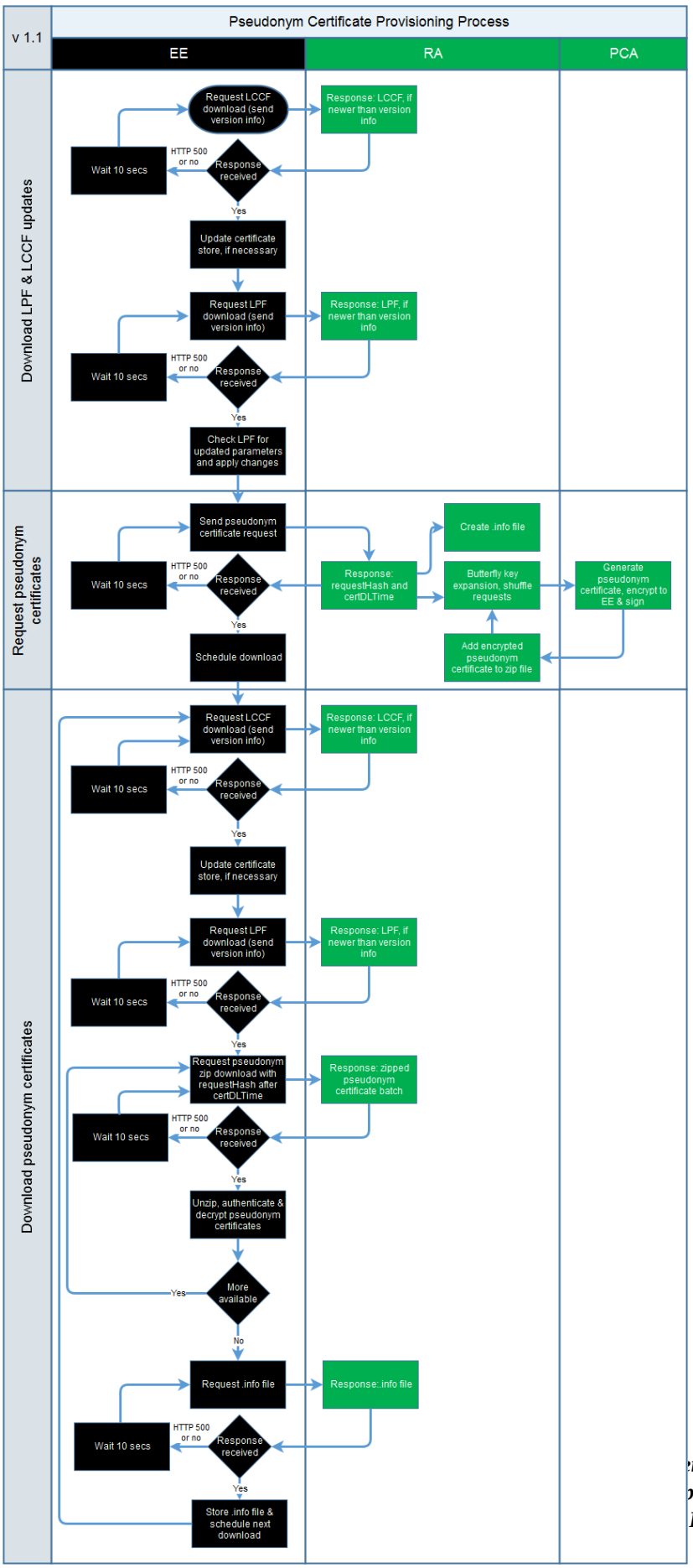
2.2.7.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-507	Tests failed	Maintain an Internal Blacklist	RA shall maintain an Internal Blacklist and keep it updated based on the communications with the MA	so that revoked EEs are not able to authenticate with the RA anymore	Every logical RA has its own internal blacklist that is not shared with anyone else. To prevent compromised components to speak with the RA the RA needs to validate against the SCMS component CRL (compare SCMS-859, https://jira.campllc.org/browse/SCMS-504~~SCMS-504~~) and the X.509 CRL (SCMS-405).	RA
SCMS-510	Implemented	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
SCMS-1270	SCMS PoC out of Scope	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-1727	SCMS PoC out of Scope	EE to verify RA FQDN matches	EEs shall verify that FQDN specified in the "id" field of the	SCMS components (server) are only	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-

Key	Status	Summary	Description	justification	notes	Component/s
		the RA SCMS certificate ID	RA's SCMS certificate matches the FQDN used to contact the RA.	reachable by standard TCP/IP networking methods.		side Equipment (RSE)

2.2.7.5 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 requirements for a complete description of the 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.*

2.2.7.6 Step 3.1: Request for Pseudonym Certificates

Target release	Release 0.1
Document owner	Biswajit Panja
Reviewer	Roger Motz, Rekha Singoria, Andre Weimerskirch

2.2.7.6.1 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 does change the number of request towards PCA though and therefore requires more computational and storage capacity at the PCA.

2.2.7.6.2 Background and strategic fit

Whenever the SCMS Manager decides to change technical policies for the SCMS, all participating devices need to 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 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 with the FQDN of the RA to which it submits the certificate batch request.

2.2.7.6.3 Assumptions

- OBE has successfully completed Use Case 2: OBE Bootstrapping

2.2.7.6.4 Process Steps

1. 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. 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.
2. 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.

2.2.7.6.5 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.

2.2.7.6.6 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-411	SCMS PoC out of Scope	EE Authentication to RA for Request	The EE shall authenticate its requests with its enrollment certificate. These messages shall include a timestamp (which the EE will obtain from its GPS reference) 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.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-507	Tests failed	Maintain an Internal Blacklist	RA shall maintain an Internal Blacklist	so that revoked EEs are not able to authenticate	Every logical RA has its own internal	RA

Key	Status	Summary	Description	justification	notes	Component/s
			and keep it updated based on the communications with the MA	with the RA anymore	blacklist that is not shared with anyone else. To prevent compromised components to speak with the RA the RA needs to validate against the SCMS component CRL (compare SCMS-859, https://jira.campllc.org/browse/SCMS-504~~SCMS-504~~) and the X.509 CRL (SCMS-405).	
SCMS-512	In Implementation	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	RA

Key	Status	Summary	Description	justification	notes	Component/s
					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).	
SCMS-515	Closed	RA requires EE authentication	The RA shall require EE authentication before any other communication process starts.	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.	RA

Key	Status	Summary	Description	justification	notes	Component/s
					EE authenticates via its IEEE 1609.2 enrollment certificate. The details of the authentication process are defined E-RA Communications - General Guidance	
SCMS-517	Implemented	Tunneling through LOP	RA shall provide downloads only via a LOP hardware interface, which removes all location information from the incoming request.	to anonymize the location of EEs.		RA
SCMS-520	SCMS PoC out of Scope	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,	so that EEs know that RA received their request.		RA

Key	Status	Summary	Description	justification	notes	Component/s
			currently set to be 1 sec.			
SCMS-522	SCMS PoC out of Scope	Retry request	If the EE does not receive acknowledgement (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, it shall retry.	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	SCMS PoC out of Scope	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-524	SCMS PoC out of Scope	RA certificate	EE shall dynamically acquire RA's SCMS certificate each time it communicates with RA.	so that EE can encrypt the request to the right RA	More information is available at RA - Retrieve Registration Authority Certificate. This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-529	Review	Store enrollment certificate and butterfly parameters	RA shall store enrollment certificate and butterfly parameters for each OBE for its lifetime, that is currently assumed to be 30 years	so that OBE can be revoked properly. Arbitrary number based on historical trends for vehicle ownership. For example, collector vehicles that are	PoC will only store 3 years	RA

Key	Status	Summary	Description	justification	notes	Component/s
				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	SCMS PoC out of Scope	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 E-RA Communications - General Guidance	This is out of scope since it defines EE's behavior.	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	to improve reliability of the download protocol.		RA

Key	Status	Summary	Description	justification	notes	Component/s
			switches the IP address.			
SCMS-709	SCMS PoC out of Scope	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.	1. If no policy file is available on the EE, the EE is allowed to make a download attempt at any time. 2. This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-754	SCMS PoC out of Scope	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	In Implementation	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	For more information: Generate Global and Local Certificate Chain File	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	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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-953	SCMS PoC out of Scope	Misbehavior report: eePolicyFileDownloadFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to download the local policy	to enable server side misbehavior detection.	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
			file (e.g. because there is none or it is corrupted).			
SCMS-954	SCMS PoC out of Scope	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-955	SCMS PoC out of Scope	Misbehavior report: eePolicyVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify the digital signature of the local policy file.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-956	SCMS PoC out of Scope	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-957	SCMS PoC out of Scope	Misbehavior report: eePolicyFileParsingFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to parse the successfully downloaded local policy file (e.g.	to enable server side misbehavior detection.	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
			because it is corrupted).			
SCMS-958	SCMS PoC out of Scope	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	In Implementation	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	In Implementation	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	In Implementation	Error code: raAuthenticationFailed	RA shall log "Error code: raAuthentication Failed", if EE-to-RA authentication fails.	to enable server side diagnostics and to avoid giving potential attackers relevant information.		RA
SCMS-979	SCMS PoC out of Scope	Error code: eeAuthenticationFailed	EE shall log "Error code: eeAuthentication Failed", 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-980	SCMS PoC out of Scope	Misbehavior report: eeAuthenticationFailed	EE shall initiate a misbehavior report to MA with the observed error, if RA-to-EE authentication fails.	to enable server side misbehavior detection.	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-981	In Implementation	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	In Implementation	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	In Implementation	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	In Implementation	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-1012	In Implementation	Error code: raWrongGlobalPolicyParameter	RA shall log "Error code: raWrongGlobalPolicyParameter", if a device sends request with parameters that are outside	to enable server side diagnostics and to avoid giving potential attackers relevant information. The Global	A request with wrong parameters might be an indication of misbehavior.	RA

Key	Status	Summary	Description	justification	notes	Component/s
			Global Policy configuration options.	Policy defines parameter and value ranges for the overall system that all participants in the system need to follow.		
SCMS-1065	In Implementation	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	Review	Error code: raDuplicateRequestReceived	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	SCMS PoC out of Scope	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	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
				trustworthy source.		
SCMS-1082	In Implementation	Error code: raInvalidSignature	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	In Implementation	Error code: raRequestNotEncrypted	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	In Implementation	Error code: raInvalidCredentials	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	In Implementation	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	In Implementation	Error code: raMalformedRequest	RA shall log "Error code: raMalformedRequest", if an EE	to enable server side diagnostics and to avoid giving potential	A malformed request might be an	RA

Key	Status	Summary	Description	justification	notes	Component/s
			makes a malformed request not captured in SCMS-1082, SCMS-1083, SCMS-1084, SCMS-1085.	attackers relevant information.	indication for misbehavior.	
SCMS-1087	In Implementation	Error code: raMismatch	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	In Implementation	Error code: raInvalidTimeReceived	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	SCMS PoC out of Scope	Trust Chain Broken - EE	EE shall not attempt to request or download pseudonym certificate batches, OBE identification certificate files, or RSE application certificate files, 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	To reduce resources, since RA will reject request anyways.	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
			local policy file or local certificate chain file from RA.			
SCMS-1203	Tests passed	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	Tests passed	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	RA

Key	Status	Summary	Description	justification	notes	Component/s
					device and put it on the internal blacklist. The RA does not send out enrollment certificates to the IBLM.	
SCMS-1263	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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	SCMS PoC out of Scope	EE request LCCF from RA	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)

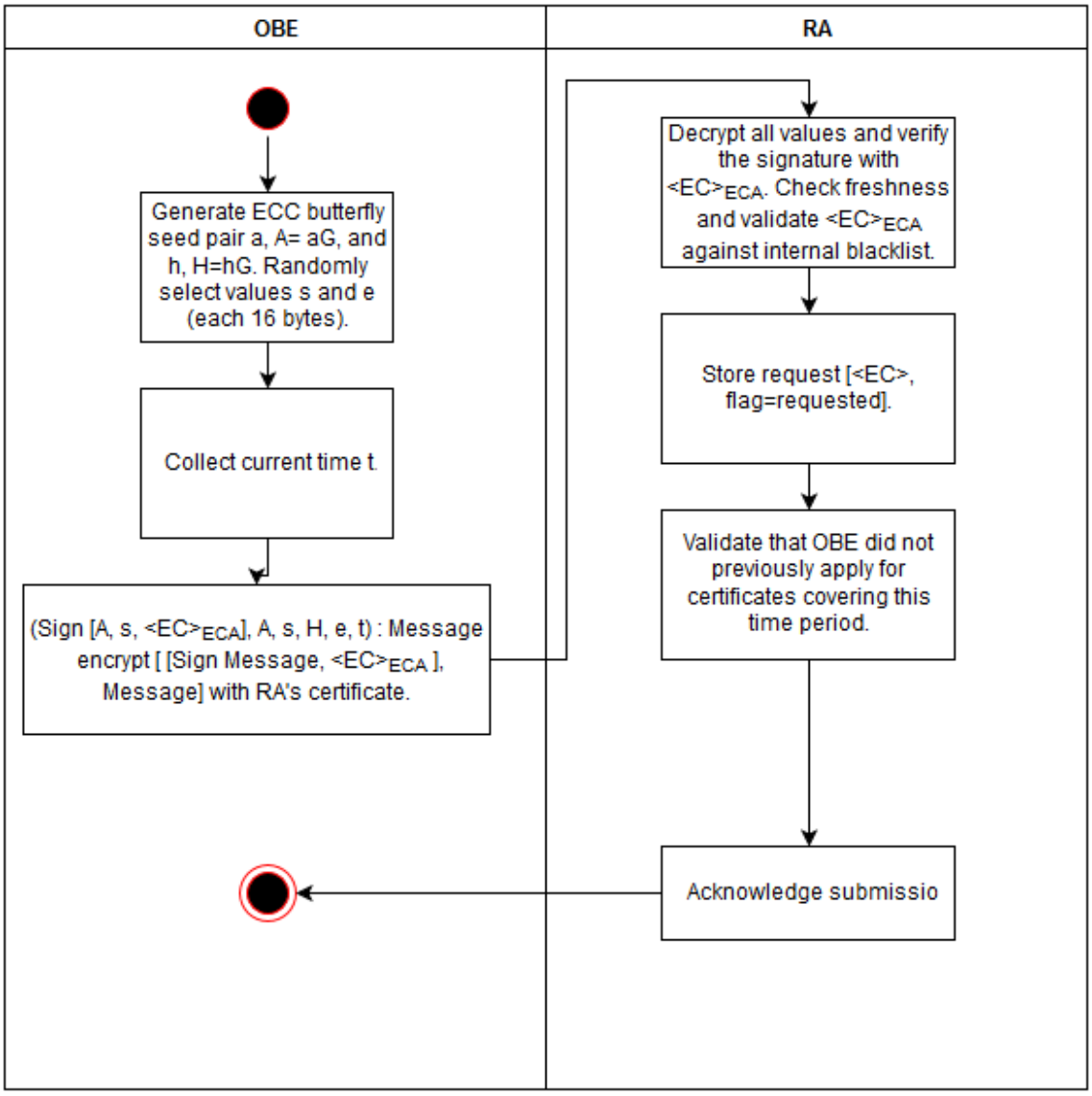
Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1356	SCMS PoC out of Scope	EE uses internal certificate store	EE shall use its internal certificate store to validate received SCMS certificates and respond to P2P certificate requests.	EEs need to be able to validate received SCMS certificates 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 EEs behavior	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1377	Review	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	Implemented	Error reporting to EE	SCMS Components shall return error code "HTTP 500" to EEs in response to all application level errors.	Specific error codes should be hidden from EEs to prevent useful information from being provided to malicious actors	• Standard TCP (SCMS-1090) and TLS (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	SCMS PoC out of Scope	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	Implemented	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	SCMS PoC out of Scope	LCCF validation in EE	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	SCMS PoC out of Scope	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	On-board Equipment (OBE)

Key	Status	Summary	Description	justification	notes	Component/s
					parameters for the certificate signature keys, and optionally for certificate encryption keys and response encryption keys.	
SCMS-1625	Review	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	as EE needs to know when and where it can go to download certificates.		On-board Equipment (OBE), RA, Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
			(common for all devices serviced by an specific RA) Case: Certificate Provisioning Request Reject 1. HTTP 500 error code			
SCMS-1727	SCMS PoC out of Scope	EE to verify RA FQDN matches the RA SCMS certificate ID	EEs shall verify that FQDN specified in the "id" field of the RA's SCMS certificate matches the FQDN used to contact the RA.	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)

2.2.7.6.7 Design



2.2.7.6.7.1 EE Request

EE initiates the Certificate Request message in order 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 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 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 is sent only once for each unique request, and no subsequent Certificate Provisioning Request is necessary to acquire new certificate batches.

2.2.7.6.7.1.1 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 EE
- The request is shared confidentially between EE 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.

2.2.7.6.7.1.2 Message Contents

The EE shall use the ASN.1 defined for creating the Request Certificate message, details can be found at EE to RA - Pseudonym 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 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)

2.2.7.6.7.2 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.

2.2.7.6.7.2.1 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.

2.2.7.6.7.3 Security / Privacy

The Request Acknowledge message shall use signing and encryption to ensure:

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

2.2.7.6.7.3.1 Message Contents

The RA shall use the ASN.1 defined for creating the Request Acknowledge message, can be found at EE to RA - Pseudonym 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

2.2.7.6.7.4 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.

2.2.7.7 Step 3.3: Initial Download of Pseudonym Certificates

Target release	Release 0.1
Document owner	Andre Weimerskirch
Reviewer	Virendra Kumar

2.2.7.7.1 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.

2.2.7.7.2 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, and
4. the local policy file.

2.2.7.7.3 Assumptions

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

2.2.7.7.4 Process Steps

5. 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, OBE applies all changes to its trust-store (necessary for PCA Certificate Validations).
   b. If there is an updated LPF, OBE applies those changes.
6. OBE downloads pseudonym certificate batches using the API documented in RA - Download Pseudonym Certificate Batch
7. OBE downloads .info file using the API documented in RA - Download .info file

2.2.7.7.5 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 need to execute the certification/bootstrap process again to exit a revoked state.

2.2.7.7.6 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-411	SCMS PoC out of Scope	EE Authentication to RA for Request	The EE shall authenticate its requests with its enrollment certificate. These messages shall include a timestamp (which	Messages from EEs to an RA must be secure against replay attacks. The signed time stamp from the EE	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 EE will obtain from its GPS reference) to avoid replay attacks on the RA.	enables the RA to validate the freshness of EE requests.		
SCMS-459	In Implementation	OCSP: Stapled for RA to OBE	The RA shall respond to an OBE request for an OCSP stapled certificate.	Most OBEs do not have access to CRL updates or a reliable network connection to an OCSP server, so the RA must provide an OCSP stapled response so that the OBE can validate the RA's TLS certificate.	OCSP stapling provides improved performance compared to CRLs. OCSP stapling is specified in RFC 6066, Section 8. The RA will be able to respond to the OBE's request for an OCSP stapled certificate. The RA itself will rely on an OCSP service to sign its certificate validation request, which it will return to the EE. For the PoC, the RA will refer to an X.509 CRL to validate certificates of SCMS back-end components (MA, LA, and PCA). OCSP will not be used for back-end component certificate validation.	RA

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-507	Tests failed	Maintain an Internal Blacklist	RA shall maintain an Internal Blacklist and keep it updated based on the communications with the MA	so that revoked EEs are not able to authenticate with the RA anymore	Every logical RA has its own internal blacklist that is not shared with anyone else. To prevent compromised components to speak with the RA the RA needs to validate against the SCMS component CRL (compare SCMS-859, https://jira.camp llc.org/browse/SCMS-504~~SCMS-504~~) and the X.509 CRL (SCMS-405).	RA
SCMS-512	In Implementation	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 before any other communication process starts.	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.	RA

Key	Status	Summary	Description	justification	notes	Component/s
					EE authenticates via its IEEE 1609.2 enrollment certificate. The details of the authentication process are defined E-RA Communications - General Guidance	
SCMS-517	Implemented	Tunneling through LOP	RA shall provide downloads only via a LOP hardware interface, which removes all location information from the incoming request.	to anonymize the location of EEs.		RA
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	For pseudonym certificates, this counters a somewhat exotic attack: if an attacker eavesdrops all individually encrypted pseudonym	On-board Equipment (OBE), RA, Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
				pseudonym certificates, that an adversary is able to read PCA-encrypted pseudonym certificates.	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	SCMS PoC out of Scope	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 E-RA Communicatio	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
				ns - General Guidance		
SCMS-541	SCMS PoC out of Scope	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-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	In Implementation	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	RA

Key	Status	Summary	Description	justification	notes	Component/s
					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	SCMS PoC out of Scope	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	• 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	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
				technical policies.	defines EE's behavior.	
SCMS-768	In Implementation	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.	For more information: Generate Global and Local Certificate Chain File	RA
SCMS-951	Review	Error code: raEeVerificationFailed	RA shall log "Error code: raEeVerificationFail	EE might need re-certification	Does not apply to POC. Might be added to MA	RA

Key	Status	Summary	Description	justification	notes	Component/s
			ed", if an EE cannot be authenticated.		integration as a misbehavior.	
SCMS-952	SCMS PoC out of Scope	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-953	SCMS PoC out of Scope	Misbehavior report: eePolicyFileDownloadFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to download the local policy file (e.g. because there is none or it is corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-954	SCMS PoC out of Scope	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-955	SCMS PoC out of Scope	Misbehavior report: eePolicyVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify the digital	to enable server side misbehavior detection.	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
			signature of the local policy file.			
SCMS-956	SCMS PoC out of Scope	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-957	SCMS PoC out of Scope	Misbehavior report: eePolicyFileParsingFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to parse the successfully downloaded local policy file (e.g. because it is corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-958	SCMS PoC out of Scope	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	In Implementation	Error code: raNoCertFileAvailable	RA shall return status code HTTP 500 to EE, if certificate batch is not available and log "Error code:	to enable EE side error handling.		RA

Key	Status	Summary	Description	justification	notes	Component/s
			raNoCertFileAvailable.			
SCMS-965	SCMS PoC out of Scope	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-966	SCMS PoC out of Scope	Misbehavior report: eeCertFileDownloadFailed	EE shall initiate a misbehavior report to MA, if EE is not able to download certificate files (e.g. because there is none or it is corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-967	SCMS PoC out of Scope	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's 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-968	SCMS PoC out of Scope	Misbehavior report: eeCertFileVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify the digital signature of an encrypted certificate.	to enable server side misbehavior detection.	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-969	SCMS PoC out of Scope	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-970	SCMS PoC out of Scope	Misbehavior report: eeCertFileDecryptionFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to decrypt an encrypted certificate.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)
SCMS-971	SCMS PoC out of Scope	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-972	SCMS PoC out of Scope	Misbehavior report: eeCertVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify a certificate.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-973	SCMS PoC out of Scope	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-974	SCMS PoC out of Scope	Misbehavior report: eeCertContentFalse	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to parse a certificate, or if the certificate has wrong content.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-976	In Implementation	Error code: raInvalidURL	RA shall log "Error code: raInvalidURL", if	to enable server side diagnostics	This is not in ASN.1 but http 404	RA

Key	Status	Summary	Description	justification	notes	Component/s
			EE requests invalid URL.	and to avoid giving potential attackers relevant information		
SCMS-977	In Implementation	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	In Implementation	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	SCMS PoC out of Scope	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-980	SCMS PoC out of Scope	Misbehavior report: eeAuthenticationFailed	EE shall initiate a misbehavior report to MA with the observed error, if RA-to-EE authentication fails.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-981	In Implementation	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	Tests passed	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-983	In Implementation	Error code: raNoInfoFileAvailable	RA shall return status code HTTP 500, if it is not able to provide a current .info file and log "Error code: raNoInfoFileAvailable".	to enable EE side error handling.		RA
SCMS-984	SCMS PoC out of Scope	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's behavior.	On-board Equipment (OBE)
SCMS-985	SCMS PoC out of Scope	Misbehavior report: eeInfoFileDownloadFailed	OBE shall initiate a misbehavior report to MA with the observed error, if OBE is not able to download the .info file (e.g. because there is none or it is corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)
SCMS-1065	In Implementation	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

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1076	SCMS PoC out of Scope	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	Implemented	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-1163	SCMS PoC out of Scope	OBE revoked	A revoked OBE shall not attempt to download pseudonym certificate batches/OBE identification certificate files.	To reduce resource usage, since RA will reject request anyways.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)
SCMS-1189	SCMS PoC out of Scope	Trust Chain Broken - EE	EE shall not attempt to request or download pseudonym certificate batches, OBE identification certificate files, or RSE application certificate files, if any component in the trust chain of EE's enrollment certificate is	To reduce resources, since RA will reject request anyways.	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
			revoked. In this case, EE also shall not attempt to download a local policy file or local certificate chain file from RA.			
SCMS-1201	SCMS PoC out of Scope	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	Tests passed	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	Tests passed	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	RA

Key	Status	Summary	Description	justification	notes	Component/s
					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	SCMS PoC out of Scope	OBE downloads .info file	OBE shall download the .info file each time OBE tries to download 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	SCMS PoC out of Scope	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 not waste resources by trying to download certificates before they are available.	This is out of scope since it defines EE's 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-1263	SCMS PoC out of Scope	EE download resume	EE shall try byte-wise resume of CRL downloads from the CRL store, certificate batches, certificate files, or	This will improve reliability of the download process and reduce		On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
			policy files from RA in case a previous download failed.	communication cost.		
SCMS-1279	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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)
SCMS-1282	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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	SCMS PoC out of Scope	EE request LCCF from RA	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	On-board Equipment (OBE), RA, Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
					scope since it defines EE behavior	
SCMS-1356	SCMS PoC out of Scope	EE uses internal certificate store	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 EEs behavior	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1377	Review	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	Implemented	Error reporting to EE	SCMS Components shall return error code "HTTP 500" to EEs in response to all application level errors.	Specific error codes should be hidden from EEs to prevent useful information from being provided to malicious actors	• Standard TCP (SCMS-1090) and TLS (SCMS-977) errors shall be reported to EEs • All errors at the HTTP and higher levels shall	CRL Store, RA

Key	Status	Summary	Description	justification	notes	Component/s
					be HTTP 500 for RA & ECA	
SCMS-1404	SCMS PoC out of Scope	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	Implemented	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	SCMS PoC out of Scope	LCCF validation in EE	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	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
				p2p certificate requests.		
SCMS-1454	Review	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	Review	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	File content must be predefined to allow EEs to process the contents.	For example: • 0_0 • 0_1 • … • 0_<*j_max-1*>	RA

Key	Status	Summary	Description	justification	notes	Component/s
			• Where there is no extension			
SCMS-1639	SCMS PoC out of Scope	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 of https://jira.campllc.org/browse/SCMS-547~~SCMS-547~~	On-board Equipment (OBE)

2.2.7.7.7 Design

- Step 0: OBE and RA authenticate to each other, see below.
- Step 1: OBE downloads the local certificate chain file (LCCF) (see Step 18.5: Generate Global and Local Certificate Chain File) and the local policy file (LPF) (see Step 18.2: Generate Local Policies for EEs).
- Step 2: OBE downloads certificate batch files X_Y.zip, where X is the lower 8-bytes of the SHA-256 hash of device request in hexadecimal and Y is the i-value in hexadecimal (both case insensitive). OBE downloads either all available files X_Y.zip, or as many as possible.
- Step 3: OBE downloads the .info file (generated and updated by RA). The .info file contains the time when the next certificate batches will be available.
    - In order for the OBE 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 the date and time the RA is predicted to update certificate batches in the device repository. 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 (case insensitive).
- The .info file shall contain a single IEEE 1609.2 Time32 timestamp (the number of (TAI) seconds since 00:00:00 UTC, 1 January 2004) that the OBE will use to schedule a

subsequent “top-up” download. If RA stopped generation of certificates for EE, the .info file shall contain an IEEE 1609.2 Time32 timestamp of value '(uint32) 0'.

For more details: See Sections 6.6.2.3 and 6.6.2.4 in “V2V-SE Minimum Performance Requirements (SAE J2945)”.

2.2.7.8 Step 3.5: Top-off Pseudonym Certificates

Target release	Release 1.0
Document owner	Roger Motz
Reviewer	Andre Weimerskirch, Virendra Kumar

2.2.7.8.1 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.

2.2.7.8.2 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 and
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.

2.2.7.8.3 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.

2.2.7.8.4 Process Steps

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

2. 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, 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. OBE downloads pseudonym certificate batches.
4. OBE downloads .info file using the API documented in RA - Download .info file

2.2.7.8.5 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.

2.2.7.8.6 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-411	SCMS PoC out of Scope	EE Authentication to RA for Request	The EE shall authenticate its requests with its enrollment certificate. These messages shall include a timestamp (which the EE will obtain from its GPS reference) 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.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-459	In Implement ation	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	OCSP stapling provides improved performance compared to CRLs. OCSP stapling is specified in	RA

Key	Status	Summary	Description	justification	notes	Component/s
				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 failed	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	RA

Key	Status	Summary	Description	justification	notes	Component/s
					needs to validate against the SCMS component CRL (compare SCMS-859, https://jira.campllc.org/browse/SCMS-504~~SCMS-504~~) and the X.509 CRL (SCMS-405).	
SCMS-509	In Implementation	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	In Implementation	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 before any other communication process starts.	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	RA

Key	Status	Summary	Description	justification	notes	Component/s
					certificate to identify itself. EE authenticates via its IEEE 1609.2 enrollment certificate. The details of the authentication process are defined E-RA Communications - General Guidance	
SCMS-517	Implemented	Tunneling through LOP	RA shall provide downloads only via a LOP hardware interface, which removes all location information from the incoming request.	to anonymize the location of EEs.		RA
SCMS-522	SCMS PoC out of Scope	Retry request	If the EE does not receive acknowledgement (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, it shall retry.	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	SCMS PoC out of Scope	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-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	On-board Equipment (OBE), RA, Road-side Equipment (RSE)

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	SCMS PoC out of Scope	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 E-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	SCMS PoC out of Scope	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	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
					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 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	This might change during the lifetime of the SCMS. It might even vary for different EEs.		RA

Key	Status	Summary	Description	justification	notes	Component/s
			configuration option max_available_cert_supply in the global policy.			
SCMS-548	In Implementation	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 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	RA

Key	Status	Summary	Description	justification	notes	Component/s
					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	Tests passed	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	SCMS PoC out of Scope	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	• If no policy file is available on the EE, the EE is allowed to make a download attempt at any time.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
				details are available at Use Case 18: Provide and enforce technical policies.	• This is out of scope since it defines EE's behavior.	
SCMS-768	In Implementation	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.	For more information: Generate Global and Local Certificate Chain File	RA
SCMS-952	SCMS PoC out of Scope	Error code: eePolicyFileDownloadFailed	EE shall log the error code in EE's error log file, if EE is not able to download the	As the policy file is essential for the system to work correctly and contains	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
			local policy file (e.g. because there is none or it is corrupted).	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-953	SCMS PoC out of Scope	Misbehavior report: eePolicyFileDownloadFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to download the local policy file (e.g. because there is none or it is corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-954	SCMS PoC out of Scope	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-955	SCMS PoC out of Scope	Misbehavior report: eePolicyVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify the digital signature of the local policy file.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-956	SCMS PoC out of Scope	Error code: eePolicyFileParsingFailed	EE shall log this error code in EE's error log	As the policy file is essential for the system	This is out of scope since it	On-board Equipment (OBE), Road-

Key	Status	Summary	Description	justification	notes	Component/s
			file, if EE is not able to parse the successfully downloaded local policy file (e.g. because it is corrupted).	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.	defines EE's behavior.	side Equipment (RSE)
SCMS-957	SCMS PoC out of Scope	Misbehavior report: eePolicyFileParsingFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to parse the successfully downloaded local policy file (e.g. because it is corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-958	SCMS PoC out of Scope	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	In Implementation	Error code: raNoCertFileAvailable	RA shall return status code HTTP 500 to EE, if certificate batch is not available and log "Error code: raNoCertFileAvailable.	to enable EE side error handling.		RA

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-965	SCMS PoC out of Scope	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-966	SCMS PoC out of Scope	Misbehavior report: eeCertFileDownloadFailed	EE shall initiate a misbehavior report to MA, if EE is not able to download certificate files (e.g. because there is none or it is corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-967	SCMS PoC out of Scope	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's 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-968	SCMS PoC out of Scope	Misbehavior report: eeCertFileVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify the	to enable server side misbehavior detection.	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
			digital signature of an encrypted certificate.			
SCMS-969	SCMS PoC out of Scope	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-970	SCMS PoC out of Scope	Misbehavior report: eeCertFileDecryptionFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to decrypt an encrypted certificate.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)
SCMS-971	SCMS PoC out of Scope	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-972	SCMS PoC out of Scope	Misbehavior report: eeCertVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify a certificate.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-973	SCMS PoC out of Scope	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-974	SCMS PoC out of Scope	Misbehavior report:	EE shall initiate a misbehavior report to MA	to enable server side	This is out of scope since it	On-board Equipment (OBE), Road-

Key	Status	Summary	Description	justification	notes	Component/s
		eeCertContent False	with the observed error, if EE is not able to parse a certificate, or if the certificate has wrong content.	misbehavior detection.	defines EE's behavior.	side Equipment (RSE)
SCMS-976	In Implementation	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	In Implementation	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	In Implementation	Error code: raAuthenticationFailed	RA shall log "Error code: raAuthentication Failed", if EE-to-RA authentication fails.	to enable server side diagnostics and to avoid giving potential attackers relevant information.		RA
SCMS-979	SCMS PoC out of Scope	Error code: eeAuthenticationFailed	EE shall log "Error code: eeAuthentication Failed", 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-980	SCMS PoC out of Scope	Misbehavior report: eeAuthenticationFailed	EE shall initiate a misbehavior report to MA with the observed error, if RA-to-EE	to enable server side misbehavior detection.	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
			authentication fails.			
SCMS-981	In Implementation	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	Tests passed	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-983	In Implementation	Error code: raNoInfoFileAvailable	RA shall return status code HTTP 500, if it is not able to provide a current .info file and log "Error code: raNoInfoFileAvailable".	to enable EE side error handling.		RA
SCMS-984	SCMS PoC out of Scope	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's behavior.	On-board Equipment (OBE)
SCMS-985	SCMS PoC out of Scope	Misbehavior report: eeInfoFileDownloadFailed	OBE shall initiate a misbehavior report to MA with the observed error, if OBE is not able to download the	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)

Key	Status	Summary	Description	justification	notes	Component/s
			.info file (e.g. because there is none or it is corrupted).			
SCMS-1065	In Implementation	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	Review	Error code: raDuplicateRequestReceived	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	SCMS PoC out of Scope	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	Implemented	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-1163	SCMS PoC out of Scope	OBE revoked	A revoked OBE shall not attempt to download pseudonym certificate batches/OBE identification certificate files.	To reduce resource usage, since RA will reject request anyways.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)
SCMS-1164	SCMS PoC out of Scope	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	On-board Equipment (OBE)

Key	Status	Summary	Description	justification	notes	Component/s
					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 or next time period, the OBE is allowed to make a download attempt at any time.	
SCMS-1167	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)

Key	Status	Summary	Description	justification	notes	Component/s
				stored on the device. This is to prevent repeated downloads of the same content.		
SCMS-1171	SCMS PoC out of Scope	EE revoked	EE shall not attempt to download a policy file, if it is revoked.	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	SCMS PoC out of Scope	Trust Chain Broken - EE	EE shall not attempt to request or download pseudonym certificate batches, OBE identification certificate files, or RSE application certificate files, 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 anyways.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1201	SCMS PoC out of Scope	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

Key	Status	Summary	Description	justification	notes	Component/s
						Equipment (RSE)
SCMS-1203	Tests passed	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	Tests passed	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	RA

Key	Status	Summary	Description	justification	notes	Component/s
					internal blacklist. The RA does not send out enrollment certificates to the IBLM.	
SCMS-1214	SCMS PoC out of Scope	OBE downloads .info file	OBE shall download the .info file each time OBE tries to download 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	SCMS PoC out of Scope	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's 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-1263	SCMS PoC out of Scope	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	SCMS PoC out of Scope	Network connection	EEs shall use TCP/IP to	SCMS components (server) are	This is out of scope since it	On-board Equipment (OBE), Road-

Key	Status	Summary	Description	justification	notes	Component/s
			communicate with the SCMS.	only reachable by standard TCP/IP networking methods.	defines EE's behavior.	side Equipment (RSE)
SCMS-1282	SCMS PoC out of Scope	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	SCMS PoC out of Scope	EE request LCCF from RA	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	SCMS PoC out of Scope	EE uses internal certificate store	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	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 EEs behavior	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
				certificate chain.		
SCMS-1377	Review	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	Implemented	Error reporting to EE	SCMS Components shall return error code "HTTP 500" to EEs in response to all application level errors.	Specific error codes should be hidden from EEs to prevent useful information from being provided to malicious actors	• Standard TCP (SCMS-1090) and TLS (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	SCMS PoC out of Scope	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	Implemented	RA accept authenticated HTTP post requests	RA shall accept HTTP post requests only from	to allow the SCMS endpoint to serve everything	RA - Services View will document the actual HTTP post details.	RA

Key	Status	Summary	Description	justification	notes	Component/s
			authenticated EEs.	based on HTTP protocol		
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	SCMS PoC out of Scope	LCCF validation in EE	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-1454	Review	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	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
			hexadecimal in uppercase • Where the extension is .zip in lowercase			
SCMS-1456	Review	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	SCMS PoC out of Scope	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 of https://jira.c	On-board Equipment (OBE)

Key	Status	Summary	Description	justification	notes	Component/s
					ampllc.org/browse/SCMS-547~~SCMS-547~~	
SCMS-1727	SCMS PoC out of Scope	EE to verify RA FQDN matches the RA SCMS certificate ID	EEs shall verify that FQDN specified in the "id" field of the RA's SCMS certificate matches the FQDN used to contact the RA.	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)

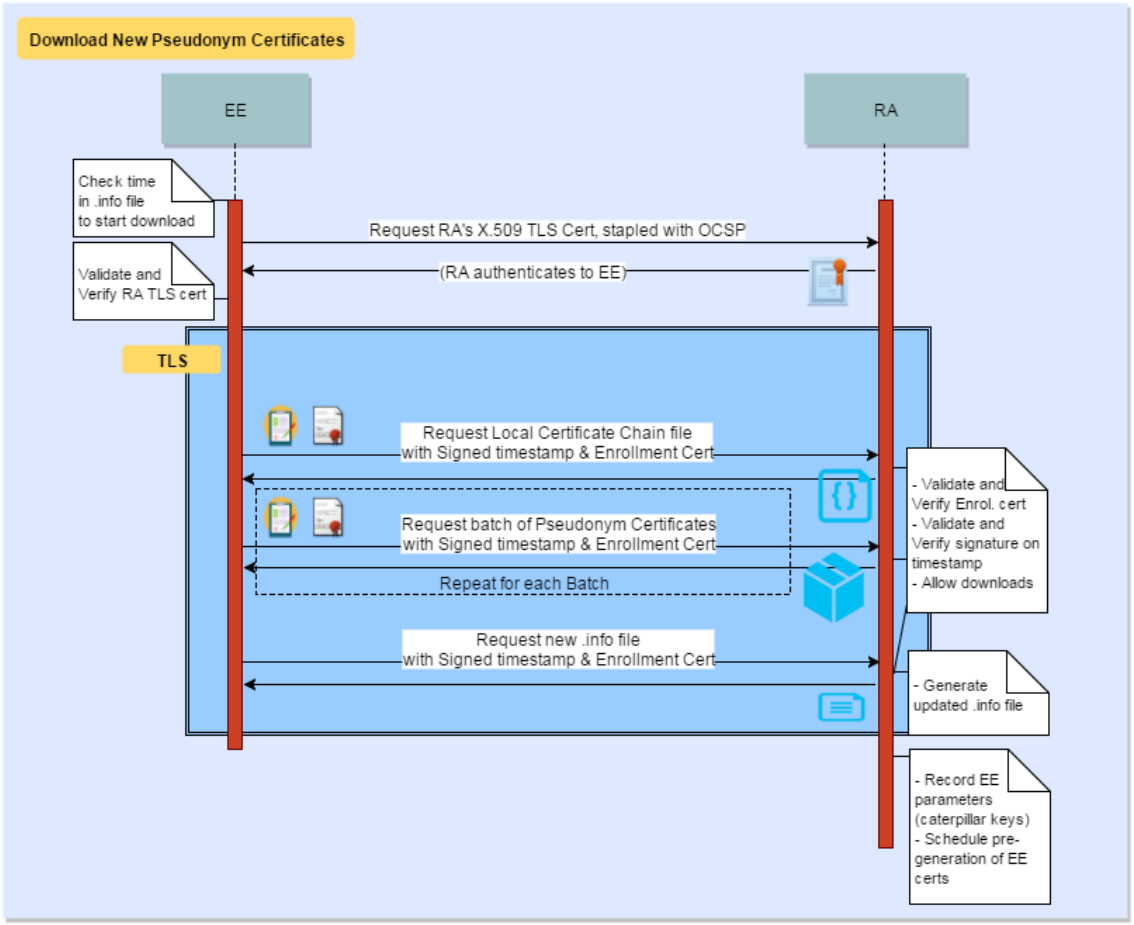
2.2.7.8.7 Design

- Step 1: OBE will use .info file from the last certificate batch download to determine the time when Certificates will be available and a download can be attempted.
- Step 2: OBE and RA authenticate to each other.
- Step 3: OBE downloads the local certificate chain file (LCCF) (see Step 18.5: Generate Global and Local Certificate Chain File) and the local policy file (LPF) (see Step 18.2: Generate Local Policies for EEs).
    - Step 3.1: The RA records the time stamp of the connection from the EE.
    - Step 3.2: If pre-generation of certificates has been stopped, RA will resume pre-generation. This step is out of scope for PoC.
- Step 4: OBE will download all or as many as possible, certificate files that it does not already have stored locally. It is the responsibility of the OBE to determine which certificate batch files to download (i.e. skip files that have already been successfully downloaded and processed).
- Step 5: OBE downloads the .info file (generated and updated by RA). The .info file contains the time when the next certificate batches will be available.

2.2.7.8.8 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.



2.2.7.8.9 Not Doing

- Stopping of pre-generation of pseudonym certificates if an OBE has not contacted the RA for a period of time. See Questions section above.

2.2.8 Use Case 5: Misbehavior Reporting

Target release	Release 1.1
Document owner	Biswajit Panja

Reviewer	Roger Motz, Virendra Kumar

2.2.8.1 Goals

1. Maintain the trust in the system
2. Identify and remove bad actors

2.2.8.2 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.

2.2.8.3 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-507	Tests failed	Maintain an Internal Blacklist	RA shall maintain an Internal Blacklist and keep it updated based on the communications with the MA	so that revoked EEs are not able to authenticate with the RA anymore	Every logical RA has its own internal blacklist that is not shared with anyone else. To prevent compromised components to speak with the RA the RA needs to validate against the SCMS component CRL (compare SCMS-859, https://jira.campllc.org/browse/SCMS-504~~SCMS-504~~) and the X.509 CRL (SCMS-405).	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,	so that EEs know that RA received their request.		RA

Key	Status	Summary	Description	justification	notes	Component/s
			currently set to be 1 sec.			
SCMS-522	SCMS PoC out of Scope	Retry request	If the EE does not receive acknowledgement (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, it shall retry.	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	SCMS PoC out of Scope	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-684	SCMS PoC out of Scope	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	Implemented	Privacy	LOP shall remove all information in the IP layer that can	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
			be used to identify the location of the OBE before forwarding the misbehavior report to the RA.			
SCMS-686	In Implementation	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	In Implementation	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-766	In Implementation	Shuffle Queue	RA shall use one shuffle queue for misbehavior reports coming from both RSE and OBE.	So that during implementation just one shuffle queue created for both RSE and OBE.		RA
SCMS-768	In Implementation	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	For more information: Generate Global and Local Certificate Chain File	RA

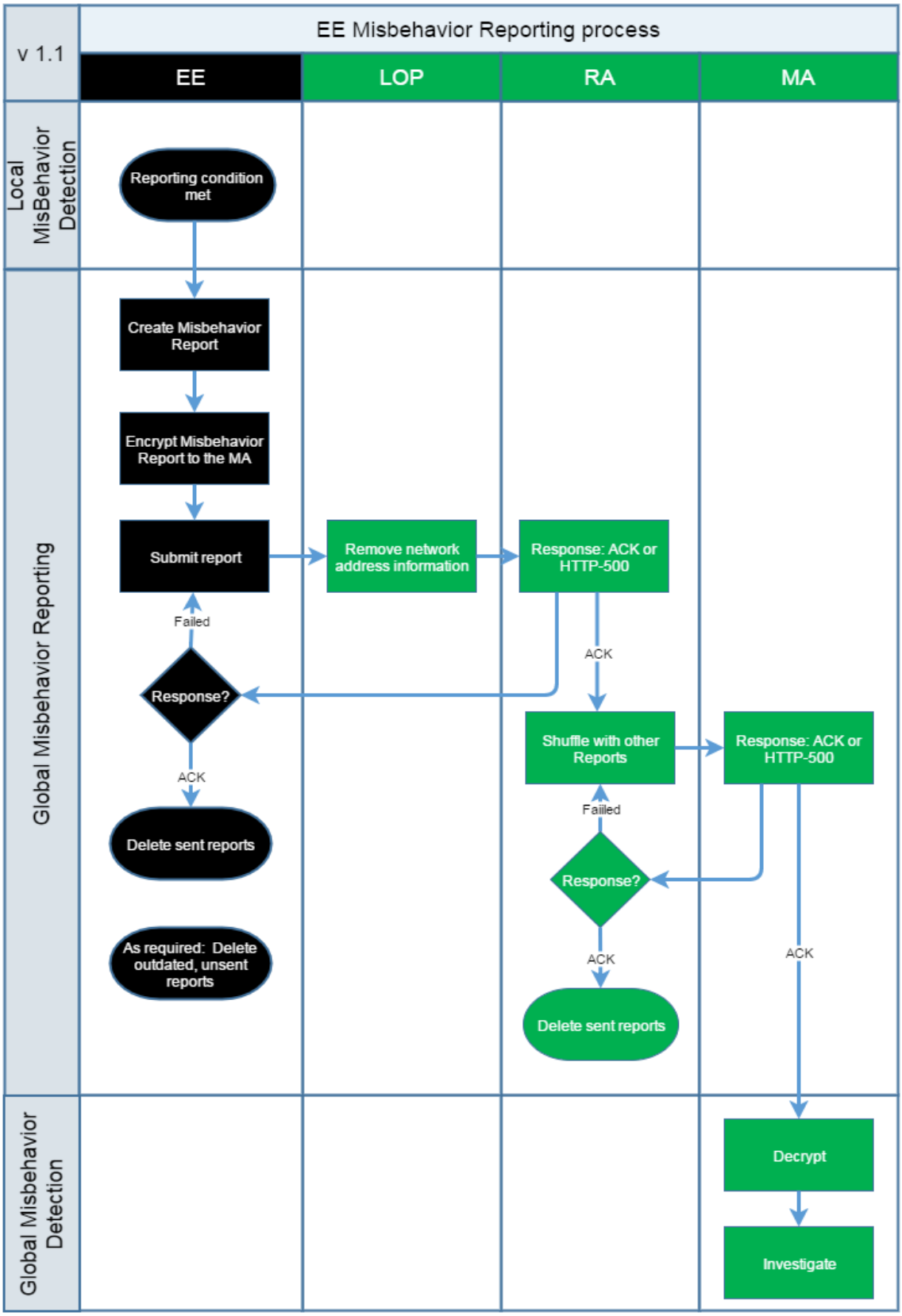
Key	Status	Summary	Description	justification	notes	Component/s
				indicates a new version, the RA will update its Local Certificate Chain File with the new chain information, as appropriate for the EEs under its jurisdiction. EEs send their current LCCF's version number in the download request to RA and the response will include a newer LCCF if available.		
SCMS-1013	SCMS PoC out of Scope	Error code: eeEncryptionFailed	EE shall log this error code, if EE encounters an error when encrypting a misbehavior report with MA's public key.	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-1014	In Implementation	Error code: maDecryptionFailed	MA shall log "Error code: maDecryptionFailed", if MA encounters an error when decrypting a misbehavior report.	to enable server side diagnostics.		MA

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1270	SCMS PoC out of Scope	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-1308	SCMS PoC out of Scope	OBE sign misbehavior reports	OBE shall sign a misbehavior report with a currently valid (at time of event observation) pseudonym certificate.	To avoid forged misbehavior reports	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)
SCMS-1309	SCMS PoC out of Scope	RSE sign misbehavior report	RSE shall sign misbehavior reports with RSE application certificate	To avoid forged misbehavior reports	RSE digitally signs misbehavior reports with an RSE application certificate intended for signing misbehavior reports (i.e., with a determined PSID for such purpose). This is out of scope since it defines EE's behavior.	Road-side Equipment (RSE)
SCMS-1339	In Implementation	Implement interface to receive misbehavior reports	RA shall implement the interface specified in ee-ma.asn to receive misbehavior reports from EEs.	to enable automatic reporting from EEs based on local misbehavior detection		RA
SCMS-1375	Review	MA verification of	MA shall verify a	This is MA's counterpart to	This is for POC only, and might	MA

Key	Status	Summary	Description	justification	notes	Component/s
		misbehavior report	misbehavior report by (1) checking the signature, and (2) checking that an OBE pseudonym certificate (or a certificate with proper PSID/SSP) was used to sign the certificate that was valid at the time of event observation.	https://jira.campllc.org/browse/SCMS-1308~~SCMS-1308~~	need revision for deployment.	
SCMS-1397	Implemented	Error reporting to EE	SCMS Components shall return error code "HTTP 500" to EEs in response to all application level errors.	Specific error codes should be hidden from EEs to prevent useful information from being provided to malicious actors	• Standard TCP (SCMS-1090) and TLS (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	SCMS PoC out of Scope	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	Implemented	RA accept authenticated	RA shall accept HTTP	to allow the SCMS endpoint	RA - Services View will	RA

Key	Status	Summary	Description	justification	notes	Component/s
		HTTP post requests	post requests only from authenticated EEs.	to serve everything based on HTTP protocol	document the actual HTTP post details.	
SCMS-1638	Review	MA verification of misbehavior report	MA shall verify a misbehavior report by (1) checking the signature, and (2) checking that an RSE application certificate (or a certificate with proper PSID/SSP) was used to sign the certificate that was valid at the time of event observation.	This is MA's counterpart to https://jira.campllc.org/browse/SCMS-1309~~SCMS-1309~~	This is for POC only, and might need revision for deployment.	MA

2.2.8.4 Design



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 reach 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

2.2.8.5 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.

2.2.9 Use Case 6: CRL Download

Target release	Release 1.0
Document owner	Rob Lambert
Reviewer	Benedikt Brecht

2.2.9.1 Goals

- To provide the CRL file from the CRL Store (a component of the MA) to the EE when requested.

2.2.9.2 Background and strategic fit

EE must be aware of revoked entities.

2.2.9.3 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 not require that the EE sends its enrollment certificate for authentication purposes.
- OBE has successfully executed Use Case 2: OBE Bootstrapping

2.2.9.4 Process Steps

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

2.2.9.5 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-335	SCMS PoC out of Scope	EE issues a CRL Request	An EE shall issues a HTTP get to the CRL Store to obtain the latest CRL.	EE needs to be provided with current CRL so that the EE can be informed of revoked components.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-340	Tests passed	CRL availability	The CRL Store shall provide a CRL for download at any given time.	To ensure that an EE can always download a CRL.		CRL Store
SCMS-341	SCMS PoC out of Scope	EE TLS Cipher Suite	The EE shall at minimum support SSL cipher suite TLS_ECDHE_ECDSA_WITH_AES_128_CCM (as defined in RFC7251) for all communications to SCMS components.	This is the requirement for the SSL transport tunnel.	Defined in Study 3 document in section 3.4.3.6 - Certificate Batch Download This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-342	SCMS PoC out of Scope	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 certificate to CRL Store but EE can download the	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
					CRL without authentication to CRL Store. This is out of scope as it defines EE behavior.	
SCMS-786	Tests passed	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-951	Review	Error code: raEeVerificationFailed	RA shall log "Error code: raEeVerificationFailed", if an EE cannot be authenticated.	EE might need re-certification	Does not apply to POC. Might be added to MA integration as a misbehavior.	RA
SCMS-991	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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	SCMS PoC out of Scope	Error code: eeCRLVerificationFailed	EE shall log "Error code: eeCRLVerificationFailed", if verification of the CRL signature fails.	In order to enable client side error handling and misbehavior reporting.	This is out of scope since it defines EE's behavior. Might be added with MA integration as potential misbehavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-997	Tests passed	CRL Store validates CRLs	The CRL store shall cryptographically verify an updated CRL before it is entered into the CRL Store.	To ensure that invalid CRLs are not distributed. This will ensure that new CRL changes take effect immediately and EEs always receive the newest CRL when requests are made.		CRL Store
SCMS-1263	SCMS PoC out of Scope	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-1264	Implemented	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	SCMS PoC out of Scope	Network connection	EEs shall use TCP/IP to communicate with the SCMS.	SCMS components (server) are only reachable by standard TCP/IP	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
				networking methods.		

2.2.9.6 ASN.1 Specification

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

2.2.10 Use Case 8: OBE Pseudonym Certificate Revocation

Target release	Release 2.0
Document owner	Andre Weimerskirch
Reviewer	Benedikt Brecht

OBE Revocation will be integrated with the to-be-awarded "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.

2.2.10.1 Goals

- Perform misbehavior investigation and eventually revocation of OBEs.

2.2.10.2 Step 8.4: OBE CRL Check

Target release	Release 1.0
Document owner	Andre Weimerskirch
Reviewer	Benedikt Brecht

2.2.10.2.1 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.

2.2.10.2.2 Assumptions

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

2.2.10.2.3 Process Steps

- 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.
- Whenever OBE receives a new unknown pseudonym certificate, it checks whether the linkage value of that unknown certificate is listed in OBE's expanded CRL (from Step 1).
    - If yes, then OBE discards the received certificate.
    - Otherwise, OBE accepts the received certificate as verified.

- Whenever OBE receives a new unknown OBE identification certificate, OBE will calculate the certificate digest of that unknown certificate and check whether the CRL lists it.
    - If yes, then OBE discards the received certificate.
    - Otherwise, OBE accepts the received certificate as verified.
- Before the end of each i-period, OBE will
    - Update its expanded CRL and calculate the linkage value for the next i-period.
    - 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.
- If 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 OBE recognizes that the Enrollment CA that issued OBE's enrollment certificate, the Pseudonym CA that issued 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.

2.2.10.2.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-786	Tests passed	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	SCMS PoC out of Scope	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	SCMS PoC out of Scope	OBE updates linkage value list	OBE shall update the list of revoked linkage values for each i-period. OBE shall either update the linkage value	OBE is able to update the linkage values for each i-period. It is left to the OEM/supplier, when the values are updated. The updated values	Linkage values are updated by hashing the linkage seed value (which is a CRL entry, a hash or a repeated hash of the CRL entry) and then recalculating the linkage value.	On-board Equipment (OBE)

Key	Status	Summary	Description	justification	notes	Component/s
			or remove the linkage value.	are needed when a new i-period starts.	This is out of scope since it defines OBE's behavior.	
SCMS-1220	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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)
SCMS-1222	SCMS PoC out of Scope	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 is also conform 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	SCMS PoC out of Scope	EE checks against CRL for all	EEs shall check all received	EEs also check all relevant certificates, i.e.	These checks are specified in IEEE 1609.2.	On-board Equipment (OBE), Road-

Key	Status	Summary	Description	justification	notes	Component/s
		certificate types	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.	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.	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, 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.	side Equipment (RSE)
SCMS-1224	SCMS PoC out of Scope	EE stops sending	EE shall stop sending over-the-air DSRC messages, if it detects that	If certificates of a particular PSID/SSP have been revoked, EE stops sending all	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side

Key	Status	Summary	Description	justification	notes	Component/s
			itself has been listed on the CRL. This is limited to the certificates of the PSID/SSP that was revoked.	messages related to that PSID/SSP. EE might still receive DSRC messages, and send messages related to other non-revoked PSID/SSPs.		Equipment (RSE)
SCMS-1285	SCMS PoC out of Scope	EE stops sending: revoked ECA for EE's enrollment certificate	EE shall stop sending over-the-air messages, if it detects (via CRL) that it is 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	SCMS PoC out of Scope	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)

2.2.11 Use Case 11: Backend Management

Target release	Release 1.0
Document owner	Brian Romansky
Reviewer	Benedikt Brecht

2.2.11.1 Goals

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

2.2.11.2 Background and strategic fit

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

This includes Root CAs. For the PoC there will 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, for example, 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 Roots CAs.

2.2.11.3 Assumptions

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

2.2.11.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-406	In Implementation	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	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	CRL Store, CRLG, DCM, ECA, IBLM, LA, MA, PCA, PG, RA

			the suite: TLS_ECDHE_ECDSA_WITH_AES_128_CCM (as defined in RFC7251)		Publication 800-57 Part 1 Rev. 3, 07/2012".	
SCMS-407	Tests passed	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 revocation. See https://jira.camplc.org/browse/SCMS-406~~SCMS-406~~ for information about the cipher suite, SCMS-1016 for information about OCSP, and https://jira.camplc.org/browse/SCMS-938~~SCMS-938~~ for TLS certificate management.	CRL Store, CRLG, DCM, ECA, IBLM, LA, MA, PCA, PG, RA
SCMS-1017	SCMS PoC out of Scope	Robustness against catastrophic failure of the components	The SCMS components must 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	For PoC only minimal robustness is required. This requirement is for the production system.	

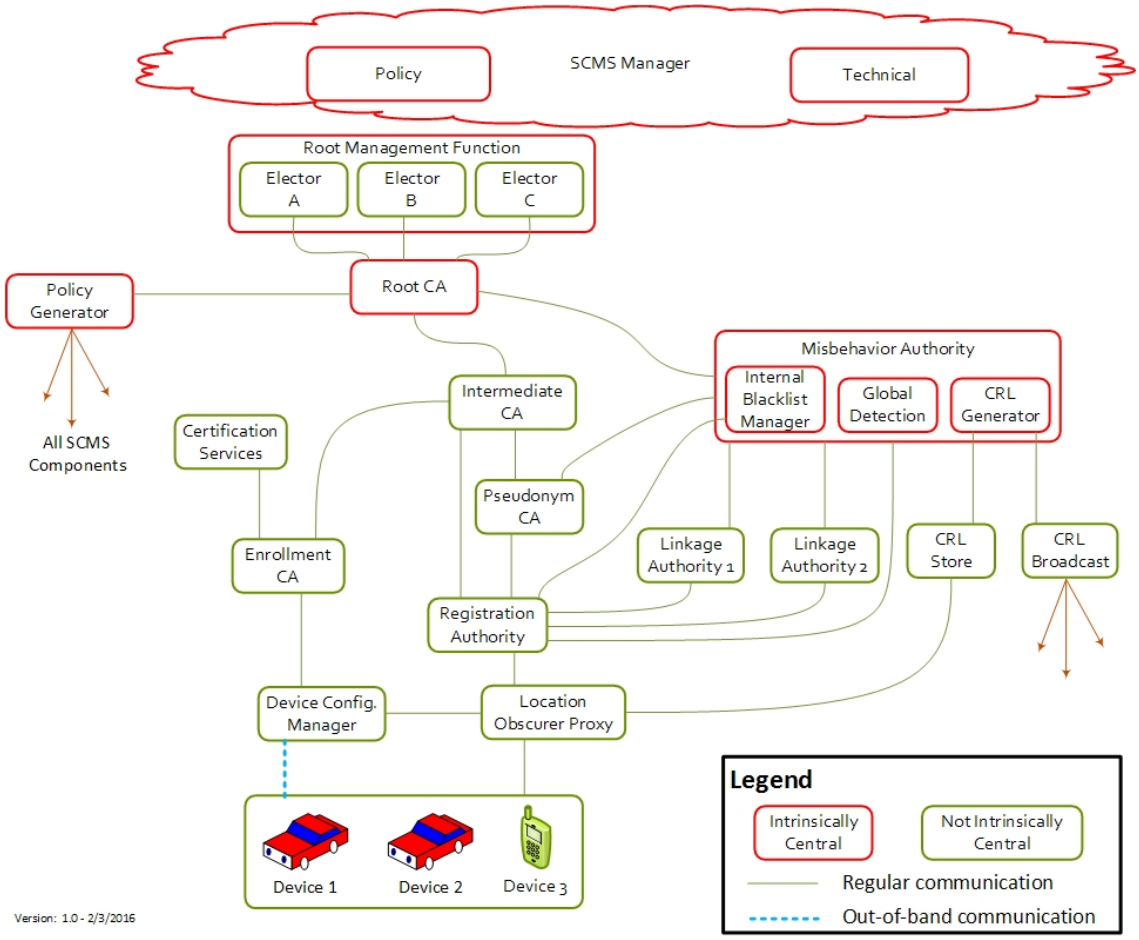
				production system.		
SCMS-1018	SCMS PoC out of Scope	Data encryption in geographically diverse locations	Databases should be encrypted and authenticated before sent to geographically diverse locations.	so that no unauthorized entity can gain access to the data.	For PoC only minimal robustness is required. 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 authenticated backups, as well as any operational secrets.	so that backups can be used for recovery when necessary.	For PoC only minimal robustness is required. This requirement is for the production system.	
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	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.	

			HSMs and reconstruct production materials from backup.			
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	Tests passed	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 CA management messages, the Root CA must be trusted, and therefore require that their Certificates be in the SCMS component trust stores.		CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA
SCMS-1314	Manual Process	SCMS component certificate types (implicit vs. explicit)	All SCMS component certificates shall be implicit, except for the following, which are explicit: PCA, ICA, Root CA,	PCA, ICA, Root CA, and elector certificates need to be of explicit type in order to support P2P distribution. All other SCMS component certificates could		CRL Store, CRLG, DCM, IBLM, ICA, LA, PCA, PG, RA, RCA

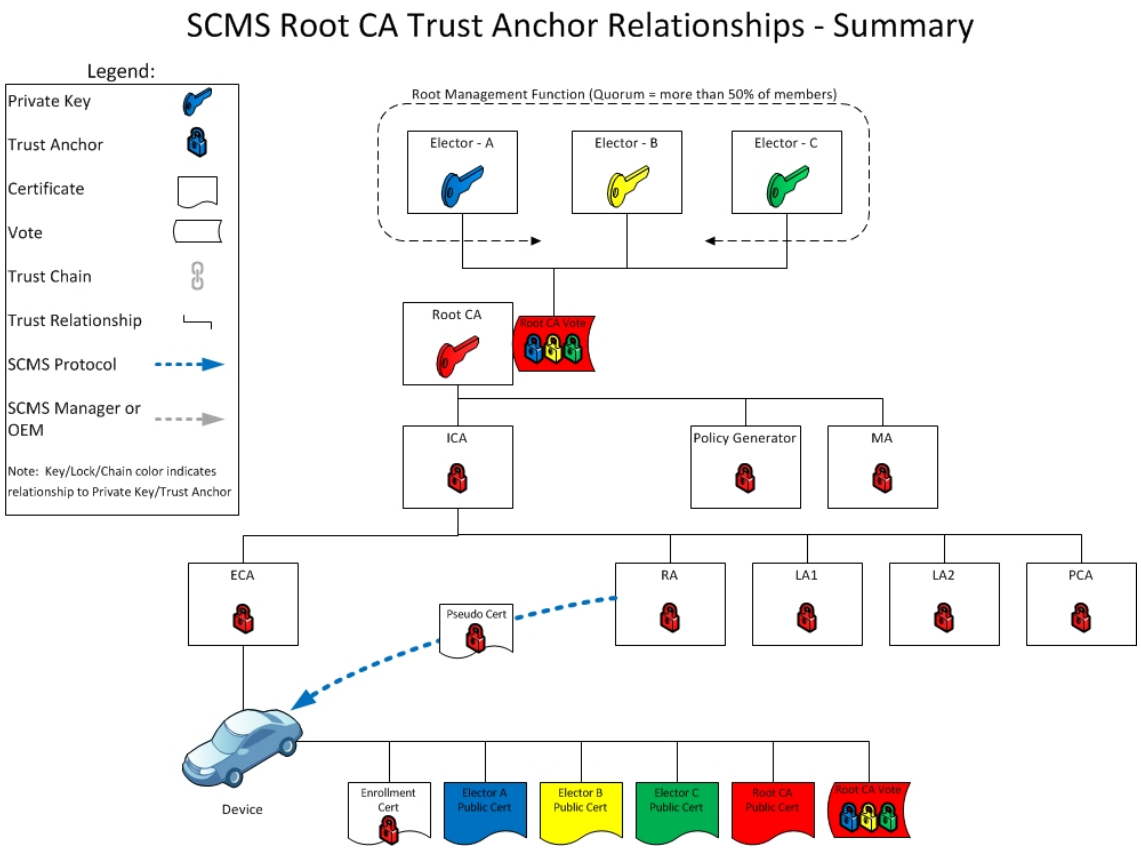
			and elector certificate.	be either implicit or explicit, and are selected as implicit for performance reasons.		
SCMS-1315	Review	Only 1 certificate valid at a time	Each SCMS component shall have only 1 valid and in-use certificate at a time.	There are no privacy concerns for SCMS components that would 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

2.2.11.5

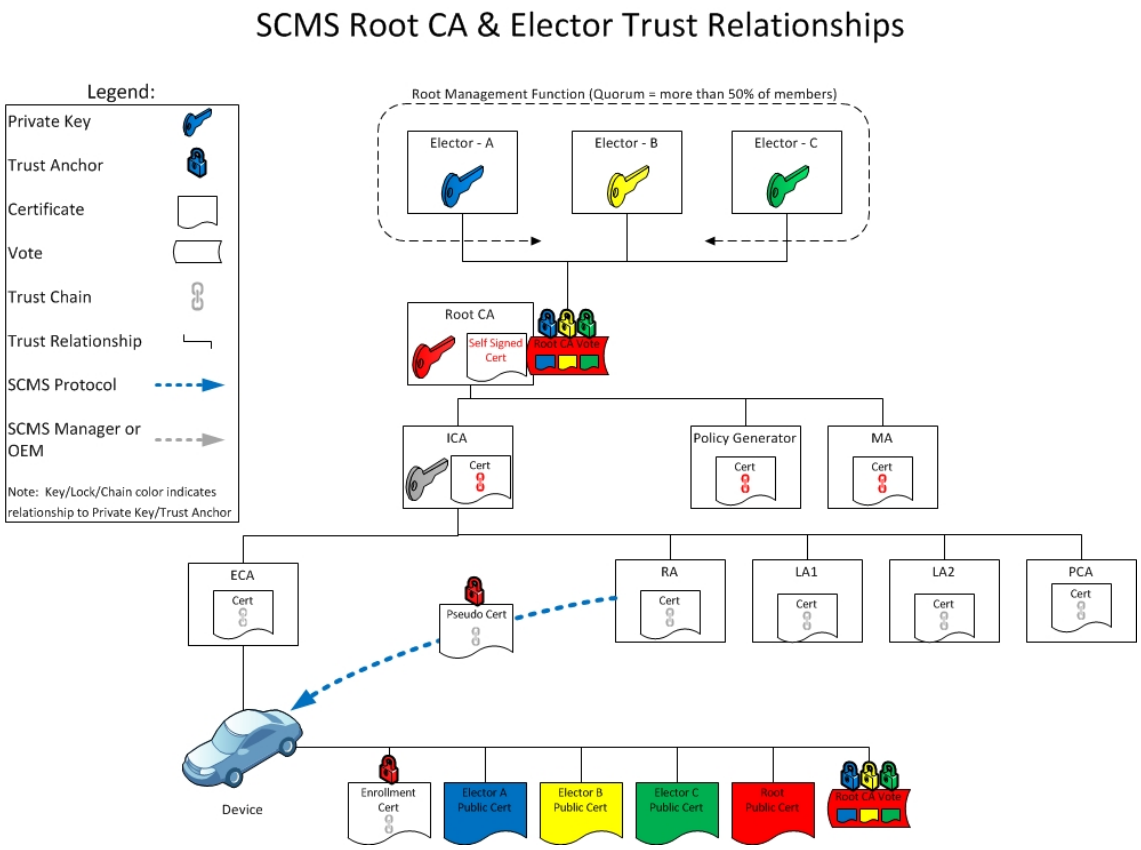
Design



2.2.11.6 Summary showing Trust Anchor relationships only.

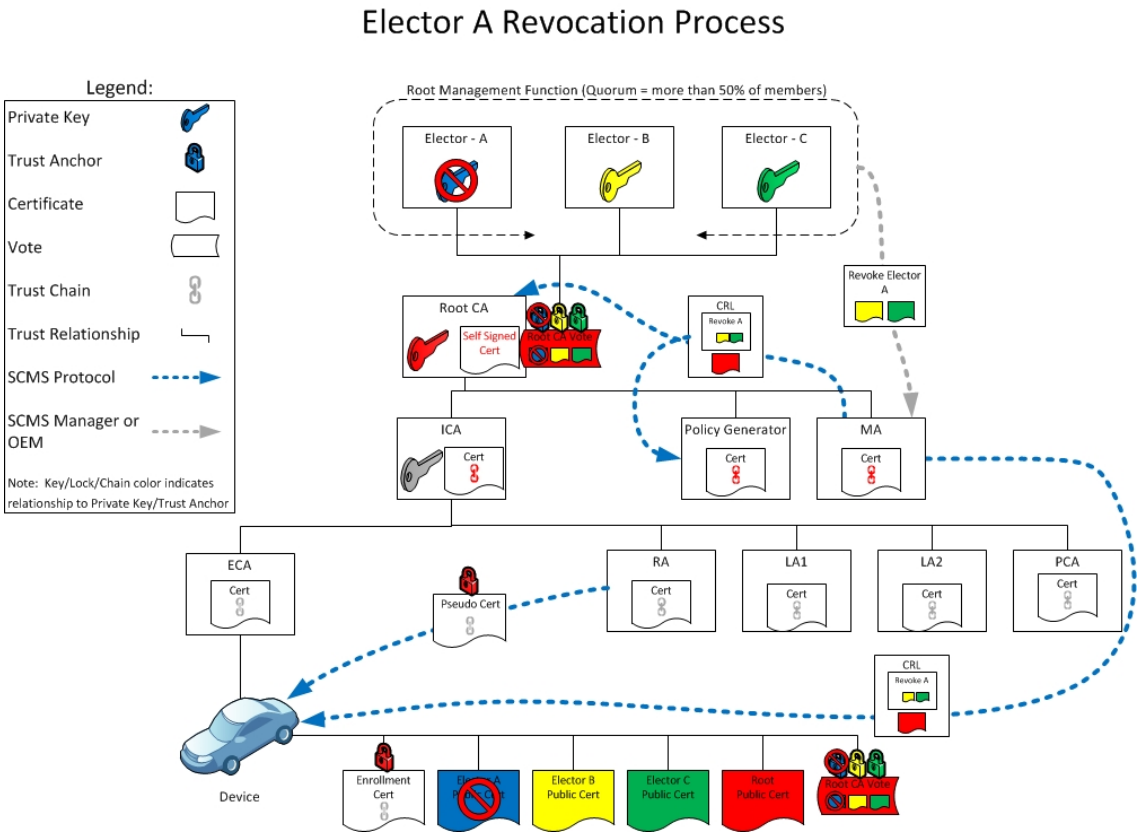


2.2.11.7 Day 1: Typical SCMS System Operations

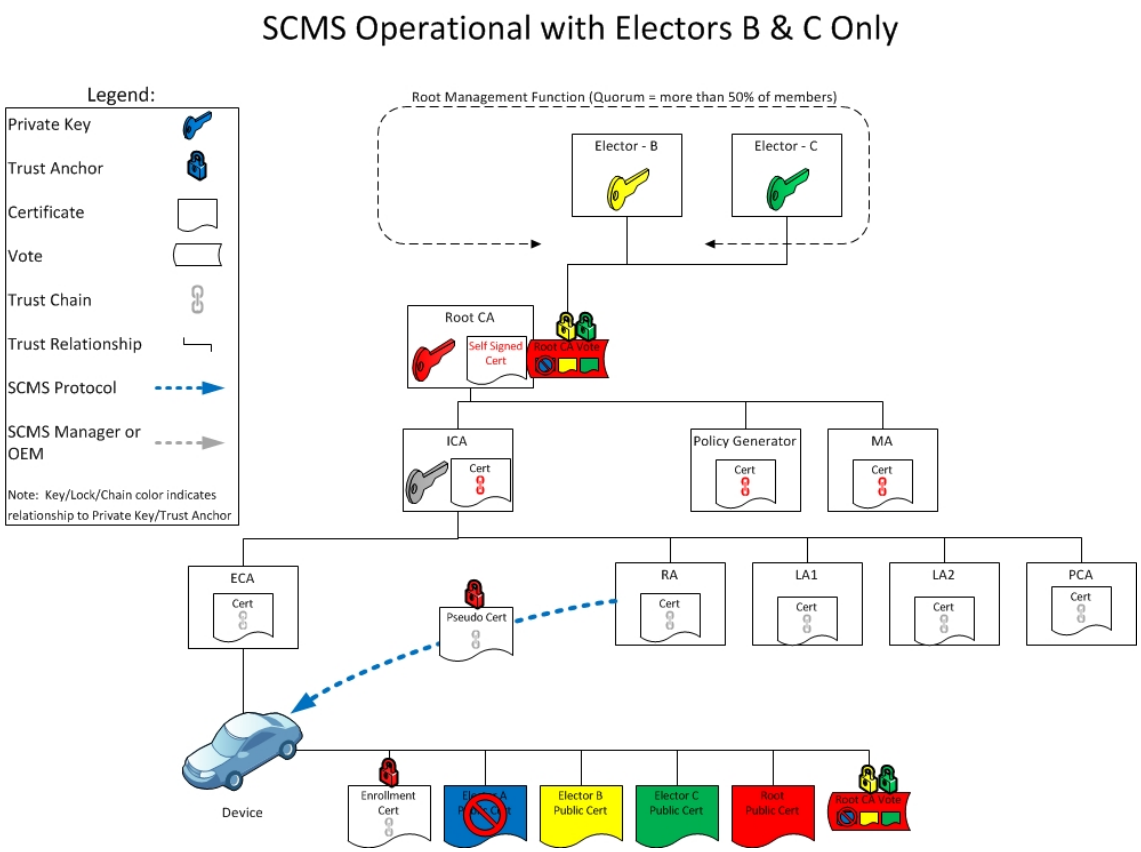


2.2.11.8 Life cycle of Elector (Level 0) revocation and replacement.

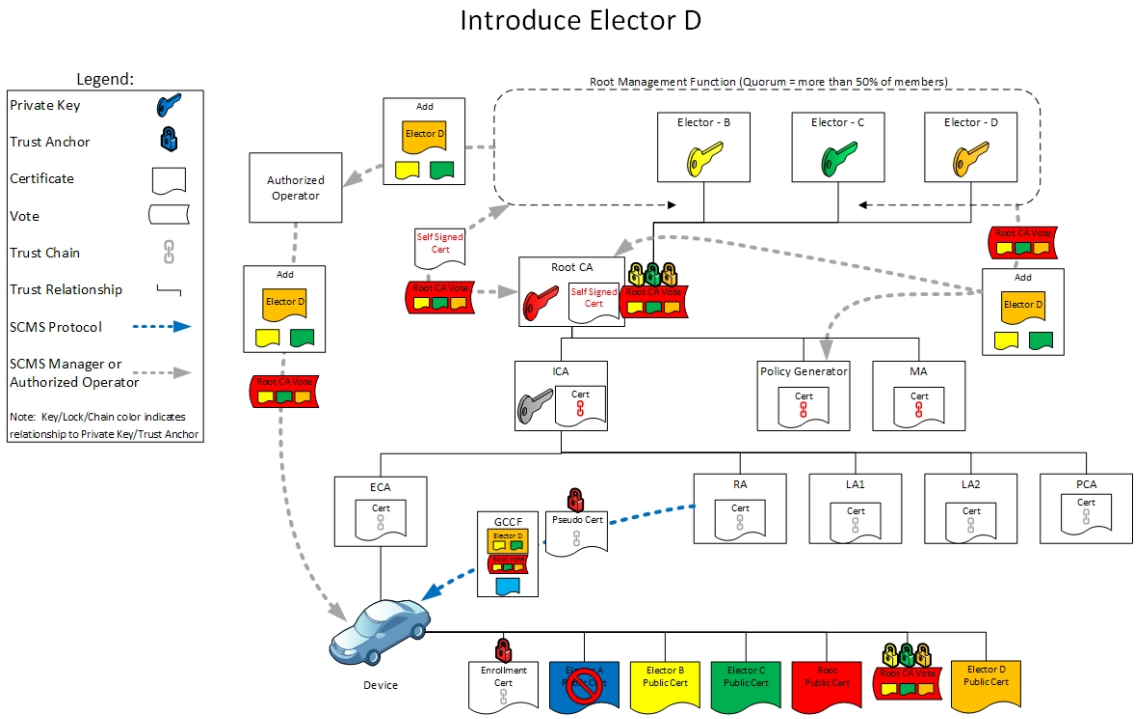
2.2.11.8.1 Day 2: Process to Revoke an Elector while maintaining functionality.



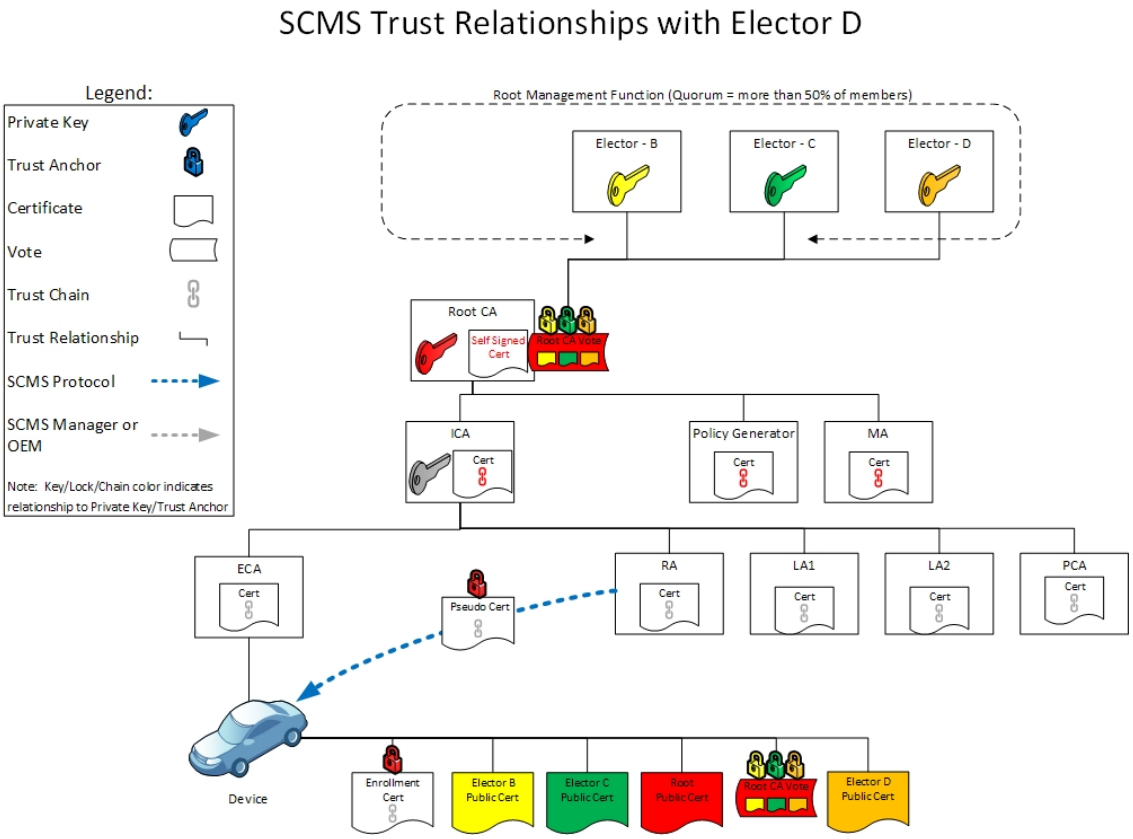
2.2.11.8.2 Day 3: System functional for period of time with two Root Endorsers.



2.2.11.8.3 Day 4: Introduction of Replacement Elector.

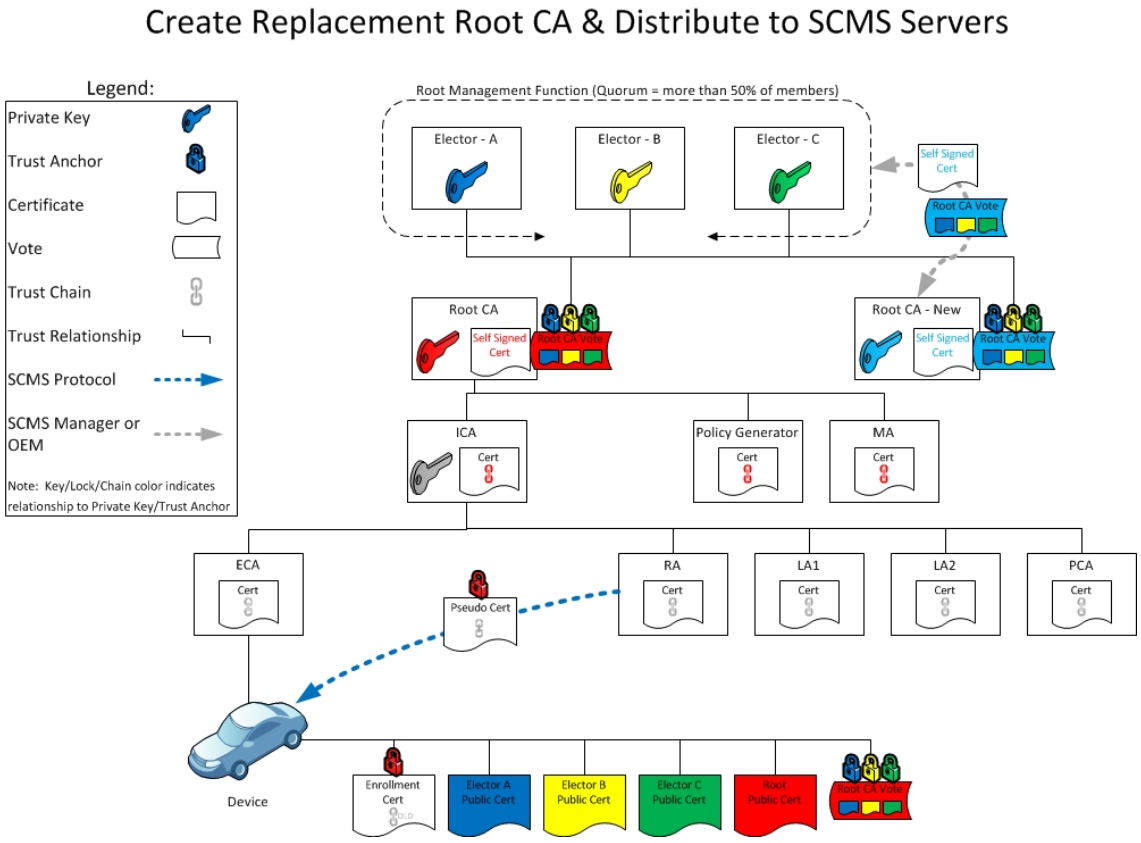


2.2.11.8.4 Day 5: Steady state operations after introduction of Replacement Elector

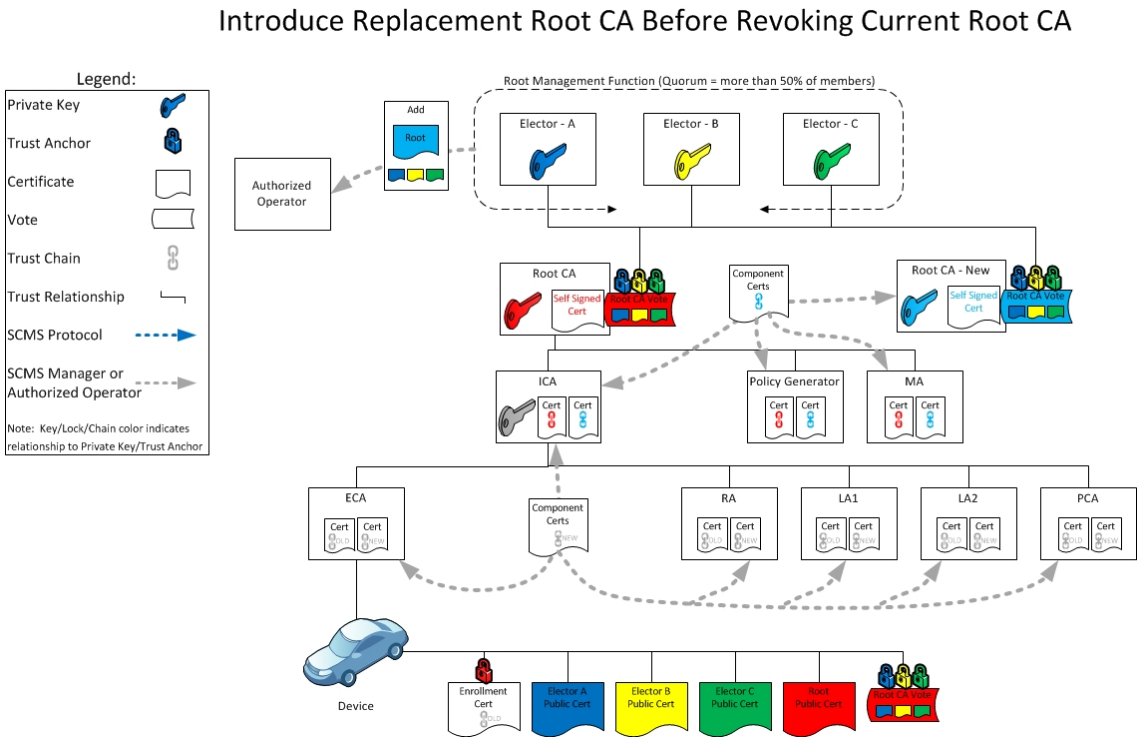


2.2.11.9 Life cycle of Root CA (Level 1) revocation and replacement.

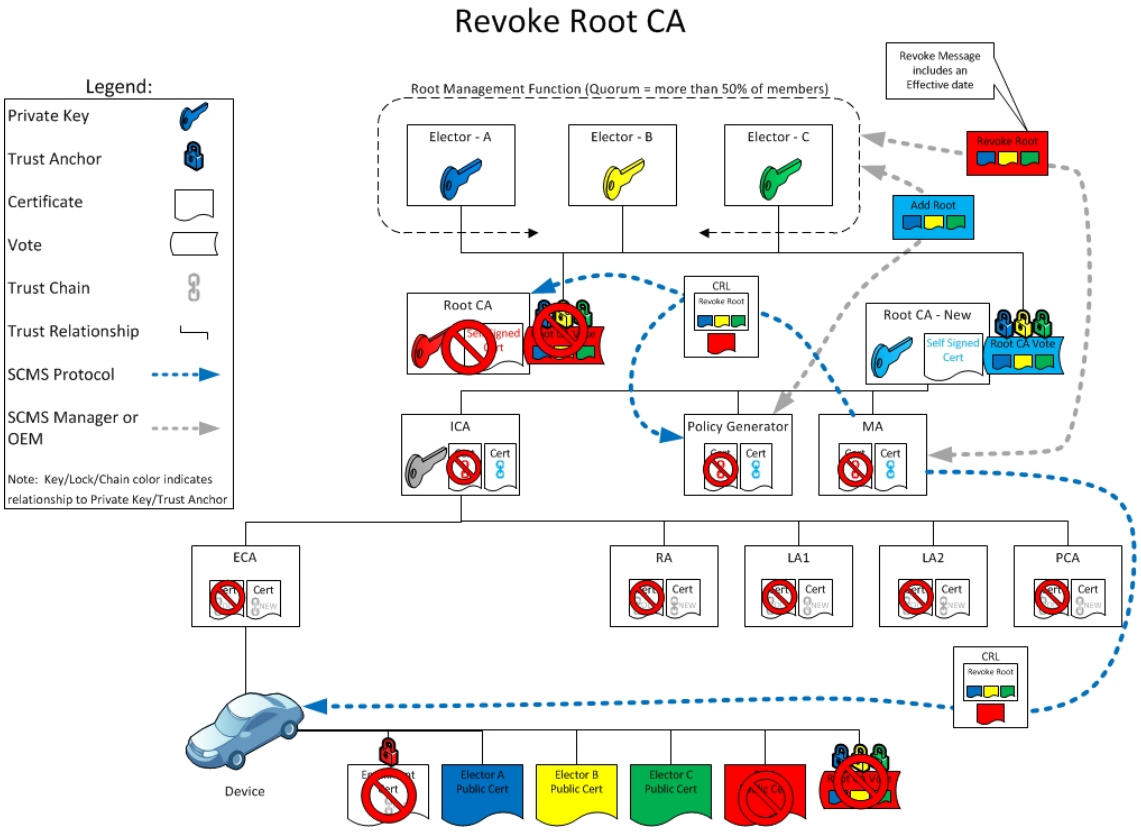
2.2.11.9.1 Day 2: Prepare New Root CA.



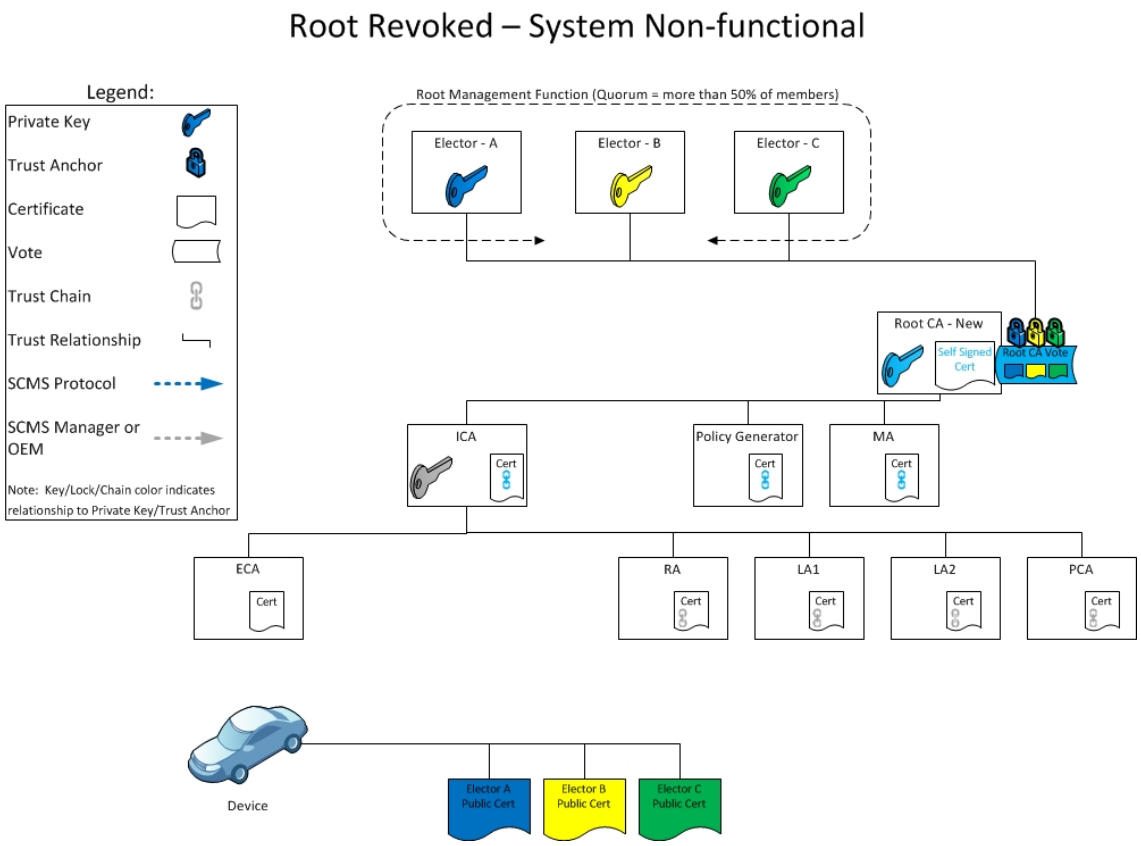
2.2.11.9.2 Day 3: Generate new certificates for all SCMS components & distribute.



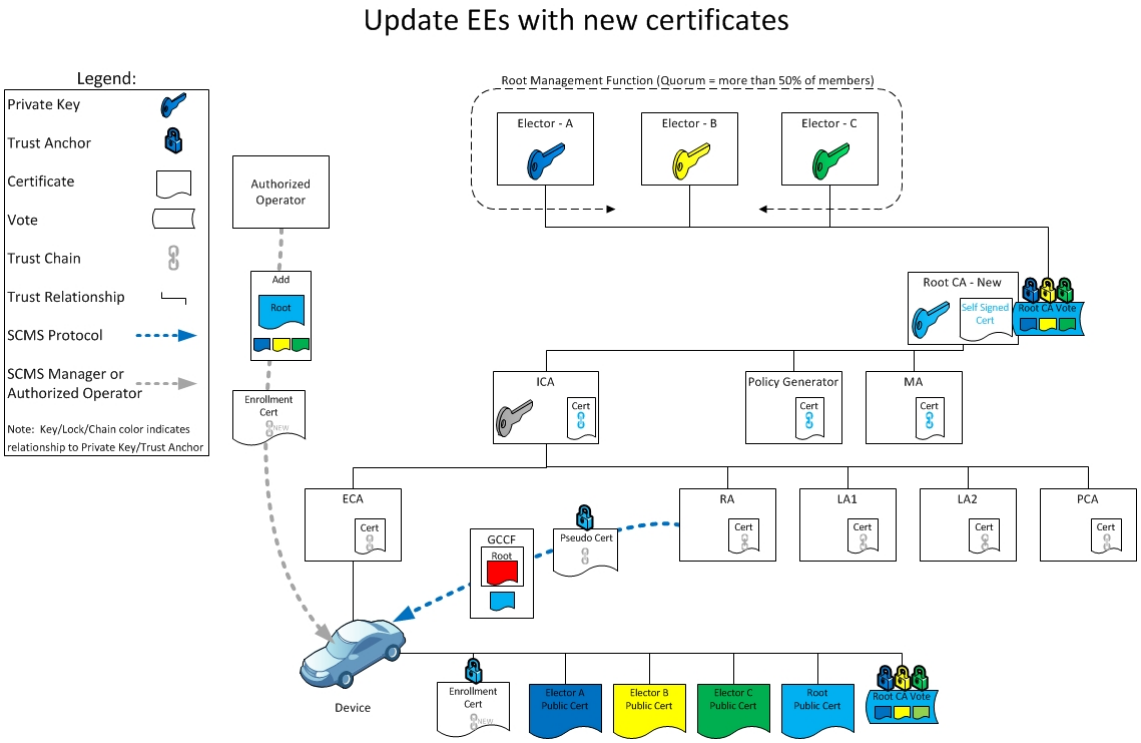
2.2.11.9.3 Day 4: Revoke Root CA.



2.2.11.9.4 Day 5: Condition of SCMS while Root CA is revoked.



2.2.11.9.5 Day 6: EEs updated with new Root certificate, new Enrollment certificate and new Pseudonym certificates.



2.2.11.10 Step 11.1: Add SCMS component

Target release	Release 1.0
Document owner	Brian Romansky
Reviewer	Jeff Hahn

2.2.11.10.1Goals

The collection of "Add" use cases describe the procedures for adding back-end 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.

2.2.11.10.2Conditions

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.

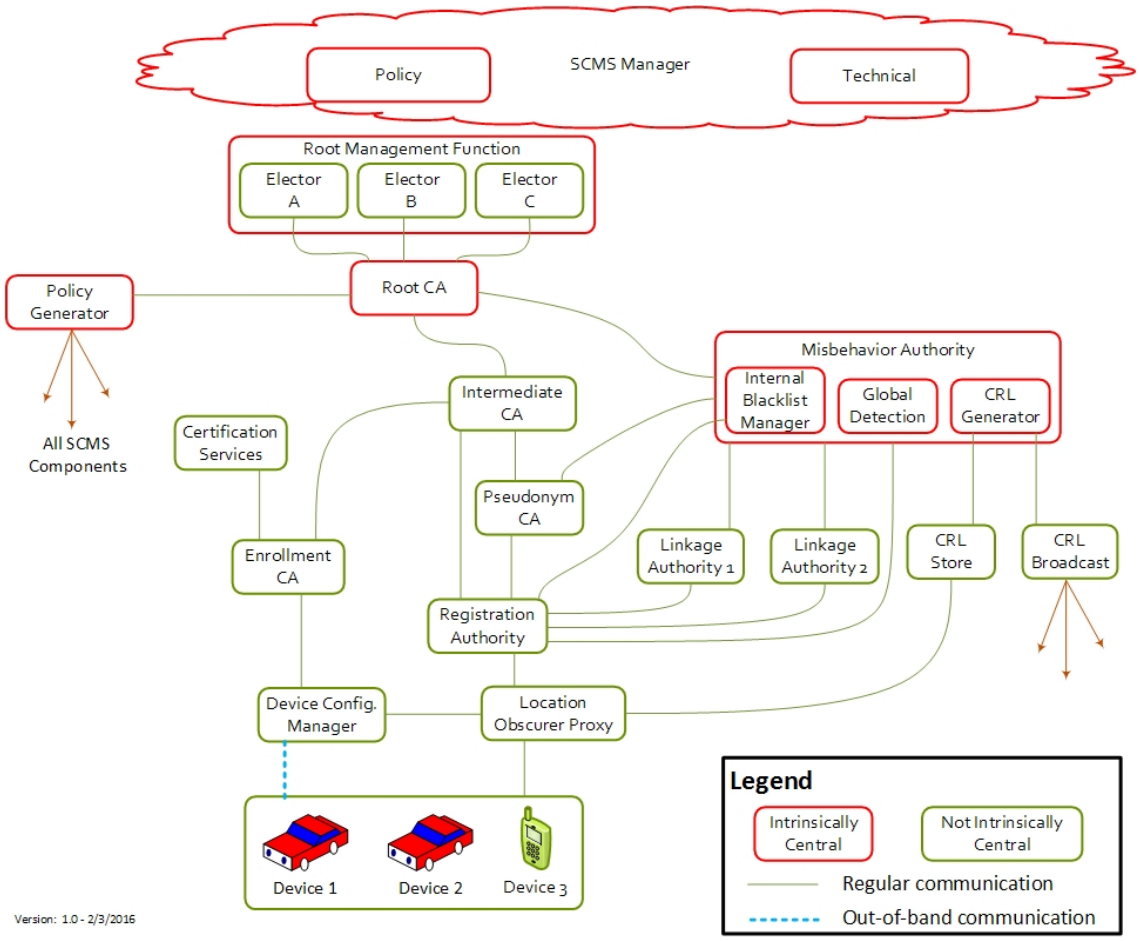
1. Net New

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.

2.2.11.10.3Design



2.2.11.10.4Assumptions

- 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 is to preserve the security and integrity of the SCMS system and ensure compatibility among individual SCMS components while granting significant latitude for diverse implementations.

2.2.11.10.5Step 11.1.1 - Add CRLG (Use Case)

Target release	Release 1.0
Document owner	Brian Romansky
Reviewer	

2.2.11.10.5.1 Goals

The CRL Generator (CRLG) is a 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.

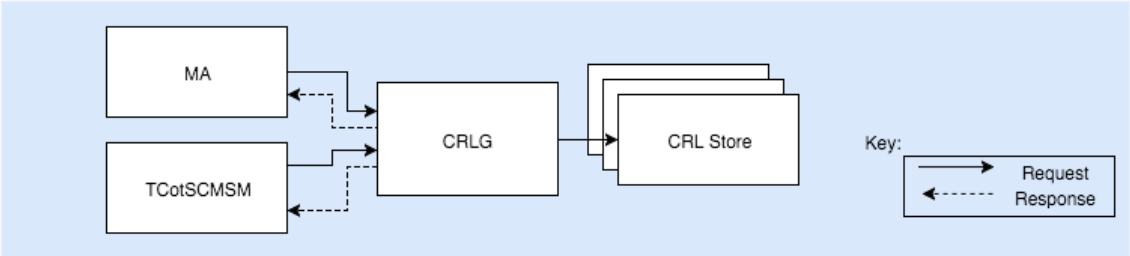
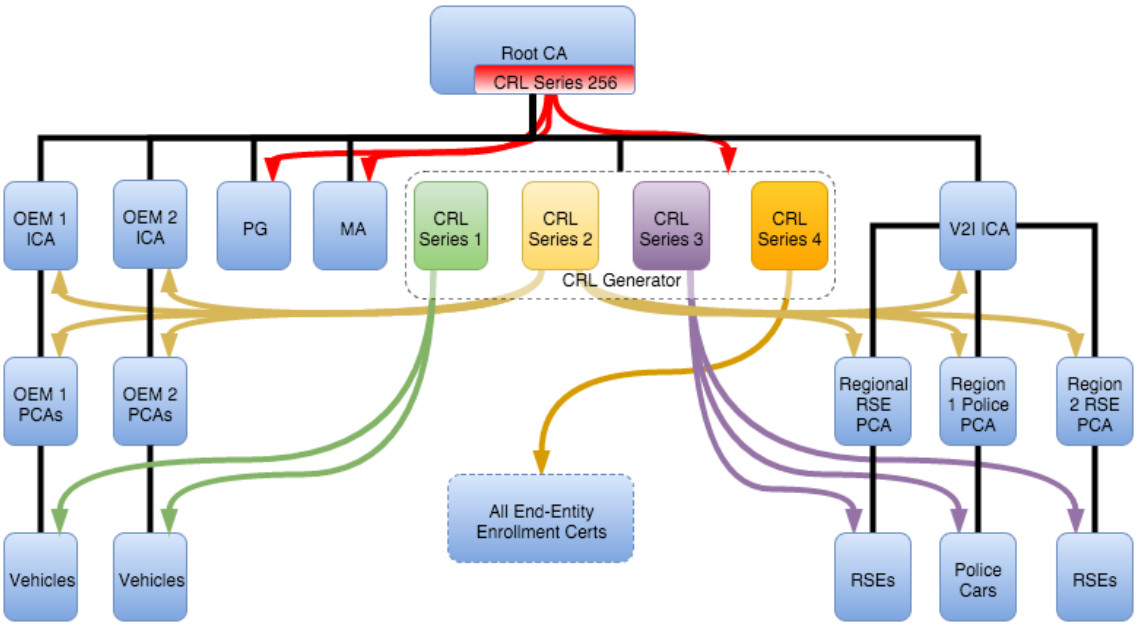


Figure 1: CRLG messaging

Figure 1 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 Store.

2.2.11.10.5.2 CRL Series

This is the CRL series diagram for POC / Pilot Deployments. We anticipate that in the future there may be local CRLGs hanging off various CAs within the V2I ICA hierarchy. Introducing a new CRLG, and assigning new certs to it, can be done without requiring any change in the existing CRLG certs, although it is obviously impossible to transfer already-issued certs from one CRLG to another.



2.2.11.10.5.3 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 Store.

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

- The FQDN and TLS certificate of one or more CRL Store.
- The TLS certificate of the MA
- 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:

- The FQDN and TLS certificate of the CRLG.

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

- The TLS certificate of the CRLG.

2.2.11.10.5.3.1 End State

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

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:

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:

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.

2.2.11.10.5.3.2 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).

2.2.11.10.5.4 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.

2.2.11.10.5.5 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-774	Manual Process	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

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1412	SCMS PoC out of Scope	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, RCA
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	Review	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, LA, MA, PG, RA

2.2.11.10.6Step 11.1.1 - Add ECA (Use Case)

Target release	Release 1.0
Document owner	Brian Romansky
Reviewer	Benedikt Brecht

2.2.11.10.6.1 Goals

The Enrollment Certificate Authority (ECA) is an SCMS back-end 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.

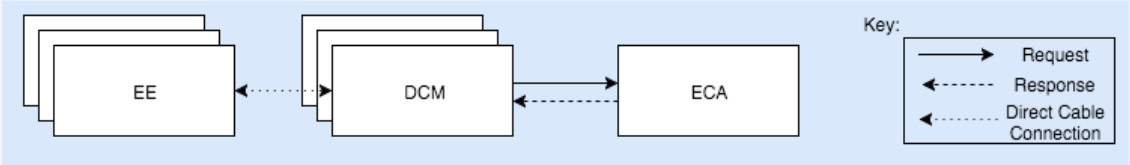


Figure 1: ECA messaging

Figure 1 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.

2.2.11.10.6.2 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:

- The FQDN of the new ECA and the ECA's TLS certificate

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

2.2.11.10.6.2.1 End State

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

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:

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

2.2.11.10.6.2.2 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 (Use Case)

2.2.11.10.6.3 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.

2.2.11.10.6.4 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	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

Key	Status	Summary	Description	justification	notes	Component/s
			SCMS identity certificate.			
SCMS-774	Manual Process	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 the ECA of the DCMs with which it will communicate.			TCotSCMSM
SCMS-1386	Manual Process	Add component's	The TCotSCMSM	For a newly added	In the PoC, this will occur by a	TCotSCMSM

Key	Status	Summary	Description	justification	notes	Component/s
		certificate to GCCF	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).	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.	manual process.	
SCMS-1412	SCMS PoC out of Scope	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, RCA
SCMS-1591	Manual Process	ECA certificate validity	ECA shall request an ECA certificate with a validity of 40 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	Use 3.5 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
			period of 3.5 years.		policy. This is for CV-Pilot only.	
SCMS-1605	Review	ECA certificate validity	ECA shall request an ECA certificate with a validity of 7 years.	To support issuing of subordinate certificates.	This is for CV-Pilot only.	ECA

2.2.11.10.7Step 11.1.1 - Add ICA (Use Case)

Target release	Release 1.0
Document owner	Brian Romansky
Reviewer	Benedikt Brecht

2.2.11.10.7.1 Goals

The Intermediate Certificate Authority (ICA) is a non-central, back-end 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.

2.2.11.10.7.2 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.

2.2.11.10.7.2.1 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 issued certificates by the ICA will make the ICA certificate available to recipients of their messages when required.

2.2.11.10.7.2.2 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.

2.2.11.10.7.2.3 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 (Use Case)

2.2.11.10.7.3 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-715	Manual Process	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 it should	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

Key	Status	Summary	Description	justification	notes	Component/s
			use in order to obtain its SCMS identity certificate.			
SCMS-774	Manual Process	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	SCMS PoC out of Scope	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, MA, PCA, PG, RA, RCA

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.			
SCMS-1596	Manual Process	ICA certificate validity	ICA shall request an ICA certificate with a validity of 50 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 10 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-1603	Manual Process	ICA certificate validity	ICA shall request an ICA certificate with a validity of 11 years.	To support issuing of subordinate certificates.	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 an in-use period of 7 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 CV-Pilot only.	ICA

2.2.11.10.8Step 11.1.1 - Add MA (Use Case)

Target release	Release 1.0
Document owner	Brian Romansky
Reviewer	Benedikt Brecht

2.2.11.10.8.1 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.

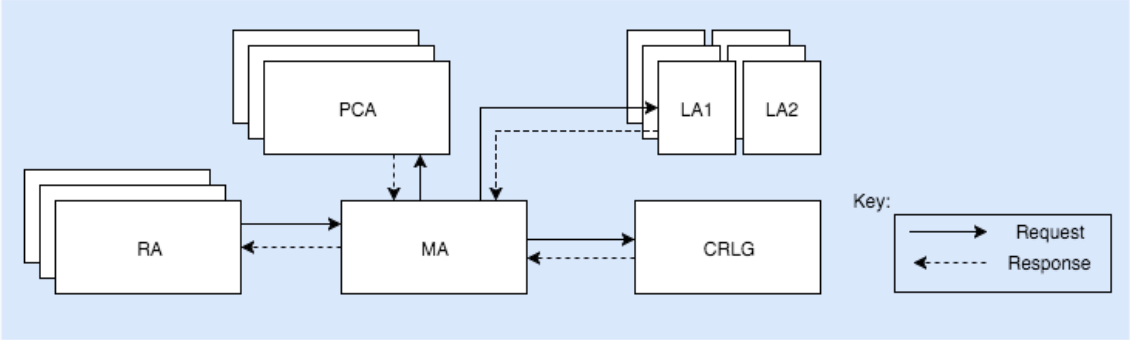


Figure 1: MA messaging

Figure 1 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.

2.2.11.10.8.2 Procedure

The addition of an MA requires that all components that communicate with it be properly configured to interact with the new MA.

2.2.11.10.8.2.1 End States

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

RA Value	Notes
MA FQDN and TLS certificate	Each RA must be able to establish a secure connection to the MA

RA Value	Notes
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:

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).

2.2.11.10.8.3 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-715	Manual Process	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-769	Manual Process	TCotSCMSM add MA	The TCotSCMSM shall inform DCMs about a recently added MA.	so that DCMs use the new MA to configure devices during bootstrapping.		TCotSCMSM

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 it should use 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	Manual Process	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-1047	SCMS PoC out of Scope	Error code: tcNotifyDCMListFailure	TCotSCMSM shall log "Error code: tcNotifyDCMListFailure", if the TCotSCMSM fails to notify the MA of the list of DCMs			TCotSCMSM
SCMS-1048	SCMS PoC out of Scope	Error code: tcNotifyDCMAuthenticationFailure	TCotSCMSM shall log "Error code: tcNotifyDCMA			TCotSCMSM

Key	Status	Summary	Description	justification	notes	Component/s
			uthenticationFailure", if the TCotSCMSM cannot authenticate to the MA when trying to notify it of DCMs			
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	SCMS PoC out of Scope	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, RCA

Key	Status	Summary	Description	justification	notes	Component/s
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	Review	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, LA, MA, PG, RA

2.2.11.10.9Step 11.1.1 - Add PCA (Use Case)

Target release	Release 1.0
Document owner	Brian Romansky
Reviewer	Benedikt Brecht

2.2.11.10.9.1 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.

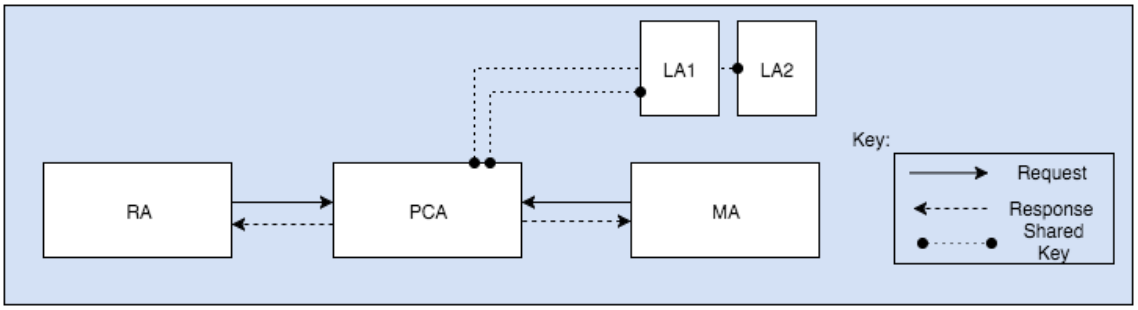


Figure 1: PCA messaging

Figure 1 shows that the PCA responds to requests from both the RA and the MA. It also requires shared symmetric encryption/decryption keys that are stored in the pair of LAs that are assigned to the PCA although there is no direct communication between the PCA and the LAs. 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.

2.2.11.10.9.2 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.

2.2.11.10.9.2.1 End States

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

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, MA will have the following information:

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:

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

2.2.11.10.9.2.2 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.

2.2.11.10.9.3 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-244	Manual Process	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	Manual Process	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	TCotSCMSM

Key	Status	Summary	Description	justification	notes	Component/s
					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 it should use 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	Manual Process	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	For a newly added component to be a valid SCMS component, its certificate must chain back to the SCMS Root CA	In the PoC, this will occur by a manual process.	TCotSCMSM

Key	Status	Summary	Description	justification	notes	Component/s
			certificate of the newly created SCMS component to the Global Certificate Chain File (GCCF).	and its chain must be available to any other component via GCCF.		
SCMS-1412	SCMS PoC out of Scope	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, RCA
SCMS-1594	Manual Process	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 & CV-Pilot 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

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1806	Review	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 the 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 component. It is expected (but not required) that a PCA, RA, and pair of LAs will typically be added as a complete set.	MA, TCotSCMSM

2.2.11.10.10 Step 11.1.1 - Add PG (Use Case)

Target release	Release 1.1
Document owner	Brian Romansky
Reviewer	

2.2.11.10.10.1 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.

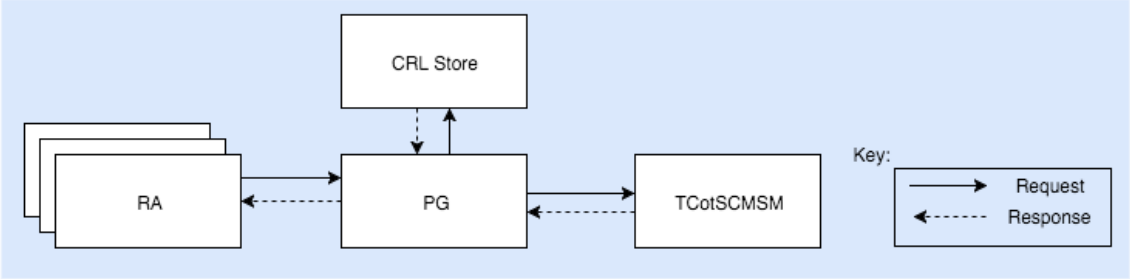


Figure 1: PG messaging

Figure 1 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.

2.2.11.10.10.2 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.

2.2.11.10.10.2.1 End State

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

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.

2.2.11.10.10.2.2 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).

2.2.11.10.10.3 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.

2.2.11.10.10.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-715	Manual Process	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	TCotSCMSM

Key	Status	Summary	Description	justification	notes	Component/s
					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 it should use 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	Manual Process	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	For a newly added component to be a valid SCMS component, its	In the PoC, this will occur by a manual process.	TCotSCMSM

Key	Status	Summary	Description	justification	notes	Component/s
			the Policy Generator in order to add the certificate of the newly created SCMS component to the Global Certificate Chain File (GCCF).	certificate must chain back to the SCMS Root CA and its chain must be available to any other component via GCCF.		
SCMS-1412	SCMS PoC out of Scope	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, RCA
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	Review	Component certificate FQDN match	The SCMS component shall have a certificate with a certificateId field that	FQDN of each component must match the official ID of the component.		CRLG, DCM, LA, MA, PG, RA

Key	Status	Summary	Description	justification	notes	Component/s
			matches the FQDN of the component.			

2.2.11.10.11 Step 11.1.1 - Add RA (Use Case)

Target release	Release 1.0
Document owner	Brian Romansky
Reviewer	Benedikt Brecht

2.2.11.10.11.1 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.

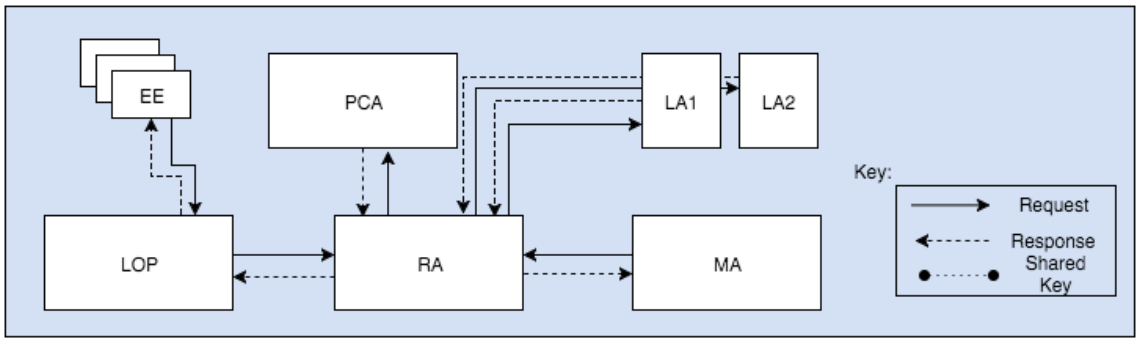


Figure 1: RA messaging

Figure 1 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.

2.2.11.10.11.2 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:

1. The MA must be updated with the 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.
2. The RA must be informed of the FQDN of the PCA.
3. The RA must be informed of the FQDNs of both LAs and their LA IDs.
4. The RA must be provided with at 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.

2.2.11.10.11.2.1End State

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

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:

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.

2.2.11.10.11.2.2Special 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 bring 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.

2.2.11.10.11.3 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-264	Manual Process	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	Manual Process	Provide Elector Certificates	The TCotSCMSM shall provision all SMCMS components with the self-signed	Root Management messages require signatures from the Electors to be validated, so authentic Root	When receiving Root Management messages through the GCCF or LCCF, the authenticity	TCotSCMSM

Key	Status	Summary	Description	justification	notes	Component/s
			certificates of all electors that are valid at the time of the component setup.	CA Certificates are also required.	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.	
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 it should use 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	Manual Process	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.	TCotSCMSM

Key	Status	Summary	Description	justification	notes	Component/s
					In the PoC, this will occur by a manual process.	
SCMS-1049	Review	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

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1412	SCMS PoC out of Scope	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, RCA
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	Review	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, LA, MA, PG, RA
SCMS-1806	Review	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	The MA must know about all PCAs, LAs, and RAs in the system so that it can execute misbehavior investigations	In the PoC, this will occur by a manual process. When a new PCA, LA, or RA is added, the local ICA manager will	MA, TCotSCMSM

Key	Status	Summary	Description	justification	notes	Component/s
			any newly added PCA, LA, or RA.	and revocation procedures.	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 component. It is expected (but not required) that a PCA, RA, and pair of LAs will typically be added as a complete set.	

2.2.11.10.12 Step 11.1.2: Add Root CA (Use Case)

Target release	Release 1.1
Document owner	Brian Romansky
Reviewer	Benedikt Brecht

2.2.11.10.12.1 Goals

- Define the procedures and requirements to add and manage Root CA certificates in the SCMS.

2.2.11.10.12.2 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 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.

2.2.11.10.12.3 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:

- 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.
- 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.
- 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. RAs will be required to include all root 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 root endorsement message 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 '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".

2.2.11.10.12.4 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.

2.2.11.10.12.5 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: Root Management and Revocation Recovery
- 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.

2.2.11.10.12.6 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	Review	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	SCMS PoC out of Scope	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 "Add Root CA" message. 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
			validation of this message shall be carried out securely in the EE's secure execution environment or HSM.			
SCMS-1094	Review	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	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		TCotSCMSM

Key	Status	Summary	Description	justification	notes	Component/s
			components and EEs to inform them of the new root CA.	management messages (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	Review	Root CA certificate validity	The Root CA certificate validity period shall be set to 70 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 (https://wiki.campllc.org/display/SP/Certificate+Types). This is for PoC & CV-Pilot only.	RCA
SCMS-1332	Review	Root CA certificate overlap	Root CA certificates shall have an overlap of 50 years (an in-use period of 20 years).	The overlap is necessary to allow rollover.	This is for POC & CV-Pilot only.	RCA
SCMS-1409	Review	Elector Trust Store Messaging Processing	The SCMS Component shall be able to process the "Add Elector" and "Revoke	Every SCMS component will need to manage Elector updates automatically, so therefore every	For the PoC, the number of Electors will be 3, and the number of Electors required	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA

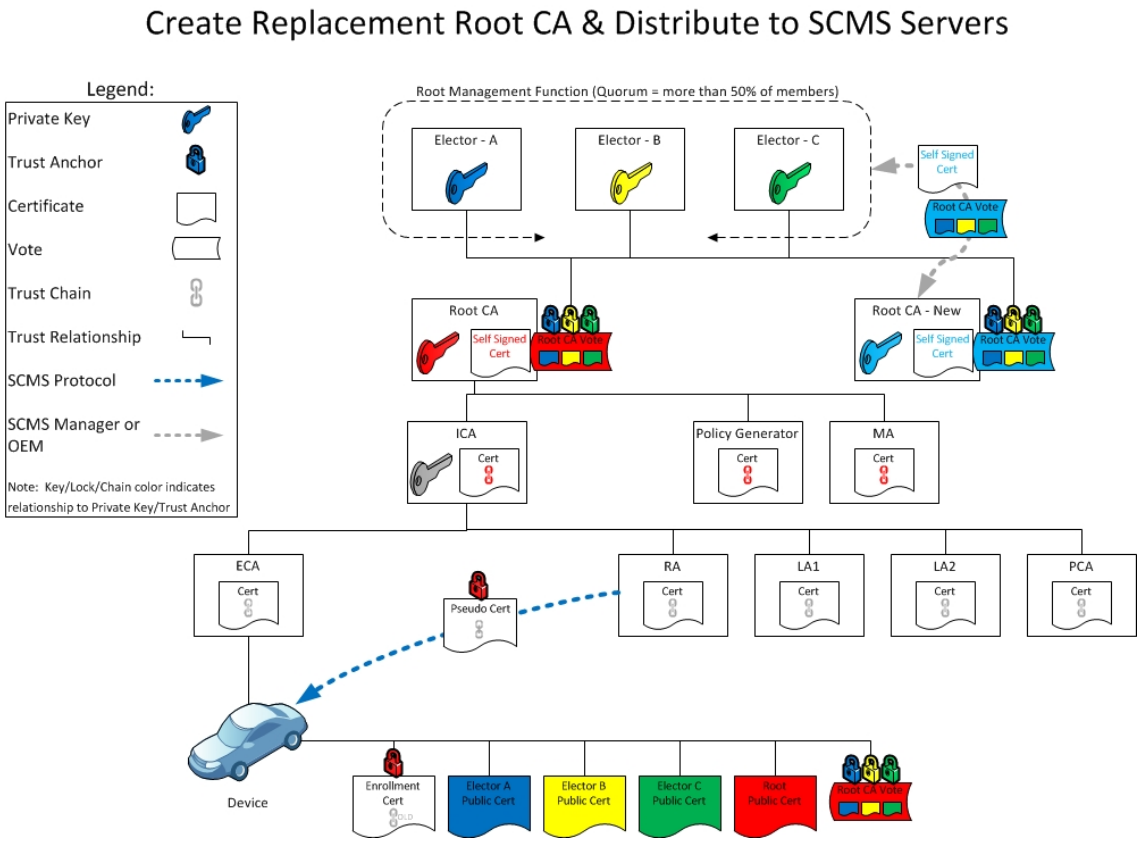
Key	Status	Summary	Description	justification	notes	Component/s
			Elector" messages, which will be signed by Electors, and shall ensure that the number of valid signatures is at least a quorum of non-revoked Electors in its trust store.	SCMS component will need to be able to process Root Management messages signed by the Electors.	to authorize any Root Management message will be 2. Elector signatures will be produced in a manual process for the PoC.	
SCMS-1412	SCMS PoC out of Scope	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, RCA
SCMS-1422	Manual Process	Renewal of component certificate	A SCMS component shall request rollover 1609 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 1609 certificates prior 3 months to the end of the In-use life of the	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

Key	Status	Summary	Description	justification	notes	Component/s
			current certificate.			

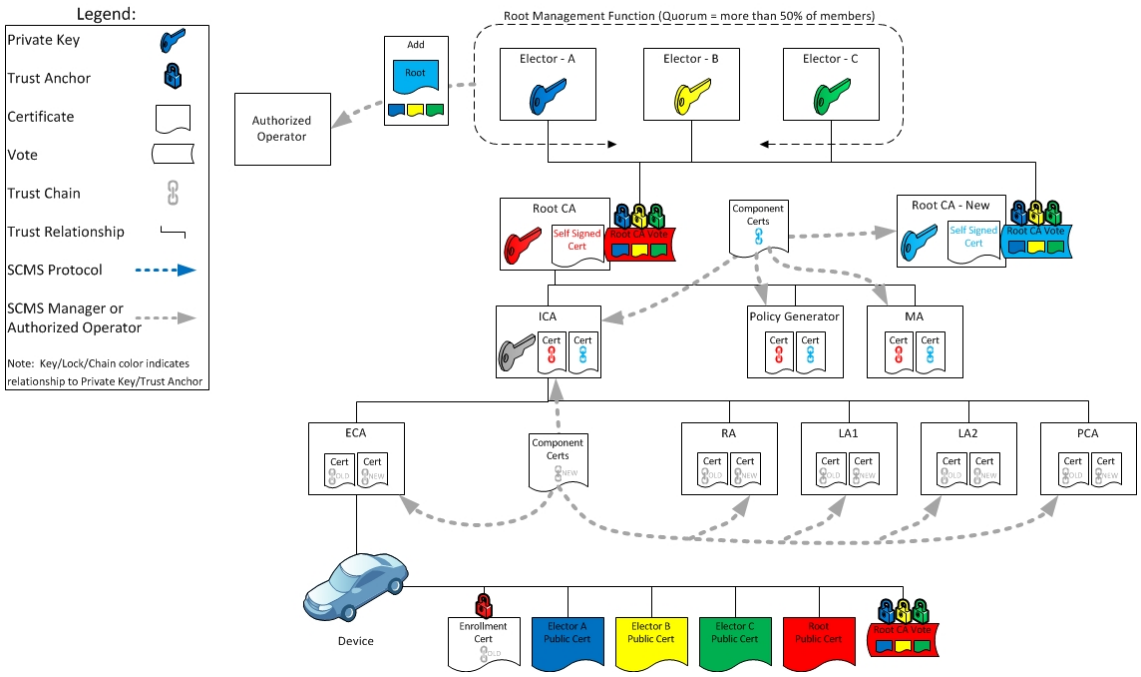
2.2.11.10.12.7 Design

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

2.2.11.10.12.8 Diagrams



Introduce Replacement Root CA Before Revoking Current Root CA



2.2.11.10.13 Step 11.1.3: Add Elector

Target release	Release 1.1
Document owner	Brian Romansky
Reviewer	Benedikt Brecht

2.2.11.10.13.1 Goals

- Define the procedures and requirements to add and manage root management Electors in the SCMS.

2.2.11.10.13.2 Background and Strategic Fit

Electors are a collection of highly trusted back-end 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).

2.2.11.10.13.3 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:

- In a secure environment, 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)
- 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.
- The complete elector 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 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 check to see if they have already added the new elector 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 '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".

2.2.11.10.13.4 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.

2.2.11.10.13.5 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1024	Review	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	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		TCotSCMSM

Key	Status	Summary	Description	justification	notes	Component/s
			(GCCF), which will be distributed to SCMS components, and EEs to inform them of the new Elector.	section for trust management messages (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.		
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 multiple signatures.	Specification of "Add Elector" message is needed (ASN.1). In the PoC this will message will be produced by a manual process. In the PoC, n is set to 3, and m is set to 2.	TCotSCMSM
SCMS-1384	SCMS PoC out of Scope	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	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)

Key	Status	Summary	Description	justification	notes	Component/s
			environment or HSM.			
SCMS-1385	Review	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 "Add Elector" message. The validation of this message shall be carried out securely in the component's HSM.	A quorum of Electors must authorize a new Elector		CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA
SCMS-1409	Review	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

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1412	SCMS PoC out of Scope	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, RCA
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	Manual Process	Renewal of component certificate	A SCMS component shall request rollover 1609 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 1609 certificates prior 3 months	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

Key	Status	Summary	Description	justification	notes	Component/s
			to the end of the In-use life of the current certificate.			
SCMS-1423	Manual Process	Elector Certificate Expiration	The Technical Component of the SCMS Manager (TCotSCMSM) shall issue Elector certificates with an expiration of 60 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 20 years, another one a certificate expiration of 40 years, to prevent multiple elector certificates from expiring at the same time. These durations are for the SCMS PoC & CV-Pilot only. For other SCMS instances, this duration should be reevaluated.	Elector
SCMS-1590	SCMS PoC out of Scope	Elector Certificate In-Use period	The Elector certificate In-Use period shall be the same as the	Out of scope as this needs to be implemented as operational policy.		Elector

Key	Status	Summary	Description	justification	notes	Component/s
			Expiration period.	To maintain a fixed number of valid Elector at all times.		
SCMS-1809	Review	Elector certificate validity	Elector certificates validity period shall be set to 60 years.	Elector certificates must have an expiration date.	Certificate types and expiration periods are defined in the Certificate Types common requirements section (https://wiki.camp llc.org/display/SP/Certificate+Types). The initial 3 elector certificates have an expiration and "in use" time of 20, 40 and 60 years, respectively. Currently, there is only 1 set of Electors for both V2V and V2I. This is for PoC & CV-Pilot only.	Elector

2.2.11.10.13.6 Design

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

2.2.11.11 Step 11.2: Revoke SCMS component

Target release	Release 1.0
Document owner	Brian Romansky
Reviewer	

2.2.11.11.1Goals

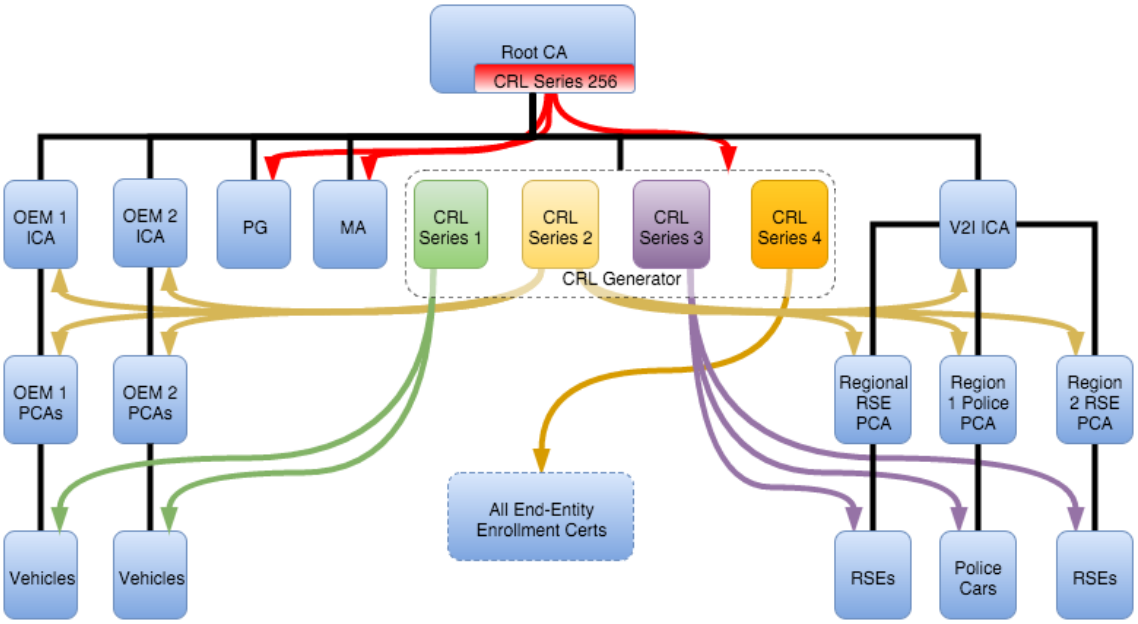
- Revoke procedure for each SCMS component

2.2.11.11.2Assumptions

- It will become necessary as the SCMS system evolves, that in the case of compromise or obsolescence, that components be revoked.
- Actual requirements will be outlined in subsections.

2.2.11.11.3CRL Series

This is the CRL series diagram for POC / Pilot Deployments. We anticipate that in the future there may be local CRLGs hanging off various CAs within the V2I ICA hierarchy. Introducing a new CRLG, and assigning new certs to it, can be done without requiring any change in the existing CRLG certs, although it is obviously impossible to transfer already-issued certs from one CRLG to another.



2.2.11.11.4Step 11.2.1 - Revoke CRLG (Use Case)

Target release	Release 1.1
Document owner	Brian Romansky
Reviewer	Rekha Singoria, William Whyte, Dean Therriault, Benedikt Brecht

2.2.11.11.4.1 Goals

- Revoke a CRLG certificate from the SCMS System

2.2.11.11.4.2 Background and strategic fit

The Technical Component of the SCMS Manager (TCotSCMSM) determines that a CRL Generator (CRLG) needs to be revoked. The TCotSCMSM shall first establish a new CRLG key pair and certificate and use the new CRLG to issue a CRL listing the previous CRLG as a revoked component.

The MA no longer uses the old CRLG to distribute CRLs (the procedure for adding a new CRLG will update the MA with the address and TLS certificate of the new CRLG).

2.2.11.11.4.2.1 End Entity process and requirements for validating CRLG revocation

In order to prevent the following attack sequence:

- A CRLG certificate is compromised by attacker
- A new valid CRLG certificate is used to sign a CRL revoking the compromised CRLG certificate
- The CRL Store makes the new valid CRL available for download
- The attacker downloads the new valid CRL
- Attacker creates a fraudulent CRL signed by the compromised certificate which revokes the new CRLG certificate
- Attacker distributes the new fraudulent CRL via collaborative distribution before all devices have downloaded the new valid CRL
- Repeat steps 2-6

EEs will perform the following mitigation steps when receiving a CRL signed by a new CRLG (where "new CRLG" means a CRLG certificate that has not been previously verified by the EE):

- The EE shall store the ValidityPeriod.start value of the last CRLG certificate that passes validation. (Note: this value does not need to be individually stored if the entire CRLG certificate is stored)
- 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 chronologically earlier then the stored ValidityPeriod.start value of the previously received valid CRLG certificate.
- If the new CRLG certificate ValidityPeriod.start value is chronologically later than the stored ValidityPeriod.start value of the previously received valid CRLG certificate and passes all other validation steps, then the CRL is accepted as valid, including any entries revoking CRLG certificates.
- The EE will store the new ValidityPeriod.start value.

Note that a newly configured EE will initialize the "current" CRLG validity start time using the value contained in the first CRL processed by the EE.

2.2.11.11.4.3 Assumptions

- The recommended procedure for recovering from a compromised or failed CRLG is to immediately establish a new CRLG and use it to issue a CRL that revokes the previous CRLG.
- The SCMS requires a valid CRLG in order to sustain operation. For PoC, there will be only one valid CRLG in operation. Therefore, when the 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.
- 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.

2.2.11.11.4.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-772	Manual Process	Standing up a Non-Root SCMS component replacing the revoked component	The Technical Component of the SCMS Manager shall stand up a replacement component to the revoked component, if necessary.	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, as in Add Non-Root SCMS Component. In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-859	Tests passed	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 be informed in order to stop requesting encrypted PLVs from the revoked LA. The MA needs 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	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	justification	notes	Component/s
					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, or • in trusting certificate chains chaining to that component's certificate, or • in trusting messages signed using this component's certificate See Assumption 1 in Revoke Root CA (Use Case) for a discussion of various scenarios, particularly applicable to ICA and ECA revocation.	
SCMS-1387	Manual Process	Remove revoked	The Technical Component of	Revoked certificates get		TCotSCMSM

Key	Status	Summary	Description	justification	notes	Component/s
		certificates from GCCF	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.	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.		
SCMS-1598	Review	Regenerate CRL	If the CRLG is revoked, the MA shall regenerate the CRL from internal data. Older versions of the CRL signed by the revoked CRLG would be discarded.	Old CRL cannot be trusted if CRLG is revoked.		MA
SCMS-1606	SCMS PoC out of Scope	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 certificate 3) The CRL Store makes the		On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
				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	SCMS PoC out of Scope	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 chronologically earlier then the stored ValidityPeriod.	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 certificate 3) The CRL Store makes the new valid CRL		On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
			start value of the previously received valid CRLG Certificate.	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		

2.2.11.11.5Step 11.2.1 - Revoke ECA (Use Case)

Target release	Release 1.1
Document owner	Brian Romansky
Reviewer	Rekha Singoria, William Whyte, Dean Therriault, Benedikt Brecht

2.2.11.11.5.1 Goals

- Revoke an ECA certificate from the SCMS System

2.2.11.11.5.2 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 and should obtain a new enrollment certificate as soon as possible (the SCMS Manager may set performance requirements for how quickly this must happen).

2.2.11.11.5.3 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.

2.2.11.11.5.4 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.

2.2.11.11.5.5 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	An authenticated message from the SCMS Manager is required to	In the PoC, this will occur by a manual process.	TCotSCMSM

Key	Status	Summary	Description	justification	notes	Component/s
			list the certificate of the component to be revoked in the components CRL and have the CRLG sign it.	revoke a component.		
SCMS-772	Manual Process	Standing up a Non-Root SCMS component replacing the revoked component	The Technical Component of the SCMS Manager shall stand up a replacement component to the revoked component, if necessary.	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, as in Add Non-Root SCMS Component. In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-859	Tests passed	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 be informed in order to stop requesting encrypted PLVs from the revoked LA. The MA needs 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, or • in trusting certificate chains chaining to that component's certificate, or • in trusting messages signed using this component's certificate See Assumption 1 in Revoke Root CA (Use Case) for a discussion of various scenarios,	

Key	Status	Summary	Description	justification	notes	Component/s
					particularly applicable to ICA and ECA revocation.	
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-1587	SCMS PoC out of Scope	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	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, or • in trusting certificate chains chaining to that component's certificate, or • in trusting messages	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
			chains up to the revoked CA.		signed using this component's certificate • in sending messages signed with certificates that chain up to this component's certificate See Assumption 1 in Revoke Root CA (Use Case) for a discussion of various scenarios, particularly applicable to ICA and ECA revocation. This is out of scope as it defines EE behavior.	
SCMS-1589	SCMS PoC out of Scope	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)

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1593	SCMS PoC out of Scope	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)

2.2.11.11.6Step 11.2.1 - Revoke ICA (Use Case)

Target release	Release 1.1
Document owner	Brian Romansky
Reviewer	Rekha Singoria, William Whyte, Dean Therriault, Benedikt Brecht

2.2.11.11.6.1 Goals

1. Revoke an ICA certificate from the SCMS System

2.2.11.11.6.2 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.

2.2.11.11.6.3 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.

2.2.11.11.6.4 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 Non-Root SCMS component replacing the revoked component	The Technical Component of the SCMS Manager shall stand up a replacement component to the revoked component, if necessary.	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, as in Add Non-Root SCMS Component. In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-859	Tests passed	All relevant components	All SCMS components	The relevant components	Particularly, in the case of LA	CRL Store, CRLG, DCM,

Key	Status	Summary	Description	justification	notes	Component/s
		cease to trust the revoked component	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.	should not use the revoked component's certificate to trust it. If their chains include the revoked component, they should receive new certificate chains.	revocation, the RA needs be informed in order to stop requesting encrypted PLVs from the revoked LA. The MA needs 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, or • in trusting certificate chains	ECA, IBLM, ICA, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	justification	notes	Component/s
					chaining to that component's certificate, or • in trusting messages signed using this component's certificate See Assumption 1 in Revoke Root CA (Use Case) for a discussion of various scenarios, particularly applicable to ICA and ECA revocation.	
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-1587	SCMS PoC out of Scope	EE shall cease to trust the revoked CA	EEs receiving and validating a CRL shall remove all revoked CA certificates	EE should not use the revoked component's certificate to trust it. If it chains include	EEs receiving the component CRL shall mark the revoked component certificates as	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
			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.	the revoked component, they need to receive new certificates with a new certificate chain.	untrusted immediately: • in sending requests to that component, or • in trusting certificate chains chaining to that component's certificate, or • in trusting messages signed using this component's certificate • in sending messages signed with certificates that chain up to this component's certificate See Assumption 1 in Revoke Root CA (Use Case) for a discussion of various scenarios, particularly applicable to ICA and ECA revocation. This is out of scope as it defines EE behavior.	

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1589	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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	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.	EEs receiving the component CRL shall mark the revoked component certificates as untrusted immediately: 1. in sending requests to	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
			that is invalidated due to a RCA, ICA, or PCA revocation.	That includes its own pseudonym/application/identification certificates that chain up to the revoked CA certificate.	that component, or 2. in trusting certificate chains chaining to that component's certificate, or 3. in trusting messages signed using this component's certificate, or 4. in sending messages signed with certificates that chain up to this component's certificate See Assumption 1 in Revoke Root CA (Use Case) for a discussion of various scenarios, particularly applicable to ICA and ECA revocation. This is out of scope as it defines EE behavior.	

2.2.11.11.7Step 11.2.1 - Revoke MA (Use Case)

Target release	Release 1.0
Document owner	Nevine Ebeid
Reviewer	Brian Romansky, Rekha Singoria, William Whyte

2.2.11.11.7.1 Goals

- Revoke an MA certificate from the SCMS System

2.2.11.11.7.2 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 (Use Case).

2.2.11.11.7.3 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.

2.2.11.11.7.4 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 Non-Root SCMS component replacing the revoked component	The Technical Component of the SCMS Manager shall stand up a replacement component to the revoked component, if necessary.	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, as in Add Non-Root SCMS	TCotSCMSM

Key	Status	Summary	Description	justification	notes	Component/s
					Component. In the PoC, this will occur by a manual process.	
SCMS-859	Tests passed	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 be informed in order to stop requesting encrypted PLVs from the revoked LA. The MA needs 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	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	justification	notes	Component/s
					that component, or • in trusting certificate chains chaining to that component's certificate, or • in trusting messages signed using this component's certificate See Assumption 1 in Revoke Root CA (Use Case) for a discussion of various scenarios, particularly applicable to ICA and ECA revocation.	
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

2.2.11.11.8Step 11.2.1 - Revoke PCA (Use Case)

Target release	Release 1.0
Document owner	Brian Romansky
Reviewer	Rekha Singoria, William Whyte

2.2.11.11.8.1 Goals

1. Revoke a PCA certificate from the SCMS System

2.2.11.11.8.2 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.

2.2.11.11.8.3 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.

2.2.11.11.8.4 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.

2.2.11.11.8.5 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-358	SCMS PoC out of Scope	Discard Certificate Batches Signed by a Revoked PCA	OBE shall discard all pseudonym certificates that were issued by a PCA upon validating that	PCA generates batches of pseudonym certificates and an OBE device cannot know when the pseudonym	This is out of scope as it defines OBE behavior.	On-board Equipment (OBE)

Key	Status	Summary	Description	justification	notes	Component/s
			this PCA has been revoked.	certificates were signed, therefore all such certificates from the revoked PCA must be untrusted even if the PCA's certificate was verified previously.		
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 Non-Root SCMS component replacing the revoked component	The Technical Component of the SCMS Manager shall stand up a replacement component to the revoked component, if necessary.	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, as in Add Non-Root SCMS Component. In the PoC, this will occur by a manual process.	TCotSCMSM
SCMS-859	Tests passed	All relevant components	All SCMS components	The relevant components	Particularly, in the case of LA	CRL Store, CRLG, DCM,

Key	Status	Summary	Description	justification	notes	Component/s
		cease to trust the revoked component	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.	should not use the revoked component's certificate to trust it. If their chains include the revoked component, they should receive new certificate chains.	revocation, the RA needs be informed in order to stop requesting encrypted PLVs from the revoked LA. The MA needs 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, or • in trusting certificate chains	ECA, IBLM, ICA, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	justification	notes	Component/s
					chaining to that component's certificate, or • in trusting messages signed using this component's certificate See Assumption 1 in Revoke Root CA (Use Case) for a discussion of various scenarios, particularly applicable to ICA and ECA revocation.	
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-1587	SCMS PoC out of Scope	EE shall cease to trust the revoked CA	EEs receiving and validating a CRL shall remove all revoked CA certificates	EE should not use the revoked component's certificate to trust it. If it chains include	EEs receiving the component CRL shall mark the revoked component certificates as	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
			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.	the revoked component, they need to receive new certificates with a new certificate chain.	untrusted immediately: • in sending requests to that component, or • in trusting certificate chains chaining to that component's certificate, or • in trusting messages signed using this component's certificate • in sending messages signed with certificates that chain up to this component's certificate See Assumption 1 in Revoke Root CA (Use Case) for a discussion of various scenarios, particularly applicable to ICA and ECA revocation. This is out of scope as it defines EE behavior.	

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1608	SCMS PoC out of Scope	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: 1. in sending requests to that component, or 2. in trusting certificate chains chaining to that component's certificate, or 3. in trusting messages signed using this component's certificate, or 4. in sending messages signed with certificates that chain up to this component's certificate See Assumption 1 in Revoke Root CA (Use Case) for a discussion of various scenarios, particularly applicable to ICA and ECA	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
					revocation. This is out of scope as it defines EE behavior.	

2.2.11.11.9Step 11.2.1 - Revoke PG (Use Case)

Target release	Release 1.0
Document owner	Brian Romansky
Reviewer	William Whyte

2.2.11.11.9.1 Goals

- Revoke a Policy Generator certificate from the SCMS System

2.2.11.11.9.2 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.

2.2.11.11.9.3 Procedure

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.

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.

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.

- 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.
- 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.

2.2.11.11.9.4 Assumptions

1. Back-end 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.
2. 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.
3. 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.

2.2.11.11.9.5 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 Non-Root SCMS component replacing the revoked component	The Technical Component of the SCMS Manager shall stand up a replacement component to the revoked component, if necessary.	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, as in Add Non-Root SCMS Component. In the PoC, this	TCotSCMSM

Key	Status	Summary	Description	justification	notes	Component/s
					will occur by a manual process.	
SCMS-859	Tests passed	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 be informed in order to stop requesting encrypted PLVs from the revoked LA. The MA needs 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: 1. in sending requests to that	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, MA, PCA, PG, RA

Key	Status	Summary	Description	justification	notes	Component/s
					component, or 2. in trusting certificate chains chaining to that component's certificate, or 3. in trusting messages signed using this component's certificate See Assumption 1 in Revoke Root CA (Use Case) for a discussion of various scenarios, particularly applicable to ICA and ECA revocation.	
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

<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-1685</td><td>SCMS PoC out of Scope</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><tr><td>(OBE only) cert_validity_model</td><td>concurrent</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) max_available_cert_supply	3 years			
			(RSE only) rse_application_cert_validity	1 week + 1 hour			
			(RSE only) rse_application_cert_overlap	1 hour			

2.2.11.11.10 Step 11.2.2: Revoke Root CA (Use Case)

Target release	Release 1.1
Document owner	Brian Romansky
Reviewer	William Whyte

2.2.11.11.10.1 Goals

- Produce "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.

2.2.11.11.10.2 Assumptions

- Root Management is performed according to the Elector scheme outlined in Root Management and Revocation Recovery

2.2.11.11.10.3 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.

2.2.11.11.10.4 Procedure

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

- 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.
- 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.
- 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.
- 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*.
- 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.

- 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.

2.2.11.11.10.5 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.	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
			The Technical Component of the SCMS Manager shall place the "Revoke Root CA" on the CRL for distribution to EEs and other SCMS components.			
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	SCMS PoC out of Scope	EEs obtain a new LCCF upon Root CA revocation	EEs shall contact an RA to obtain a new Local Certificate Chain File (LCCF) when	EE's require a valid certificate chain that can be used to validate their own pseudonym certificates 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
			their current Root CA has been revoked.	relevant SCMS component certificates.		
SCMS-865	Manual Process	EEs obtaining new Enrollment Certificates upon Root CA revocation	EEs shall obtain new Enrollment Certificates from their ECAs, if the Root CA was revoked. Refreshed Enrollment Certs are encrypted to the old Enrollment Certificate.	EEs need to obtain new enrollment certificates valid in the new PKI hierarchy.	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 Certificate). This implies a strong link between the OEM and their ECA. This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-866	SCMS PoC out of Scope	OBEs obtaining new Pseudonym/ Identification Certificates upon Root CA revocation	OBEs shall use the new Enrollment Certificate (cp. https://jira.camp llc.org/browse/SCMS-865~~SCMS-865~~) to obtain new Pseudonym or Identification	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	On-board Equipment (OBE)

Key	Status	Summary	Description	justification	notes	Component/s
			Certificates that chain up to the new Root CA.		defines OBE behavior.	
SCMS-1024	Review	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 Root CA: PG Update Global Certificate Chain File	The Policy Generator shall update the GCCF as soon as it receives the "Revoke Root CA" message and remove "Add Root CA" message of that certificate as well as remove all chains containing the revoked Root CA certificate	Having an updated certificate chain file makes verification processes at EEs more efficient.		PG

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1170	SCMS PoC out of Scope	RSEs obtain new application certificates	RSEs shall use the new Enrollment Certificate (cp. https://jira.camppllc.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	Review	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	Every SCMS component will need to manage Elector updates automatically, so therefore every SCMS component will need to be able to process Root Management	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
			that the number of valid signatures is at least a quorum of non-revoked Electors in its trust store.	messages signed by the Electors.	be produced in a manual process for the PoC.	
SCMS-1587	SCMS PoC out of Scope	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, or • in trusting certificate chains chaining to that component's certificate, or • in trusting messages signed using this component's certificate • in sending messages signed with certificates that chain up to this component's certificate See Assumption 1 in Revoke	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
					Root CA (Use Case) for a discussion of various scenarios, particularly applicable to ICA and ECA revocation. This is out of scope as it defines EE behavior.	
SCMS-1589	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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		On-board Equipment (OBE), Road-side Equipment (RSE)

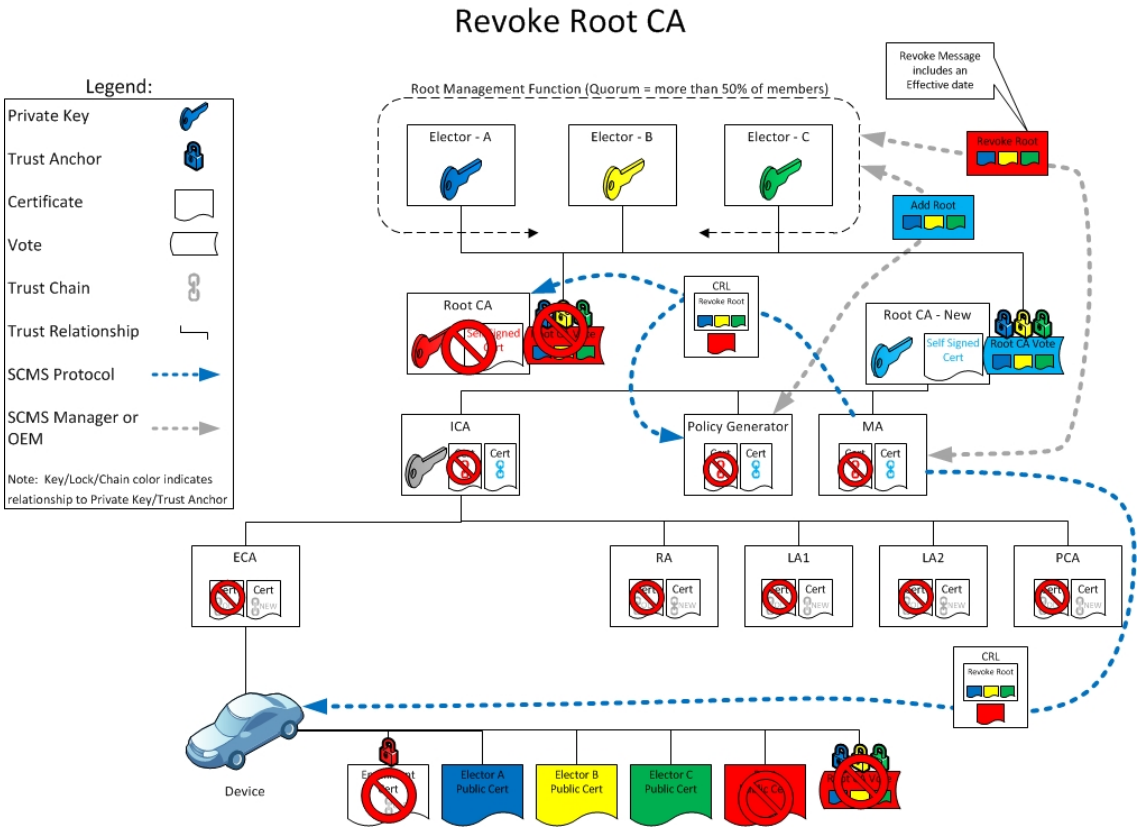
Key	Status	Summary	Description	justification	notes	Component/s
				that chain up to the revoked CA certificate.		
SCMS-1608	SCMS PoC out of Scope	EE receive new pseudonym/ application/identification certificates after PCA revocation	EE shall request new pseudonym, application, or identification certificates 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, or • in trusting certificate chains chaining to that component's certificate, or • in trusting messages signed using this component's certificate, or • in sending messages signed with certificates that chain up to this component's certificate See Assumption 1 in Revoke Root CA (Use Case) for a discussion of various scenarios,	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
					particularly applicable to ICA and ECA revocation. This is out of scope as it defines EE behavior.	

2.2.11.11.10.6 Design

The design for the elector-based management system is described in the Root Management and Revocation Recovery section.

2.2.11.11.10.7 Diagrams



2.2.11.11.11 Step 11.2.3: Revoke Elector

Target release	Release 1.1
Document owner	Brian Romansky
Reviewer	Benedikt Brecht, William Whyte

2.2.11.11.11.1 Goals

- Produce "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.

2.2.11.11.11.2 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.

2.2.11.11.11.3 Procedure

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

- 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.
- 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.
- 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.
- SCMS components (including EEs) that receive a composite CRL with one or more elector removal message 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*.

- 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.

2.2.11.11.11.4 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.

2.2.11.11.11.5 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1024	Review	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-1381	Manual Process	Revoke an Elector	The Technical Component of the SCMS Manager (TCotSCMSM) shall communicate the multi-signed "Revoke	Messages revoking Electors 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

Key	Status	Summary	Description	justification	notes	Component/s
			Elector" message to CRL Generator to be included in the SCMS component CRL that will be distributed to SCMS components and EEs to inform them of the revoked Elector.			
SCMS-1408	Manual Process	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	Review	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	Review	Revoke Elector: PG Update	The Policy Generator shall update the	Having an updated certificate chain		PG

Key	Status	Summary	Description	justification	notes	Component/s
		Global Certificate Chain File	GCCF as soon as it receives the "Revoke Elector" message and remove the "Add Elector" message of the revoked Elector.	file makes verification processes at EEs more efficient.		

2.2.11.11.11.6 Design

The design for the elector-based management system is described in the Root Management and Revocation Recovery section.

2.2.12 Use Case 12: RSE Bootstrapping

Target release	Release 1.0
Document owner	Biswajit Panja
Reviewer	Benedikt Brecht

2.2.12.1 Goals

RSE Bootstrap encompasses two distinct activities: initialization and enrollment. Initialization is the process by which RSE receives keys that allow it to trust other devices. Enrollment is the process by which RSE receives a long-term certificate, which it can use in interactions with the SCMS to allow other devices to trust it. Data provided to the DCM is handled via a notification service that is maintained by the SCMS Manager. For example, the SCMS Manager can keep a list of all DCMs and alert them as necessary.

2.2.12.2 Background and strategic fit

Bootstrap is executed at the start of RSE's lifecycle. At the start of bootstrap, RSE has no certificates and no knowledge of how to contact the SCMS. At the end of bootstrap, the RSE has:

- An Enrollment Certificate and information that allows it to apply for pseudonym certificates:
  - A correctly issued enrollment certificate and the corresponding private key, to allow it to authenticate its certificate batch request for application certificates.
  - The RA certificate and contact information for the RA, to allow it to request pseudonym certificates. This includes the RA's X.509 Root CA certificate, which might be a different Root CA than the 1609.2 Root CA.
  - The Enrollment CA certificate and contact information for the ECA, to allow it to request new enrollment certificates.
- Certificates and information that allow it to send and receive received messages securely:
  - The Root CA certificate(s) (required), Intermediate CA, and Pseudonym CA certificates (optional) to allow it to verify received messages. The device can learn to trust the optional certificates by observing them in ongoing operation as certificates signed by

the Root CA and properly verified by the device. At minimum, a device needs the PCA certificate that will issue certificates to it and the PCA's ICA certificate.
    - CRL Generator certificates (optional), to allow it to trust received CRLs.
    - Contact information for the CRL store, to allow it to request missing CRLs.
    - The MA certificate and contact information for the MA, to allow it to submit misbehavior reports.

Bootstrap must protect RSE from getting incorrect information and the ECA from issuing a certificate to devices, which do not have a right to that certificate. Any bootstrap process is acceptable that results in this information being established securely.

Bootstrap is considered to consist of two distinct logical operations, initialization and enrollment. Initialization is the process by which the device obtains firmware, certificates and other information it needs to trust other system components. Enrollment is the process by which RSE obtains certificates it will need to send messages.

There are multiple methods by which RSEs can be provisioned with enrollment certificates, with these two being most likely:

1. Certificate Request/Response method: The RSE is initialized with firmware, roots of trust and essential network information in a trusted environment. The RSE then subsequently connects to the DCM through a trusted channel, performs an Enrollment certificate request, and receives an Enrollment certificate response through the DCM.
2. Certificate Injection method: The RSE enrollment public/private key pair is generated in a secure environment outside of the RSE (for example in the DCM). The DCM then performs an Enrollment certificate request to the ECA and receives an Enrollment certificate on behalf of the RSE. Subsequently, the RSE is initialized with firmware, roots of trust, essential network information, the enrollment public/private key pair and the Enrollment certificate through a trusted channel with the DCM.

2.2.12.3 Assumptions

- All required certificates are provided upfront to the DCM.
- A “secure environment” as defined in Secure Environment for Device Enrollment ensures that the entirety of the connection between the DCM and the device is under the control of the operator running the bootstrap operation.
- At the start of bootstrap, a device has no certificates and no knowledge of how to contact the SCMS.

2.2.12.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-556	SCMS PoC out of Scope	Secure process	DCM shall use a secure operational process to inject EE	Physical and operational security involving EEs is	See the wiki page on Secure Environment for Device Enrollment for	DCM

Key	Status	Summary	Description	justification	notes	Component/s
			firmware, enrollment certificates etc. as defined by the SCMS Manager.	crucial to their security.	guidelines on physical security for device provisioning. Does not apply to POC.	
SCMS-557	SCMS PoC out of Scope	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 the wiki page on 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)
SCMS-559	Manual Process	Certified Devices	DCM shall ensure that only certified EEs are provisioned.	Rogue devices will compromise the security of the EE, and could spread insecurity further than a single device.	See the wiki page on Secure Environment for Device Enrollment for guidelines on physical security for device provisioning. Not software testable for POC, procedural	DCM
SCMS-560	SCMS PoC out of Scope	Certified Software	EEs shall ensure that during bootstrapping process only certified software is provisioned.	Improper software installation will compromise security of the EEs.	See the wiki page on Secure Environment for Device Enrollment for guidelines on physical security for device provisioning. Not software testable for POC, procedural	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1270	SCMS PoC out of Scope	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)

2.2.12.5 Step 12.1: RSE initialization

Target release	Release 1.0
Document owner	Biswajit Panja
Reviewer	Andre Weimerskirch, Benedikt Brecht

2.2.12.5.1 Goals

Initialization is the process by which a RSE receives public keys and certificates that allow it to trust other devices in the system. Therefore the overall goal of the initialization process is:

- Provisioning of SCMS component certificates
- Configuration, e.g. URL for RA, ECA, and MA services
- Current CRL
- Current Local Policy File
- Current Local Certificate Chain File

2.2.12.5.2 Background and strategic fit

The use case Initialization involves the following components:

- Actively involved:
  - The DCM
  - RSE
- Provide information to the DCM beforehand:
  - Root CA, ICA, PCA, MA, ECA (certificates)
  - RA, ECA (URL)

Overview:

The DCM gathers the current certificates of:

- All Electors
- All Root CAs
- The Intermediate CAs and Pseudonym CAs that may issue certificates that the device will use to trust received application messages. These certificates can be communicated to the device via peer-to-peer protocol as defined in 1609.2 and via the Local Certificate Chain File
- The MA
- Policy Generator

- Any CRL Generators that may issue CRLs that the device will need to process. These certificates can be communicated to the device as part of the CRL itself.

The DCM installs these certificates on the OBE using the Local Certificate Chain File. The Elector and the Root CA certificates have to be installed in a secure environment for the SCMS PoC implementation. Given sufficient Elector votes, the Root CA certificate could also be validated. All other certificates can be installed in a non-secure environment as the OBE now has the certificate of the Root CA to validate whether these certificates are genuine.

The Local Certificate Chain File details for downloading and file format of the can be found here: Step 18.5: Generate Global and Local Certificate Chain File.

2.2.12.5.3 Assumptions

- For the given design, it is assumed that the process takes place in a secure environment as recommended in Secure Environment for Device Enrollment.
- The DCM is only accessible from a secure environment and sets up a secure connection to the SCMS.
- The DCM will be configured with the set of Elector, Root CAs, ICAs, PCAs, ECA and MA certs to be used for any given RSE or collection of RSEs.

2.2.12.5.4 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

Key	Status	Summary	Description	justification	notes	Component/s
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-562	Tests passed	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	Tests passed	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	Tests passed	MA certificate and FQDN	DCM shall provide the EE with the MA certificate and the FQDN for the MA.	The EE will need to communicate securely with the MA (e.g. in order to download CRLs)		DCM
SCMS-565	Tests passed	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	Tests passed	PCA certificates	DCM shall provide the EE with its own PCA certificate. Optionally,	The EE needs its PCA certificate, e.g. to provide this to other EE in peer-to-peer		DCM

Key	Status	Summary	Description	justification	notes	Component/s
			include other existing PCA certificates.	certificate updates.		
SCMS-567	Tests passed	CRL	DCM shall provide the EE with the latest CRL and contact information for the CRL (CRACA certificate is part of the CRL).	The EE will be provided with the current CRL so as to reject communication from invalidated devices.		DCM
SCMS-568	Tests passed	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-946	Tests passed	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 the Misbehavior Authority.		DCM
SCMS-948	In Implementation	Bootstrap: Local Certificate Chain File	DCM shall provide the EE with the latest Local	The EE will use this in the verification process of		DCM

Key	Status	Summary	Description	justification	notes	Component/s
			Certificate Chain File.	SCMS certificates.		
SCMS-949	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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-1158	Review	Elector certificates	DCM shall provide the device with all Elector certificates.	The Elector certificates will be required to perform any future Root Management operations.		DCM
SCMS-1159	SCMS PoC out of Scope	EE securely stores Elector certificates	EE shall store the Elector certificates in tamper-evident storage.	The Elector 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 be updated when the proper Root Management authentication	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
				mechanisms have been satisfied.		
SCMS-1160	SCMS PoC out of Scope	EE securely stores Root CA certificates	EE shall store all Root CA certificates in tamper-evident 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 be updated when the proper Root (Elector) Management authentication mechanisms have been satisfied.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1174	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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	Tests passed	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-1207	SCMS PoC out	EE stores Certificate	EE shall store the Certificate Revocation	The EE will be provided with the current CRL	This is out of scope since it	On-board Equipment (OBE), Road-

Key	Status	Summary	Description	justification	notes	Component/s
	of Scope	Revocation List	List in tamper-evident storage.	so as to reject communication from invalidated devices.	defines EE's behavior.	side Equipment (RSE)
SCMS-1208	SCMS PoC out of Scope	EE securely stores X.509 root certificate	EE shall store the X.509 root certificate in tamper-evident 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	SCMS PoC out of Scope	EE securely stores Local Certificate Chain File	EE shall store the Local Certificate Chain File in tamper-evident 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)

2.2.12.6 Step 12.2: RSE enrollment

Target release	Release 1.0
Document owner	Biswajit Panja
Reviewer	

2.2.12.6.1 Goals

To provide RSEs with enrollment certificate.

2.2.12.6.2 Assumptions

- Device has been securely initialized and held within a secure chain of custody since initialization, see Step 12.1: RSE initialization for details.
    - As a result of initialization the device has the ECA certificate and any necessary certificates to construct a chain back to the root (so it can verify its own enrollment certificate)

2.2.12.6.3 Background and strategic fit

This process is identical to enrollment of OBEs 2.2. Enrollment (Bootstrapping).

2.2.12.6.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
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	SCMS PoC out of Scope	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-1095	In Implementation	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, Road-side Equipment (RSE)
SCMS-1210	SCMS PoC out of Scope	EE Secure Key Storing	EE shall store the following keys in tamper-evident storage: • Private enrollment key • Butterfly key	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	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
			parameters (seed + expansion function parameter) • All private keys (e.g. of OBE application certificates and private keys calculated from the Butterfly key parameters)		mechanism that offers secure boot and that protects the keys against software-based attacks. Additional details are listed in Hardware, Software and OS Security	
SCMS-1305	Review	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 associated with a particular (PSID, SSP) combination 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	ECA

Key	Status	Summary	Description	justification	notes	Component/s
					certificate are likely to be related to policy decisions to be made by the SCMS Manager.	
SCMS-1307	Review	Enrollment certificate lifetime	ECA shall issue Enrollment Certificates with a lifetime of 30 years.	For PoC, enrollment certificates use a life span of 30 years to avoid any need to update enrollment certificates.	This is for PoC only	ECA
SCMS-1411	SCMS PoC out of Scope	CV pilots: DCM keep track of generated enrollment certificates	For the CV pilot deployment the Single Point of Contact (SPOC) of the DCMs shall keep track of all issued enrollment certificates.	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
SCMS-1419	Review	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	DCM

Key	Status	Summary	Description	justification	notes	Component/s
					the same PSID/SSP.	
SCMS-1600	Review	Enrollment certificate lifetime	ECA shall issue Enrollment Certificates with a maximum lifetime of 7 years. All EE Enrollment certificates shall be issued with an expiration at year 7 regardless of the date they are issued.	For CV-Pilot, enrollment certificates use a maximum life span of 7 years to avoid any need to update enrollment certificates.	This is for CV-Pilot only.	ECA
SCMS-1906	Review	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.		DCM, On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1907	Review	Enrollment certificate verification	The enrollment key-pair generator (OBE, RSE, or DCM) shall check that the enrollment certificate certificate correctly verifies, including building a	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)

Key	Status	Summary	Description	justification	notes	Component/s
			chain back to the root.			
SCMS-1910	SCMS PoC out of Scope	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)

2.2.13 Use Case 13: RSE Application Certificate Provisioning

Target release	Release 1.0
Document owner	Virendra Kumar
Reviewer	Biswajit Panja

2.2.13.1 Goals

Provide a bootstrapped RSE with an application certificate that it can use in relevant applications.

2.2.13.2 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.

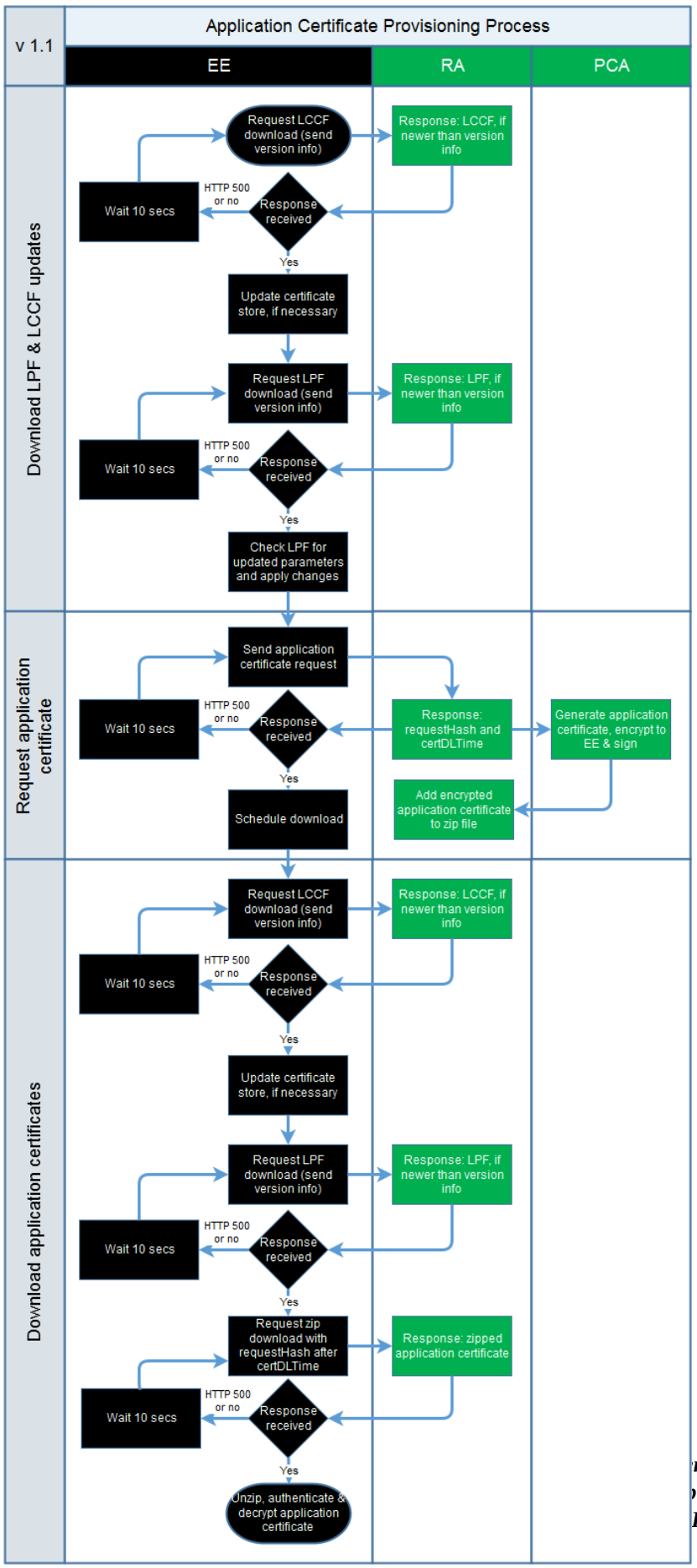
2.2.13.3 Assumptions

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.

2.2.13.4 Design

The following flow chart documents the general flow of steps a 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 requirements for a complete description of the process.



At a high level, two steps are relevant towards a RSE:

- Request RSE Application Certificate
- 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 and 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.*

2.2.13.5 Step 13.1: Request RSE Application Certificate

Target release	Release 1.0
Document owner	Virendra Kumar
Reviewer	Rekha Singoria, Andre Weimerskirch, Biswajit Panja

2.2.13.5.1 Goals

Define messages and other requirements for an RSE to request application certificate.

2.2.13.5.2 Background and strategic fit

The RSE decides to request 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.

2.2.13.5.3 Assumptions

- RSE has successfully completed Use Case 12: RSE Bootstrapping

2.2.13.5.4 Process Steps

- 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
  - If there is an updated LCCF, RSE applies all changes to its trust-store (necessary for PCA Certificate Validations).
  - If there is an updated LPF, RSE applies those changes.

- 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.
- The RA ensures that the certificate batch request is correct and authorized, before it starts Step 13.2: Generate RSE Application Certificate.

2.2.13.5.5 Error Handling

- The RSE will abandon further interactions with the RA after a certain number of failed communication attempts resulted in errors.

2.2.13.5.6 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-507	Tests failed	Maintain an Internal Blacklist	RA shall maintain an Internal Blacklist and keep it updated based on the communications with the MA	so that revoked EEs are not able to authenticate with the RA anymore	Every logical RA has its own internal blacklist that is not shared with anyone else. To prevent compromised components to speak with the RA the RA needs to validate against the SCMS component CRL (compare SCMS-859, https://jira.camplc.org/browse/SCMS-504~~SCMS-504~~) and the X.509 CRL (SCMS-405).	RA
SCMS-512	In Implementation	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-521	Closed	Acknowledge request	RA shall acknowledge	so that EEs know that the		RA

Key	Status	Summary	Description	justification	notes	Component/s
			the receipt of EE's request with a TCP ACK within a specified amount of time, currently set to be 1 sec.	RA received their request.		
SCMS-522	SCMS PoC out of Scope	Retry request	If the EE does not receive acknowledgement (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, it shall retry.	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	SCMS PoC out of Scope	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-524	SCMS PoC out of Scope	RA certificate	EE shall dynamically acquire RA's SCMS certificate each time it communicates with RA.	so that EE can encrypt the request to the right RA	More information is available at RA - Retrieve Registration Authority Certificate. This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-709	SCMS PoC out	Check for and	EE shall check for and	It is necessary to ensure that the	If no policy file is available on	On-board Equipment

Key	Status	Summary	Description	justification	notes	Component/s
	of Scope	Download Policy Updates	download policy updates upon establishing communications with the RA	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.	the EE, the EE is allowed to make a download attempt at any time. This is out of scope since it defines EE's behavior.	(OBE), Road-side Equipment (RSE)
SCMS-754	SCMS PoC out of Scope	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	In Implementation	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	For more information: Generate Global and Local Certificate Chain File	RA

Key	Status	Summary	Description	justification	notes	Component/s
				current LCCF's version number in the download request to RA and the response will include a newer LCCF if available.		
SCMS-776	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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-955	SCMS PoC out of Scope	Misbehavior report: eePolicyVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify the digital signature of the local policy file.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-956	SCMS PoC out of Scope	Error code: eePolicyFileParsingFailed	EE shall log this error code in EE's error log file, if EE is not able to parse the successfully	As the policy file is essential for the system to work correctly and contains security relevant information, it is	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
			downloaded local policy file (e.g. because it is corrupted).	important to have an error handling whenever the EE is not able to read the latest version of that file.		
SCMS-958	SCMS PoC out of Scope	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-981	In Implementation	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	In Implementation	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	In Implementation	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		RA

Key	Status	Summary	Description	justification	notes	Component/s
				allowed within 2 seconds		
SCMS-990	In Implementation	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	In Implementation	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	Review	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

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1068	In Implementation	Error code: raRequestForMultipleCerts	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	Review	Error code: raDuplicateRequestReceived	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-1082	In Implementation	Error code: raInvalidSignature	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	In Implementation	Error code: raRequestNotEncrypted	RA shall log "Error code: raRequestNotEncrypted", if the EE does	to enable server side diagnostics and to avoid giving potential attackers	An unencrypted certificate request might be an indication for misbehavior.	RA

Key	Status	Summary	Description	justification	notes	Component/s
			not encrypt the certificate request using the RA's 1609 certificate.	relevant information		
SCMS-1084	In Implementation	Error code: raInvalidCredentials	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	In Implementation	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	In Implementation	Error code: raMalformedRequest	RA shall log "Error code: raMalformedRequest", if an EE makes a malformed request not captured in SCMS-1082, SCMS-1083, 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
SCMS-1087	In Implementation	Error code: raMismatch	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

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1088	In Implementation	Error code: raInvalidTimeReceived	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	SCMS PoC out of Scope	Trust Chain Broken - EE	EE shall not attempt to request or download pseudonym certificate batches, OBE identification certificate files, or RSE application certificate files, 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 anyways.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1204	Tests passed	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

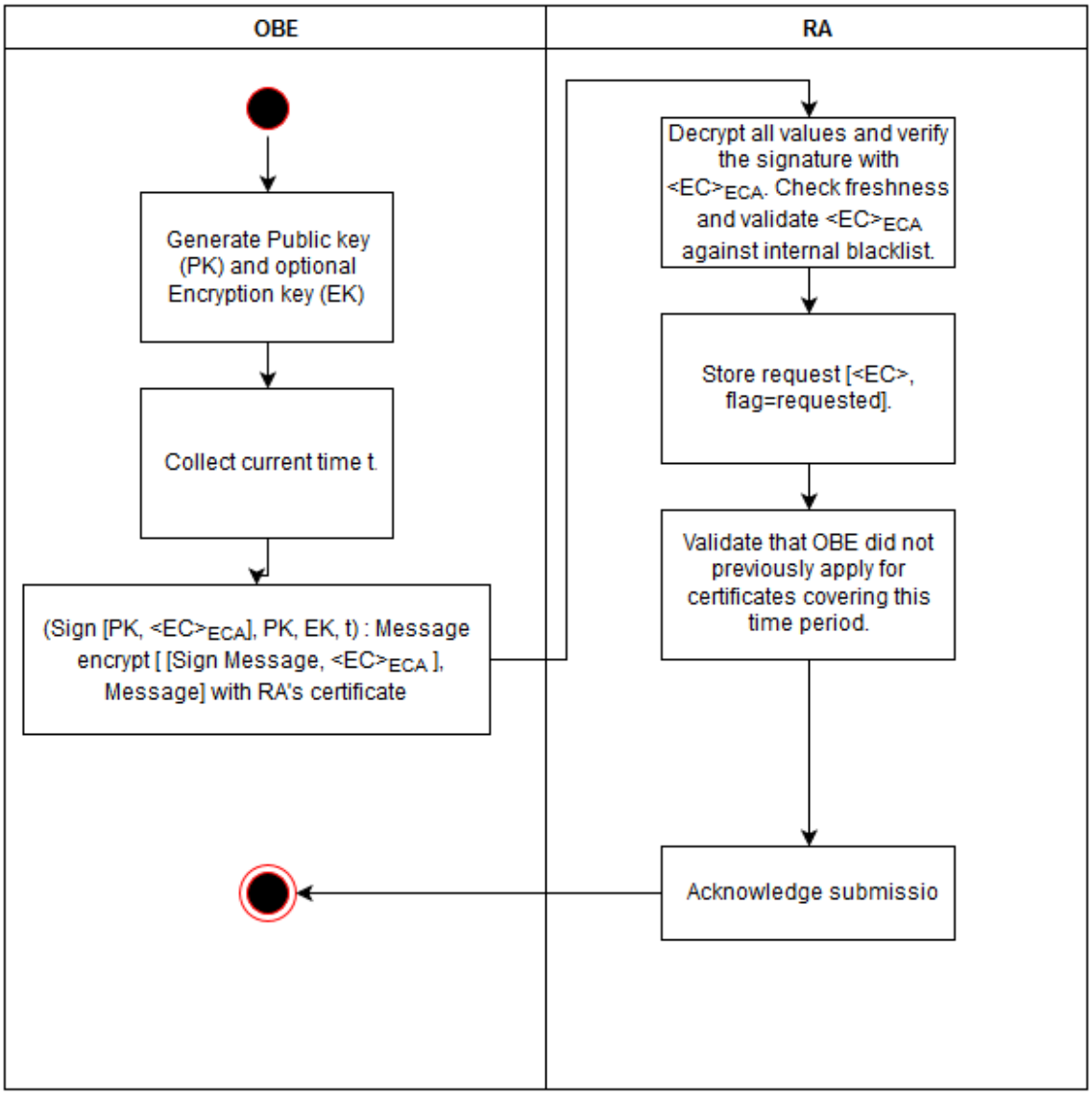
Key	Status	Summary	Description	justification	notes	Component/s
					authentication process. The Internal Blacklist Manager (IBLM) of the Misbehavior Authority (MA) updates the RAs on which devices to exclude from granting certificates. Therefore, it sends out revocation information (e.g. linkage information, 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-1270	SCMS PoC out of Scope	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	SCMS PoC out	EE request LCCF from RA	EE shall check for an updated Local	to be able to verify SCMS certificates	All the certificate chains will contain	On-board Equipment (OBE), RA,

Key	Status	Summary	Description	justification	notes	Component/s
	of Scope		Certificate Chain File (LCCF) upon establishing communications with the RA	based on their certificate chain.	certificates up to the Root CA including elector endorsement for the Root CA certificate. This is out of scope since it defines EE behavior	Road-side Equipment (RSE)
SCMS-1356	SCMS PoC out of Scope	EE uses internal certificate store	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 EEs behavior	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1397	Implemented	Error reporting to EE	SCMS Components shall return error code "HTTP 500" to EEs in response to all application level errors.	Specific error codes should be hidden from EEs to prevent useful information from being provided to malicious actors	• Standard TCP (SCMS-1090) and TLS (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	SCMS PoC out of Scope	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	Implemented	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	SCMS PoC out of Scope	LCCF validation in EE	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	Review	RA-EE Certificate Request Ack Message	RA-EE Certificate Request Ack Message shall contain the following information: Case: Certificate Provisioning Request Accept 1. Version 2. Low order 8-bytes of the SHA-256 hash of the encoded "ToBeSign	as EE needs to know, when and where it can go to download certificates.		On-board Equipment (OBE), RA, Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
			ed" certificate request from the device 3. Time at which the first certificate batches will be available for download (represented by IEEE 1609.2 Time32) 4. URL of the certificate repository (common for all devices serviced by an specific RA) Case: Certificate Provisioning Request Reject • HTTP 500 error code			

2.2.13.5.7 Design



2.2.13.5.7.1 EE Request

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.

2.2.13.5.7.1.1 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.

2.2.13.5.7.1.2 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)

2.2.13.5.7.2 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. RA shall log the specific error for future investigation.

2.2.13.5.7.2.1 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 certificates batches will be available for download.

2.2.13.5.7.2.2 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 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.

2.2.13.5.7.2.3 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

2.2.13.5.7.3 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 having completed the prerequisites.

2.2.13.6 Step 13.3: Download RSE Application Certificate

Target release	Release 1.1
Document owner	Virendra Kumar
Reviewer	Andre Weimerskirch

2.2.13.6.1 Goals

Provide a reliable, secure and timely method for RSEs to download certificates.

2.2.13.6.2 Background and strategic fit

The download will include RSE application certificate, local certificate chain file (LCCF), and local policy file (LPF). The RSE will first attempt to download LCCF (containing the PCA certificate chain required to validate the application certificate) and LPF, and process both LCCF and LPF to ensure that it is able to interpret certificates generated by the SCMS correctly. RSE will then attempt to download the RSE application certificate.

2.2.13.6.3 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.

2.2.13.6.4 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

2.2.13.6.5 Error Handling

- The RSE will abandon further interactions with the RA after a certain number of failed communication attempts resulted in errors.

2.2.13.6.6 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-411	SCMS PoC out of Scope	EE Authentication to RA for Request	The EE shall authenticate its requests with its enrollment certificate. These messages shall include a timestamp (which the EE will obtain from its GPS reference) 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.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-459	In Implementation	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	OCSP stapling provides improved performance compared to CRLs. OCSP stapling is	RA

Key	Status	Summary	Description	justification	notes	Component/s
				provide an OCSP stapled response so that the OBE can validate the RA's TLS certificate.	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 failed	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 (compare SCMS-859, https://jira.camplc.org/browse/SCMS-504~~SCMS-504~~) and the X.509 CRL (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.camplc.org/browse/SCMS-537~~SCMS-537~~) and RA-EE authentication (https://jira.camplc.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	The RA shall require EE	to ensure that only a proper EE	It is not cost effective to	RA

Key	Status	Summary	Description	justification	notes	Component/s
		authentication	authentication before any other communication process starts.	can send requests, download certificates or files.	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 E-RA Communications - General Guidance	
SCMS-522	SCMS PoC out of Scope	Retry request	If the EE does not receive acknowledgement (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, it shall retry.	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	SCMS PoC out of Scope	Number of retries	EE shall limit the number of retries to a maximum of	To reduce resource usage, EEs shall limit	This is out of scope as it defines EE behavior.	On-board Equipment (OBE), Road-

Key	Status	Summary	Description	justification	notes	Component/s
			10 in a 60 minute period	the number of retries.		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.	On-board Equipment (OBE), RA, Road-side Equipment (RSE)
SCMS-539	SCMS PoC out of Scope	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.	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
				RA authenticates via its TLS X.509 certificate. The details of the authentication process are defined E-RA Communications - General Guidance		
SCMS-541	SCMS PoC out of Scope	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	to improve reliability of the download protocol.		RA

Key	Status	Summary	Description	justification	notes	Component/s
			switches the IP address.			
SCMS-590	In Implementation	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	In Implementation	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	SCMS PoC out of Scope	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.	1. If no policy file is available on the EE, the EE is allowed to make a download attempt at any time. 2. This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-768	In Implementation	RA - Local Certificate Chain File	RA shall provide a Local Certificate Chain File to	to enable EEs to verify certificates without further CA certificate	For more information: Generate Global and Local	RA

Key	Status	Summary	Description	justification	notes	Component/s
			EEs for download.	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.	Certificate Chain File	
SCMS-951	Review	Error code: raEeVerificationFailed	RA shall log "Error code: raEeVerificationFailed", if an EE cannot be authenticated.	EE might need re-certification	Does not apply to POC. Might be added to MA integration as a misbehavior.	RA
SCMS-952	SCMS PoC out of Scope	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-953	SCMS PoC out of Scope	Misbehavior report: eePolicyFileDownloadFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to download the local policy file (e.g. because there is none or it is corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-957	SCMS PoC out of Scope	Misbehavior report: eePolicyFileParsingFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to parse the successfully downloaded local policy file (e.g. because it is corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-958	SCMS PoC out of Scope	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-966	SCMS PoC out of Scope	Misbehavior report: eeCertFileDownloadFailed	EE shall initiate a misbehavior report to MA, if EE is not able to download certificate files (e.g. because	to enable server side misbehavior detection.	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
			there is none or it is corrupted).			
SCMS-967	SCMS PoC out of Scope	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's 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-968	SCMS PoC out of Scope	Misbehavior report: eeCertFileVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify the digital signature of an encrypted certificate.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-969	SCMS PoC out of Scope	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-970	SCMS PoC out of Scope	Misbehavior report: eeCertFileDecryptionFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to decrypt an encrypted certificate.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-971	SCMS PoC out of Scope	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-972	SCMS PoC out of Scope	Misbehavior report: eeCertVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify a certificate.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-973	SCMS PoC out of Scope	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-974	SCMS PoC out of Scope	Misbehavior report: eeCertContentFalse	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to parse a certificate, or if the certificate has wrong content.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-976	In Implementation	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

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-977	In Implementation	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	In Implementation	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	SCMS PoC out of Scope	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-980	SCMS PoC out of Scope	Misbehavior report: eeAuthenticationFailed	EE shall initiate a misbehavior report to MA with the observed error, if RA-to-EE authentication fails.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-981	In Implementation	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	In Implementation	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	SCMS PoC out of Scope	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-1089	In Implementation	Error code: raCertificateUnavailable	RA shall return status code HTTP 500 and log "Error code: raCertificateUnavailable" as well as identifying information of the RSE, if RA does not have the certificate available for download by the RSE	In order to give RSEs the ability to implement error handling		RA

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1090	Implemented	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	SCMS PoC out of Scope	Trust Chain Broken - EE	EE shall not attempt to request or download pseudonym certificate batches, OBE identification certificate files, or RSE application certificate files, 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 anyways.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1201	SCMS PoC out of Scope	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)

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1203	Tests passed	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	Tests passed	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-1263	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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)
SCMS-1282	SCMS PoC out of Scope	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)

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1303	SCMS PoC out of Scope	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	SCMS PoC out of Scope	EE request LCCF from RA	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	Review	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	Implemented	Error reporting to EE	SCMS Components shall return error code "HTTP 500" to EEs in response to all application level errors.	Specific error codes should be hidden from EEs to prevent useful information from being provided to malicious actors	1. Standard TCP (SCMS-1090) and TLS (SCMS-977) errors shall be reported to EEs 2. All errors at the HTTP and higher levels shall	CRL Store, RA

Key	Status	Summary	Description	justification	notes	Component/s
					be HTTP 500 for RA & ECA	
SCMS-1404	SCMS PoC out of Scope	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	Implemented	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	SCMS PoC out of Scope	LCCF validation in EE	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-1455	Review	Certificate batch format	RA shall generate certificate batch files in	File format must be predefined to allow EEs to	The specific version/format of zip used is defined by the	RA

Key	Status	Summary	Description	justification	notes	Component/s
			the zip format. The file shall be created without compression and without extended attributes.	process the contents.	Apache Commons Compress version 1.11 implementation	
SCMS-1691	Review	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. 1. X 2. X shall be the lower 8-bytes of the SHA-256 hash of the device request in hexadecimal (case insensitive) 3. 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.		RA
SCMS-1692	Review	RSE application certificate files	RA shall provide each application certificate to be downloaded by	this convention gives the RSE the ability to locate the file at the RA.		RA

Key	Status	Summary	Description	justification	notes	Component/s
			EE as a X.zip file in the folder provided in the ack message to the provisioning request. • 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			

2.2.13.6.7 Design

- Step 1: RSE will check whether the time has passed at which the certificate should be available, or wait until then. RA provided that time-stamp in Step 13.1: Request RSE Application Certificate.
- Step 2: RSE and RA authenticate to each other, see below.
- Step 3: RSE downloads the local certificate chain file (see file definition in Step 18.5: Generate Global and Local Certificate Chain File) and local policy file (see Step 18.3: Generate Global Policies for EEs), and processes these files.
- Step 4: RSE downloads the application certificate file X.zip using the URL provided by RA in Step 13.1: Request RSE Application Certificate. X is the lower 8-bytes of the SHA-256 hash of the device request in hexadecimal (case insensitive).

2.2.14 Use Case 16: RSE Application and OBE Identification Certificate Revocation

Target release	Release 2.0
Document owner	Andre Weimerskirch

Reviewer	Benedikt Brecht

RSE Application and OBE Identification certificate revocation will be integrated with the to-be-awarded "Misbehavior Authority Integration" sub project as SCMS PoC release 2.0.

2.2.14.1 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.

2.2.14.2 Background and strategic fit

2.2.14.2.1 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.

2.2.14.2.2 Revocation

Revocation works as follows for 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.

2.2.14.3 Step 16.4: RSE CRL Check

Target release	Release 1.0
Document owner	Virendra Kumar
Reviewer	Benedikt Brecht

2.2.14.3.1 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.

2.2.14.3.2 Assumptions

- The RSE received a CRL as defined in Use Case 6: CRL Download

2.2.14.3.3 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.

2.2.14.3.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-786	Tests passed	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-1221	SCMS PoC out	EE processes CRL	EE shall process the updated	CRLs/CRL chunks are updated daily	This is out of scope since it	On-board Equipment (OBE), Road-

Key	Status	Summary	Description	justification	notes	Component/s
	of Scope		CRL/CRL chunk and update it's CRL within 1 minute after receiving the update CRL or CRL chunk.	and EE must always update its stored CRL in a timely fashion.	defines EE's behavior.	side Equipment (RSE)
SCMS-1222	SCMS PoC out of Scope	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 is also conform with requirement https://jira.camplc.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	SCMS PoC out of Scope	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	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 linkage seeds listed in the CRL, and comparing the calculated linkage value against the linkage value in the inspected certificate. Clause 6.4.10	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
			IEEE 1609.2-2016.	messages that are not processed, against the CRL.	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, 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-1263	SCMS PoC out of Scope	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	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
			download failed.			
SCMS-1286	SCMS PoC out of Scope	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)

2.2.14.3.5 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.

2.2.15 Use Case 18: Provide and enforce technical policies

Target release	Release 1.1
Document owner	Tom Schaffnit
Reviewer	Brian Romansky, Masafumi Sakakida

2.2.15.1 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

2.2.15.2 Background and strategic fit

The SCMS Manager needs to set up a list of SCMS Manager technical configuration choices. Those are displayed in Step 18.4: SCMS Manager Configuration Options.

The SCMS Manager will then 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. Any such changes in the technical global policies, which directly affect the EEs operating under the jurisdiction of a particular RA, may also result in an updated local policy file, specific to that particular 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 18.3: Generate Global Policies for EEs.

The OEM, or other authorized manager of EE operations, may provide any technical global or local policy changes directly affecting the EEs in a proprietary manner to EE. The minimum security requirements for these proprietary communications are out of scope for PoC, but must be established by the SCMS Manager for a deployment 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.

2.2.15.3 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

2.2.15.4 Design

- There is a global Policy Generator (PG), operated by 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, to the EEs through local policy files constructed by each RA.

- For 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.

2.2.15.5 Step 18.1: Policy configuration options

Target release	Release 1.0
Document owner	Tom Schaffnit
Reviewer	Masafumi Sakakida, Brian Romansky, Biswajit Panja

2.2.15.5.1 Configuration Options

Configuration options are available for global and local policy parameters.

2.2.15.5.1.1 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 EEs for PoC, but should be included in the global file

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
			appropriate driver warning indicator).			for PoC. There must be some point at which this transition occurs, or CRLs 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 certificates per week are all concurrently valid during that week;

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
						also affects CRL.
max_available_cert_supply	RA, PCA, EE	Maximum time with which to provision OBEs with pseudonym certificates	How many years worth of pseudo certificates 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

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
						acceptable option value limits; Local sets option value within Global limits.
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	
rse_application_cert_overlap	RA, PCA, RSE	Overlap period of RSE application certificates		Y	1 hour	

2.2.15.5.1.2 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

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
						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 certificate 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

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
						SCMS Manager?
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

2.2.15.5.2 Timely 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.

2.2.15.5.2.1 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).

2.2.15.5.2.2 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.

2.2.15.5.2.3 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.

2.2.15.5.3 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.

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	shuffle_threshold and certs_per_i_peri	For PoC, these configuration options will be	

Key	Status	Summary	Description	justification	notes	Component/s
			configuration options from the list of configuration options listed in 18.1 - Policy Configuration Options	od 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	implemented manually.	
SCMS-1226	SCMS PoC out of Scope	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	SCMS PoC out of Scope	EE Timely Limited Configuration Options: POC	For POC, EE shall support the parsing of a timely limited configuration option policy file.	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 is more than one choice, EE will only consider the first choice and assume that this first choice is always valid.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1349	SCMS PoC out	RA Timely Limited	RA shall support the use	It must be possible to		RA

Key	Status	Summary	Description	justification	notes	Component/s
	of Scope	Configuration Options	of timely limited configuration options.	define a time at which configuration option values change.		
SCMS-1350	Review	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 be 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

2.2.15.6 Step 18.2: Generate Local Policies for EEs

Target release	Release 1.1
Document owner	Tom Schaffnit
Reviewer	Biswajit Panja

2.2.15.6.1 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.

2.2.15.6.2 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 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.

The LPF shall be named according to the following format: local_policy_<globalversion>_<localversion>.abc, where abc is the encoding format (4 hex digits) for <globalversion> and <localversion>.

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.

2.2.15.6.3 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1513	Review	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	PG, RA

Key	Status	Summary	Description	justification	notes	Component/s
					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.	
SCMS-1583	SCMS PoC out of Scope	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 global policies, and include all fields in the global policy file (GPF) that are relevant to the EEs within that RA's jurisdiction.	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.		RA

Key	Status	Summary	Description	justification	notes	Component/s

SCMS-1726	Review	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 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.
				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
			For each file, the counter value shall be unique to that file. The value shall be incremented each time the file's content changes.			

2.2.15.6.4 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 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.
2. Local Policy - This section contains local parameters that are not included in the Global Policy File, but help managing 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.

2.2.15.7 Step 18.3: Generate Global Policies for EEs

Target release	Release 1.1
Document owner	Andre Weimerskirch
Reviewer	Tom Schaffnit

2.2.15.7.1 Goals

- Provide global policies that are valid for all EEs

2.2.15.7.2 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.

2.2.15.7.3 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
- 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
- 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
- RA will make the RA-specific integrated policy file (local policy file - LPF) available to all EEs within its jurisdiction.
- RA will convey changes to the global policies that affect EEs to all EEs within its jurisdiction through an updated LPF.

2.2.15.7.4 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	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.	RA

Key	Status	Summary	Description	justification	notes	Component/s
				convey them to the EEs	This might be a manual process for PoC.	

SCMS-634	Tests passed	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.
				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
			For each file, the counter value shall be unique to that file. The value shall be incremented each time the file's content changes.			
SCMS-635	Tests passed	Generation time	The global policy shall have a generation time	In addition to the identifier, the generation time helps to establish and confirm the precedence order of the global policy file	A generation time confirmation would help with version control mechanisms	PG
SCMS-636	Tests passed	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

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-637	Tests passed	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 needs to sign the global policy files to ensure authenticity	This file preparation and signing may be a manual process in PoC, since the SCMS Manager function is not being implemented	PG
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	The global policy shall be capable of changing the	Technological evolution may require longer field sizes for	Out-of-scope for PoC	PG

Key	Status	Summary	Description	justification	notes	Component/s
		and SCMS datatypes	field sizes for SCMS protocols and SCMS data types (see global policy parameters in 18.1 - Policy Configuration Options)	global policy parameters listed in 18.1 in the future; capability to change these allows for evolutionary change within the system		
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 (see global policy parameters in 18.1 - Policy Configuration Options)	Expansion of the number of components in the SCMS may require longer identifier sizes in the future for global policy parameters listed in Step 18.1: Policy configuration options; capability to change these allows for evolutionary change within the system	Out-of-scope for PoC	PG
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, listed in 18.1 - Policy Configuration Options, 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

2.2.15.7.5 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, for example 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.

2.2.15.8 Step 18.5: Generate Global and Local Certificate Chain File

Target release	Release 1.1
Document owner	Biswajit Panja
Reviewer	Tom Schaffnit, Brian Romansky, Masafumi Sakakida

2.2.15.8.1 Goals

The intention 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.

2.2.15.8.2 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 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.

2.2.15.8.3 Access & Download

To download the LCCF, EE will retrieve it from an URL defined in RA - Services View.

EE will download the files via a HTTP get request, analogous with the mechanism used to download the PCA certificate batch files.

2.2.15.8.4 Format

The GCCF shall be named according to

Key	Summary	Description	justification	notes	Component/s

SCMS-634	File name format GPF and GCCF	PG shall name GPF and GCCF using the following scheme:
		`global_policy_<gpfglobalversion>.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

The LCCF shall be named according to

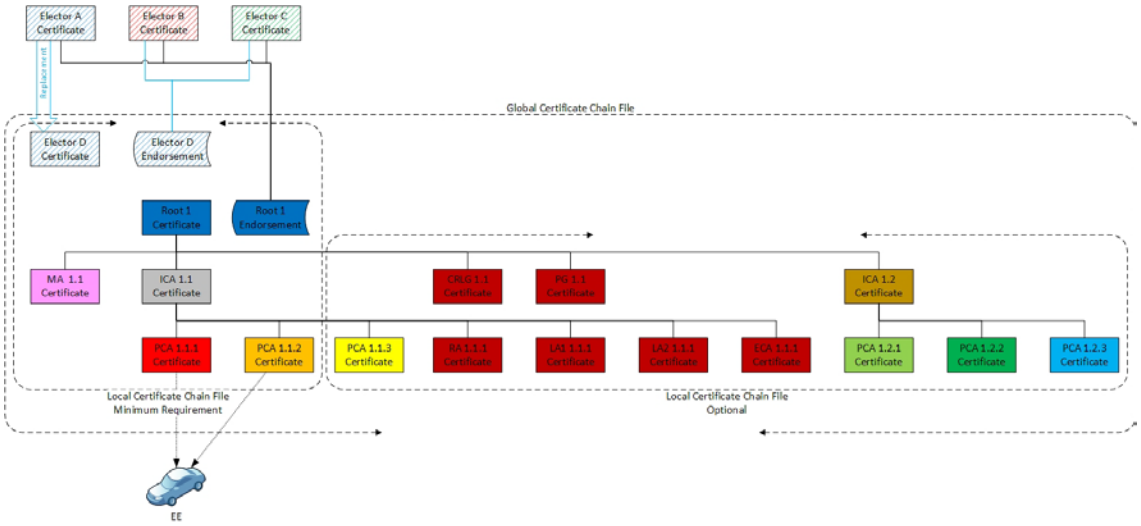
Key	Summary	Description	justification	notes	Component/s
SCMS-1726	File name format	RA shall name LPF and LCCF using the following scheme:	to have a defined	abc could e.g. be zip or tar.	RA

Key	Summary	Description	justification	notes	Component/s

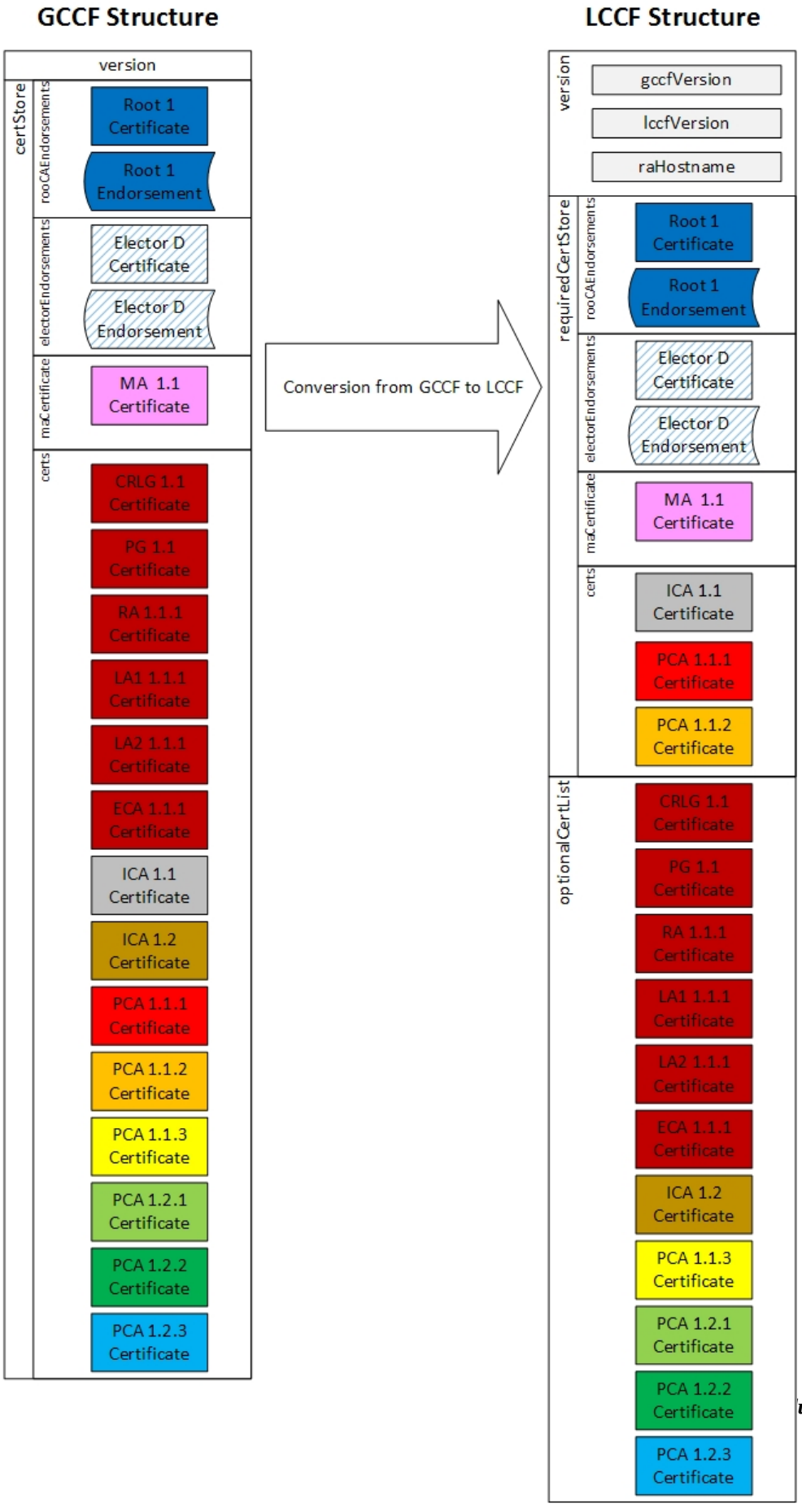
	LPF and LCCF	`local_policy_<lpfglobalversion>_<lpflocalversion>.abc`
		`local_certificate_chains_<lccfglobalversion>_<lccflocalversion>.abc`
		where:
		<*globalversion> is the version id of the file.
		Both <*globalversion> and <*localversion> is 4 hex digit counter starting at 0000.
		abc is the file 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.
			naming scheme for files to be downloaded by EEs.	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.	

Note: It is assumed all URLs and file names are case-insensitive.

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.



The following diagram shows the structure of GCCF and LCCF.


GCCF Structure
version
certStore
rooCAEndorsements
Root 1 Certificate
Root 1 Endorsement
electorEndorsements
Elector D Certificate
Elector D Endorsement
maCertificate
MA 1.1 Certificate
certs
CRLG 1.1 Certificate
PG 1.1 Certificate
RA 1.1.1 Certificate
LA1 1.1.1 Certificate
LA2 1.1.1 Certificate
ECA 1.1.1 Certificate
ICA 1.1 Certificate
ICA 1.2 Certificate
PCA 1.1.1 Certificate
PCA 1.1.2 Certificate
PCA 1.1.3 Certificate
PCA 1.2.1 Certificate
PCA 1.2.2 Certificate
PCA 1.2.3 Certificate
Conversion from GCCF to LCCF
LCCF Structure
version
gccfVersion
lccfVersion
raHostname
requiredCertStore
rooCAEndorsements
Root 1 Certificate
Root 1 Endorsement
electorEndorsements
Elector D Certificate
Elector D Endorsement
maCertificate
MA 1.1 Certificate
certs
ICA 1.1 Certificate
PCA 1.1.1 Certificate
PCA 1.1.2 Certificate
optionalCertList
CRLG 1.1 Certificate
PG 1.1 Certificate
RA 1.1.1 Certificate
LA1 1.1.1 Certificate
LA2 1.1.1 Certificate
ECA 1.1.1 Certificate
ICA 1.2 Certificate
PCA 1.1.3 Certificate
PCA 1.2.1 Certificate
PCA 1.2.2 Certificate
PCA 1.2.3 Certificate

uct

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:

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	Copy of the 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.

2.2.15.8.4.1 Creation of Local Certificate Chain File (LCCF)

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:

Element	Notes
version	This is a structure that holds the following values:

<table>
<tr><th>Element</th><th>Notes</th></tr>
<tr><td></td><td>
<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.

2.2.15.8.4.2 Use cases affected

- Use Case 1: SCMS Component Setup
- Use Case 2: OBE Bootstrapping and Use Case 12: RSE Bootstrapping
  - During bootstrap the device gets all the necessary certificates, ECA, RA, MA and LCCF
- 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
  - RA provides the updated LCCF
- Use Case 11: Backend Management

2.2.15.8.5 Requirements

Key	Status	Summary	Description	justification	notes	Component/s

SCMS-634	Tests passed	File name format GPF and GCCF	PG shall name GPF and GCCF using the following scheme:
			`global_policy_<gpfglobalversion>.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
				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
			value shall be unique to that file. The value shall be incremented each time the file's content changes.			
SCMS-711	Manual Process	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 Root CA: PG Update Global Certificate Chain File	The Policy Generator shall update the GCCF as soon as it receives the "Revoke Root CA" message and remove "Add Root CA" message of that certificate as well as remove all chains containing the revoked Root CA certificate	Having an updated certificate chain file makes verification processes at EEs more efficient.		PG
SCMS-1352	Review	Local Certificate Chain File	RA shall use appropriate information from the	to support P2P certificate distribution.	Based upon the current GCCF, each RA creates its own LCCF	RA

Key	Status	Summary	Description	justification	notes	Component/s
		(LCCF) generation	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.		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.	
SCMS-1355	Review	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	Review	Revoke Elector: PG Update Global Certificate Chain File	The Policy Generator shall update the GCCF as soon as it receives the "Revoke Elector" message and remove the "Add Elector" message of the revoked Elector.	Having an updated certificate chain file makes verification processes at EEs more efficient.		PG

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1626	Manual Process	Global Certificate Chain File Distribution	RA shall retrieve the Global Certificate Chain File (GCCF) from the Policy Generator (PG) from an URL as defined in RA - Services View. The files will be downloaded via a HTTP get request. The RA shall retrieve the GCCF at a regular interval - at least as frequently as specified in max_gpf_gccf_retrieval_interval. For PoC this interval is daily.	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. This might be a manual process for PoC.	RA
SCMS-1632	SCMS PoC out of Scope	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	Review	File name format LPF and LCCF	RA shall name LPF and LCCF using the	to have a defined naming scheme for files to be	abc could e.g. be zip or tar. Version number is required to	RA

Key	Status	Summary	Description	justification	notes	Component/s

			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 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
				downloaded by EEs.	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.	

Key	Status	Summary	Description	justification	notes	Component/s
			unique to that file. The value shall be incremented each time the file's content changes.			

2.2.16 Use Case 19: OBE Identification Certificate Provisioning

Target release	Release 1.1
Document owner	Andre Weimerskirch
Reviewer	Virendra Kumar

2.2.16.1 Goals

- Initial request of OBE identification certificates, and then subsequent top-up

2.2.16.2 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)

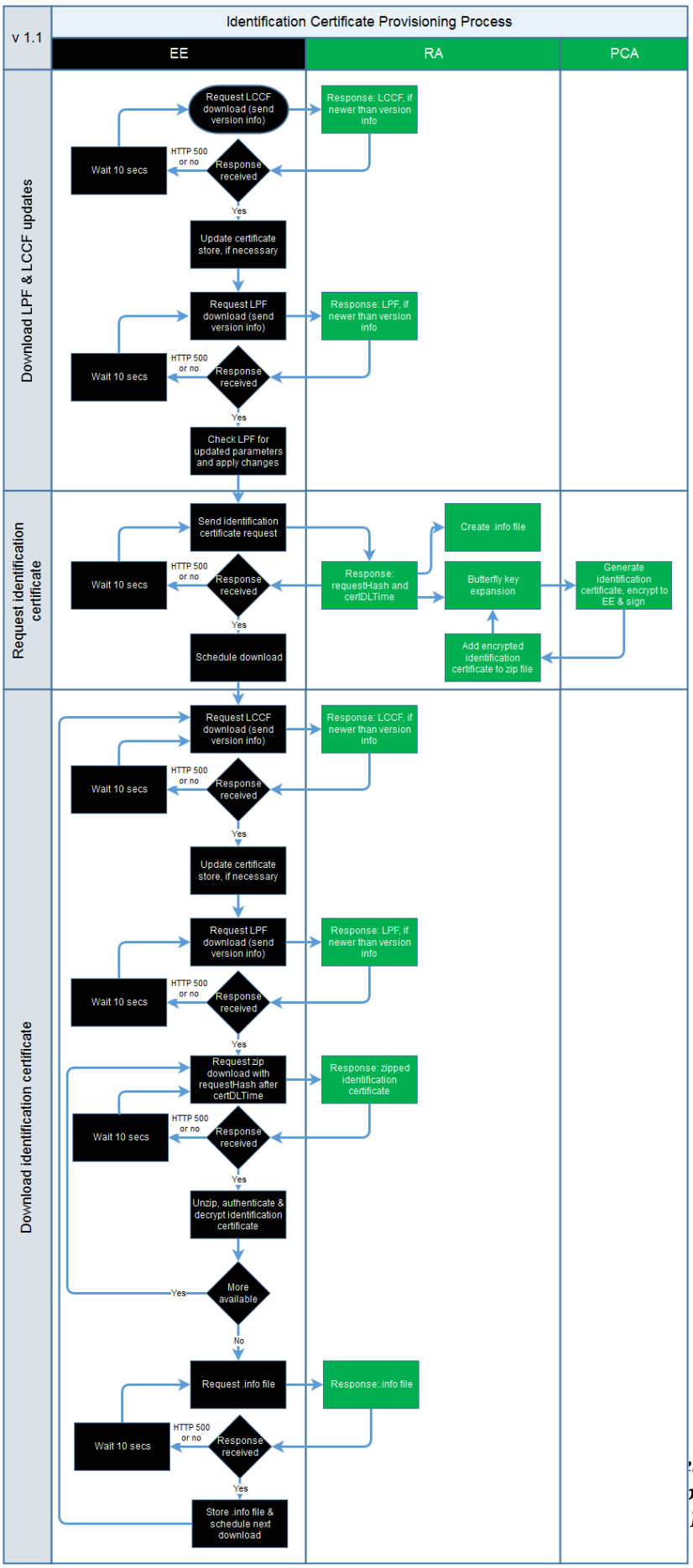
The validity duration of identification certificate is dependent on the connectivity of the OBE. Smaller validity durations will potentially reduce the number of CRL entries but require more connectivity of OBE to RA.

2.2.16.3 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.

2.2.16.4 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 requirements for a complete description of the 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 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. 1 certificate per month for month, 1 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 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
1. Step 19.3: Initial Download of OBE Identification Certificates
2. Step 19.5: Top-off OBE identification certificates

2.2.16.5 Step 19.1: Request for OBE Identification Certificates

Target release	Release 1.1
Document owner	Rekha Singoria
Reviewer	Andre Weimerskirch, Biswajit Panja

2.2.16.5.1 Goals

The goal of this use case is to define the messages and actions, which allow a device to request new identification certificates from the RA.

2.2.16.5.2 Background and Strategic Fit

The OBE decides to request 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.

2.2.16.5.3 Assumptions

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

- OBE has successfully completed Use Case 2: Bootstrapping

2.2.16.5.4 Process Steps

1. 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. 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.
2. 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 Identity Certificate Provisioning.
3. The RA ensures that the request is correct and authorized, before it starts Step 19.2: OBE Identification Certificate Generation.

2.2.16.5.5 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.

2.2.16.5.6 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-507	Tests failed	Maintain an Internal Blacklist	RA shall maintain an Internal Blacklist and keep it updated based on the communications with the MA	so that revoked EEs are not able to authenticate with the RA anymore	Every logical RA has its own internal blacklist that is not shared with anyone else. To prevent compromised components to speak with the RA the RA needs to validate against the SCMS component CRL (compare SCMS-859, https://jira.camplc.org/browse/SCMS-504~~SCMS-504~~) and the X.509 CRL (SCMS-405).	RA
SCMS-512	In Implementation	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-520	SCMS PoC out of Scope	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	because top-up certificates are generated automatically by the RA.	This is out of scope as it defines OBE behavior.	On-board Equipment (OBE)

Key	Status	Summary	Description	justification	notes	Component/s
			parameters change			
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 the RA received their request.		RA
SCMS-522	SCMS PoC out of Scope	Retry request	If the EE does not receive acknowledgement (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, it shall retry.	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	SCMS PoC out of Scope	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-524	SCMS PoC out of Scope	RA certificate	EE shall dynamically acquire RA's SCMS certificate each time it communicates with RA.	so that EE can encrypt the request to the right RA	More information is available at RA - Retrieve Registration Authority Certificate. This is out of scope as it	On-board Equipment (OBE), Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
					defines EE behavior.	
SCMS-529	Review	Store enrollment certificate and butterfly parameters	RA shall store enrollment certificate and butterfly parameters for each OBE for its lifetime, that is currently assumed to be 30 years	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-709	SCMS PoC out of Scope	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's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-754	SCMS PoC out of Scope	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)

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-768	In Implementation	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.	For more information: Generate Global and Local Certificate Chain File	RA
SCMS-776	SCMS PoC out of Scope	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	SCMS PoC out of Scope	Error code: eePolicyFile DownloadFailed	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	As the policy file is essential for the system to work correctly and contains security relevant information, it is important to have an error	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
			is none or it is corrupted).	handling whenever the EE is not able to get the latest version of that file.		
SCMS-953	SCMS PoC out of Scope	Misbehavior report: eePolicyFileDownloadFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to download the local policy file (e.g. because there is none or it is corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-954	SCMS PoC out of Scope	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-955	SCMS PoC out of Scope	Misbehavior report: eePolicyVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify the digital signature of the local policy file.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-956	SCMS PoC out	Error code: eePolicyFile	EE shall log this error code	As the policy file is essential	This is out of scope since it	On-board Equipment

Key	Status	Summary	Description	justification	notes	Component/s
	of Scope	ParsingFailed	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).	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.	defines EE's behavior.	(OBE), Road-side Equipment (RSE)
SCMS-957	SCMS PoC out of Scope	Misbehavior report: eePolicyFile ParsingFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to parse the successfully downloaded local policy file (e.g. because it is corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-987	In Implementation	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	In Implementation	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.		RA

Key	Status	Summary	Description	justification	notes	Component/s
				Retry not allowed within 2 seconds		
SCMS-990	In Implementation	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-1012	In Implementation	Error code: raWrongGlobalPolicyParameter	RA shall log "Error code: raWrongGlobalPolicyParameter", if a device sends request with parameters that are outside Global Policy configuration options.	to enable server side diagnostics and to avoid giving potential attackers relevant information. The Global Policy defines parameter and value ranges for the overall system that all participants in the system need to follow.	A request with wrong parameters might be an indication of misbehavior.	RA
SCMS-1065	In Implementation	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	SCMS PoC out	Error code: eePolicyVer	EE shall log this error code,	As the local policy file	This is out of scope since it	On-board Equipment

Key	Status	Summary	Description	justification	notes	Component/s
	of Scope	ificationFailed	if EE is not able to verify the digital signature of 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.	defines EE's behavior.	(OBE), Road-side Equipment (RSE)
SCMS-1082	In Implementation	Error code: raInvalidSignature	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	In Implementation	Error code: raRequestNotEncrypted	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	In Implementation	Error code: raInvalidCredentials	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

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1085	In Implementation	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	In Implementation	Error code: raMalformedRequest	RA shall log "Error code: raMalformedRequest", if an EE makes a malformed request not captured in SCMS-1082, SCMS-1083, 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
SCMS-1087	In Implementation	Error code: raMismatch	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	In Implementation	Error code: raInvalidTimeReceived	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-1171	SCMS PoC out of Scope	EE revoked	EE shall not attempt to download a policy file, if it is revoked.	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
SCMS-1189	SCMS PoC out of Scope	Trust Chain Broken - EE	EE shall not attempt to request or download pseudonym certificate batches, OBE identification certificate files, or RSE application certificate files, 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 anyways.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1204	Tests passed	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	RA

Key	Status	Summary	Description	justification	notes	Component/s
					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-1263	SCMS PoC out of Scope	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-1353	SCMS PoC out of Scope	EE request LCCF from RA	EE shall check for an updated Local Certificate Chain File (LCCF) upon	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	On-board Equipment (OBE), RA, Road-side Equipment (RSE)

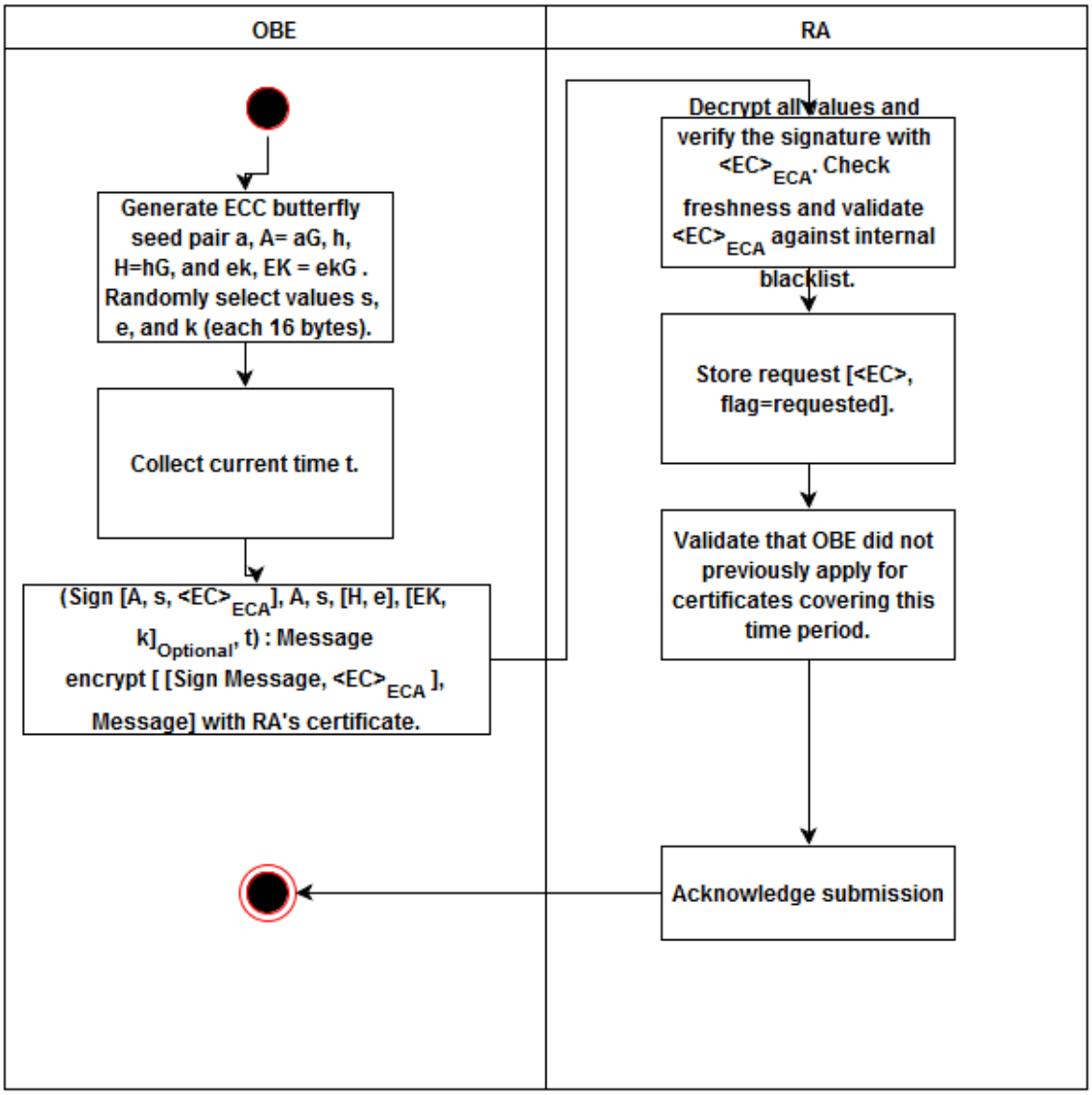
Key	Status	Summary	Description	justification	notes	Component/s
			establishing communications with the RA		endorsement for the Root CA certificate. This is out of scope since it defines EE behavior	
SCMS-1356	SCMS PoC out of Scope	EE uses internal certificate store	EE shall use its internal certificate 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 EEs behavior	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1397	Implemented	Error reporting to EE	SCMS Components shall return error code "HTTP 500" to EEs in response to all application level errors.	Specific error codes should be hidden from EEs to prevent useful information from being provided to malicious actors	• Standard TCP (SCMS-1090) and TLS (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	SCMS PoC out of Scope	EE send data via HTTP post over TCP/IP	EE shall use HTTP post to send data	to allow the SCMS endpoint to serve everything based	RA - Services View will document the actual HTTP	On-board Equipment (OBE), Road-side

Key	Status	Summary	Description	justification	notes	Component/s
			towards the RA	on HTTP protocol	post details. This is out of scope as it defines EE behavior.	Equipment (RSE)
SCMS-1405	Implemented	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	SCMS PoC out of Scope	LCCF validation in EE	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	SCMS PoC out of Scope	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	Review	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	as EE needs to know, when and where it can go to download certificates.		On-board Equipment (OBE), RA, Road-side Equipment (RSE)

Key	Status	Summary	Description	justification	notes	Component/s
			for all devices serviced by an specific RA) Case: Certificate Provisioning Request Reject • HTTP 500 error code			

2.2.16.5.7 Design



2.2.16.5.7.1 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 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.

2.2.16.5.7.1.1 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.

2.2.16.5.7.1.2 Message Contents

The EE shall use the ASN.1 defined for creating the Request Certificate message, details can be found at EE to 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)

2.2.16.5.7.2 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.

2.2.16.5.7.2.1 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.

2.2.16.5.7.2.2 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.

2.2.16.5.7.2.3 Message Contents

The RA shall use the ASN.1 defined for creating the Request Acknowledge message, can be found at EE to 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

2.2.16.5.7.3 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 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.

2.2.16.6 Step 19.3: Initial Download of OBE Identification Certificates

Target release	Release 1.1
Document owner	Andre Weimerskirch
Reviewer	Virendra Kumar

2.2.16.6.1 Goals

The goal is to provide a reliable, secure and timely method for certified devices to download OBE identification certificates.

2.2.16.6.2 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. is valid for a period consistent with its associated application(s) and
4. a local certificate chain file containing all PCA certificate chains required to validate the identification certificates, but not the policy file.

2.2.16.6.3 Assumptions

- OBE has successfully completed Step 19.1: Request for OBE Identification Certificates.
- RA retrieved the issued certificates from PCA, zipped, and stored them in a folder for OBE to download.

2.2.16.6.4 Process Steps

1. 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, EE applies all changes to its trust-store (necessary for PCA Certificate Validations).
   b. If there is an updated LPF, EE applies those changes.
2. OBE downloads the new OBE identification certificates using the API documented in RA - Download Identity Certificate
3. OBE downloads .info file using the API documented in RA - Download .info file

2.2.16.6.5 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.

2.2.16.6.6 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-411	SCMS PoC out of Scope	EE Authentication to RA for Request	The EE shall authenticate its requests with its enrollment certificate. These messages shall include a timestamp (which the EE will obtain from its GPS reference) 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.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-459	In Implementation	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.	RA

Key	Status	Summary	Description	justification	notes	Component/s
					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 failed	Maintain an Internal Blacklist	RA shall maintain an Internal Blacklist and keep it updated based on the communications with the MA	so that revoked EEs are not able to authenticate with the RA anymore	Every logical RA has its own internal blacklist that is not shared with anyone else. To prevent compromised components to speak with the RA the RA needs to validate against the SCMS component CRL (compare SCMS-859, https://jira.camplc.org/browse/SCMS-504~~SCMS-504~~) and the X.509 CRL (SCMS-405).	RA
SCMS-512	In Implementation	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 before any other communication process starts.	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	RA

Key	Status	Summary	Description	justification	notes	Component/s
					SCMS certificate to identify itself. EE authenticates via its IEEE 1609.2 enrollment certificate. The details of the authentication process are defined E-RA Communications - General Guidance	
SCMS-517	Implemented	Tunneling through LOP	RA shall provide downloads only via a LOP hardware interface, which removes all location information from the incoming request.	to anonymize the location of EEs.		RA
SCMS-522	SCMS PoC out of Scope	Retry request	If the EE does not receive acknowledgement (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, it shall retry.	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	SCMS PoC out of Scope	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.	On-board Equipment (OBE), RA, Road-side Equipment (RSE)
SCMS-539	SCMS PoC out of Scope	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	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
				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 E-RA Communications - General Guidance		
SCMS-541	SCMS PoC out of Scope	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-543	Closed	Individual certificate downloads	RA shall support individual certificate batch, or certificate file,	The design allows download of individual certificate batches, or files, to avoid that an		RA

Key	Status	Summary	Description	justification	notes	Component/s
			downloads by EEs.	EE needs to download all certificates each time. This also allows easier 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	In Implementation	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	RA

Key	Status	Summary	Description	justification	notes	Component/s
					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 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	to recover from a loss of certificates at the device level (e.g., disk corruption).		RA

Key	Status	Summary	Description	justification	notes	Component/s
			the certificates are not expired.			
SCMS-709	SCMS PoC out of Scope	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	In Implementation	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	For more information: Generate Global and Local Certificate Chain File	RA

Key	Status	Summary	Description	justification	notes	Component/s
				newer LCCF if available.		
SCMS-952	SCMS PoC out of Scope	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-953	SCMS PoC out of Scope	Misbehavior report: eePolicyFileDownloadFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to download the local policy file (e.g. because there is none or it is corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-954	SCMS PoC out of Scope	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-955	SCMS PoC out	Misbehavior report: eePolicyVer	EE shall initiate a misbehavior	to enable server side misbehavior detection.	This is out of scope since it	On-board Equipment (OBE), Road-

Key	Status	Summary	Description	justification	notes	Component/s
	of Scope	ificationFailed	report to MA with the observed error, if EE is not able to verify the digital signature of the local policy file.		defines EE's behavior.	side Equipment (RSE)
SCMS-956	SCMS PoC out of Scope	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-957	SCMS PoC out of Scope	Misbehavior report: eePolicyFileParsingFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to parse the successfully downloaded local policy file (e.g. because it is corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-958	SCMS PoC out of Scope	Error code: eeConnectionFailed	EE shall log this error code, if it cannot connect to RA	to enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side

Key	Status	Summary	Description	justification	notes	Component/s
			because there is a connection timeout.			Equipment (RSE)
SCMS-964	In Implementation	Error code: raNoCertFileAvailable	RA shall return status code HTTP 500 to EE, if certificate batch is not available and log "Error code: raNoCertFileAvailable.	to enable EE side error handling.		RA
SCMS-965	SCMS PoC out of Scope	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-966	SCMS PoC out of Scope	Misbehavior report: eeCertFileDownloadFailed	EE shall initiate a misbehavior report to MA, if EE is not able to download certificate files (e.g. because there is none or it is corrupted).	to enable server side misbehavior detection.	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-969	SCMS PoC out of Scope	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-970	SCMS PoC out of Scope	Misbehavior report: eeCertFileDecryptionFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to decrypt an encrypted certificate.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)
SCMS-971	SCMS PoC out of Scope	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-972	SCMS PoC out of Scope	Misbehavior report: eeCertVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify a certificate.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-973	SCMS PoC out of Scope	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-974	SCMS PoC out of Scope	Misbehavior report: eeCertContentFalse	EE shall initiate a misbehavior report to MA	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side

Key	Status	Summary	Description	justification	notes	Component/s
			with the observed error, if EE is not able to parse a certificate, or if the certificate has wrong content.			Equipment (RSE)
SCMS-976	In Implementation	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	In Implementation	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	In Implementation	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	SCMS PoC out of Scope	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-980	SCMS PoC out of Scope	Misbehavior report: eeAuthenticationFailed	EE shall initiate a misbehavior report to MA with the observed error, if RA-to-EE	to enable server side misbehavior detection.	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
			authentication fails.			
SCMS-981	In Implementation	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	Tests passed	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-983	In Implementation	Error code: raNoInfoFileAvailable	RA shall return status code HTTP 500, if it is not able to provide a current .info file and log "Error code: raNoInfoFileAvailable".	to enable EE side error handling.		RA
SCMS-984	SCMS PoC out of Scope	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's behavior.	On-board Equipment (OBE)
SCMS-985	SCMS PoC out of Scope	Misbehavior report: eeInfoFileDownloadFailed	OBE shall initiate a misbehavior report to MA with the observed error,	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)

Key	Status	Summary	Description	justification	notes	Component/s
			if OBE is not able to download the .info file (e.g. because there is none or it is corrupted).			
SCMS-1065	In Implementation	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-1090	Implemented	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-1171	SCMS PoC out of Scope	EE revoked	EE shall not attempt to download a policy file, if it is revoked.	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	SCMS PoC out of Scope	Trust Chain Broken - EE	EE shall not attempt to request or download pseudonym certificate batches, OBE	To reduce resources, since RA will reject request anyways.	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
			identification certificate files, or RSE application certificate files, 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-1201	SCMS PoC out of Scope	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	Tests passed	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	Tests passed	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.	RA

Key	Status	Summary	Description	justification	notes	Component/s
					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	SCMS PoC out of Scope	OBE downloads .info file	OBE shall download the .info file each time OBE tries to download 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	SCMS PoC out of Scope	EE contacts RA for certificate download	EE shall try to download certificates any time after the	to avoid wasting resources by trying to download	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side

Key	Status	Summary	Description	justification	notes	Component/s
			time provided by the time-stamp in the .info file that has been recovered last time EE tried to download, or downloaded certificates.	certificates before they are available.	The timestamp shall be in the IEEE 1609.2 Time32 format (the number of (TAI) seconds since 00:00:00 UTC, January 1, 2004).	Equipment (RSE)
SCMS-1228	Review	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 • 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)	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, the 4 billion-th certificate is stored in X_EE6B2800.zip, and so on.	RA

Key	Status	Summary	Description	justification	notes	Component/s
			• Where the extension is .zip in lowercase			
SCMS-1263	SCMS PoC out of Scope	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-1303	SCMS PoC out of Scope	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	SCMS PoC out of Scope	EE request LCCF from RA	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	SCMS PoC out of Scope	EE uses internal certificate store	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 EEs behavior	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1377	Review	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	Implemented	Error reporting to EE	SCMS Components shall return error code "HTTP 500" to EEs in response to all application level errors.	Specific error codes should be hidden from EEs to prevent useful information from being provided to malicious actors	1. Standard TCP (SCMS-1090) and TLS (SCMS-977) errors shall be reported to EEs 2. 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	SCMS PoC out of Scope	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	Implemented	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	SCMS PoC out of Scope	LCCF validation in EE	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-1455	Review	Certificate batch format	RA shall generate certificate batch files in the zip format. The file shall be created without compression	File format must be predefined to allow EEs to process the contents.	The specific version/format of zip used is defined by the Apache Commons Compress version 1.11 implementation	RA

Key	Status	Summary	Description	justification	notes	Component/s
			and without extended attributes.			
SCMS-1637	Review	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 • 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	There is only one OBE identification certificate allowed at any given time (except for overlap) and therefore there should only be one certificate per zip file.	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 billion-th certificate is stored in X_EE6B2800, and so on.	RA
SCMS-1639	SCMS PoC out	Download certificate batches	OBE shall not attempt to download	To reduce resource usage by not	1. This is out of scope as it	On-board Equipment (OBE)

Key	Status	Summary	Description	justification	notes	Component/s
	of Scope		certificate batches for i-value periods more than max_available_cert_supply in the future	attempting to download certificate batches that do not exist.	defines EE behavior. 2. This is the OBE counterpart of https://jira.campllc.org/browse/SCMS-547~~SCMS-547~~	

2.2.16.6.7 Design

- Step 1: EE and RA authenticate to each other, see EE-RA Communications - General Guidance.
- Step 2: EE downloads the local certificate chain file (LCCF) (see Step 18.5: Generate Global and Local Certificate Chain File) and the local policy file (LPF) (see Step 18.2: Generate Local Policies for EEs).
- Step 3: EE downloads certificate files X_i.zip, where X is the lower 8-bytes of the SHA-256 hash of device request in hexadecimal (case insensitive) and i is an iterator, starting at 0, in hexadecimal (case insensitive). EE downloads either all available files X_i.zip, or as many as possible. Each X_i.zip includes a single identification certificate file X_i.
- Step 4: EE downloads the .info file (generated and updated by RA). The .info file contains the time when a new certificate will be available. In order for the EE to determine the earliest time, which a new certificate will be available for download, the RA maintains a signed file in each device specific repository. This file will contain the date and time the RA is predicted to add new certificates to the device repository. The .info contains a single IEEE 1609.2 Time32 timestamp that the EE will use to schedule a subsequent “top-up” download. The file is 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 (case insensitive).

2.2.16.7 Step 19.5: Top-off OBE identification certificates

Target release	Release 1.1
Document owner	Andre Weimerskirch
Reviewer	Virendra Kumar

2.2.16.7.1 Goals

The goal is to provide a reliable, secure and timely method for certified devices to download credentials.

2.2.16.7.2 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.

2.2.16.7.3 Assumptions

- OBE has successfully completed Step 19.1: Request for OBE Identification Certificates
- OBE has successfully completed Step 19.3: Initial Download of OBE Identification Certificates
- RA retrieved the issued certificates from PCA, zipped, and stored them in a folder for OBE to download.

2.2.16.7.4 Process Steps

- OBE checks that, and if necessary waits until, the current time matches or is after the timestamp given in the .info file.
- 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.
  - If there is an updated LCCF, OBE applies all changes to its trust-store (necessary for PCA Certificate Validations).
  - If there is an updated LPF, OBE applies those changes.
- OBE downloads the new OBE identification certificates.
- OBE downloads .info file using the API documented in RA - Download .info file

2.2.16.7.5 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.

2.2.16.7.6 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-411	SCMS PoC out of Scope	EE Authentication to RA for Request	The EE shall authenticate its requests with its enrollment certificate. These messages shall	Messages from EEs to an RA must be secure against replay attacks. The signed time stamp from the	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
			include a timestamp (which the EE will obtain from its GPS reference) to avoid replay attacks on the RA.	EE enables the RA to validate the freshness of EE requests.		
SCMS-507	Tests failed	Maintain an Internal Blacklist	RA shall maintain an Internal Blacklist and keep it updated based on the communications with the MA	so that revoked EEs are not able to authenticate with the RA anymore	Every logical RA has its own internal blacklist that is not shared with anyone else. To prevent compromised components to speak with the RA the RA needs to validate against the SCMS component CRL (compare SCMS-859, https://jira.camplc.org/browse/SCMS-504~~SCMS-504~~) and the X.509 CRL (SCMS-405).	RA
SCMS-509	In Implementation	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	so that computing resources are not wasted by generating certificates for revoked devices		RA

Key	Status	Summary	Description	justification	notes	Component/s
			RA's internal blacklist.			
SCMS-512	In Implementation	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
SCMS-515	Closed	RA requires EE	The RA shall require EE	to ensure that only a proper EE	It is not cost effective to	RA

Key	Status	Summary	Description	justification	notes	Component/s
		authentication	authentication before any other communication process starts.	can send requests, download certificates or files.	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 E-RA Communications - General Guidance	
SCMS-517	Implemented	Tunneling through LOP	RA shall provide downloads only via a LOP hardware interface, which removes all location information from the incoming request.	to anonymize the location of EEs.		RA
SCMS-522	SCMS PoC out of Scope	Retry request	If the EE does not receive acknowledgement (TCP ACK, RA accept request ACK, HTTP 500, or HTTP 304)	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
			within a specified amount of time, currently set to be 10 sec from the time of request, it shall retry.			
SCMS-523	SCMS PoC out of Scope	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	SCMS PoC out of Scope	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 E-RA Communications - General Guidance	This is out of scope since it defines EE's behavior.	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,	to improve reliability of the download protocol.		RA

Key	Status	Summary	Description	justification	notes	Component/s
			even if EE switches the IP address.			
SCMS-576	Tests passed	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 earliest the next download is allowed to happen.	Timestamp in .info file is dynamically calculated base on system load. PoC scope will be to update .info file for non-revoked EEs only.	RA
SCMS-709	SCMS PoC out of Scope	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's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-768	In Implementation	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	For more information: Generate Global and Local Certificate Chain File	RA

Key	Status	Summary	Description	justification	notes	Component/s
				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	SCMS PoC out of Scope	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-953	SCMS PoC out of Scope	Misbehavior report: eePolicyFileDownloadFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to download the local policy file (e.g. because there is none or it is corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-954	SCMS PoC out	Error code: eePolicyVer	EE shall log this error code	to enable EE side diagnostics.	This is out of scope since it	On-board Equipment

Key	Status	Summary	Description	justification	notes	Component/s
	of Scope	ificationFailed	in EE's error log file, if EE is not able to verify the digital signature of the local policy file.		defines EE's behavior.	(OBE), Road-side Equipment (RSE)
SCMS-955	SCMS PoC out of Scope	Misbehavior report: eePolicyVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify the digital signature of the local policy file.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-956	SCMS PoC out of Scope	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-957	SCMS PoC out of Scope	Misbehavior report: eePolicyFileParsingFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to parse	to enable server side misbehavior detection.	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 successfully downloaded local policy file (e.g. because it is corrupted).			
SCMS-958	SCMS PoC out of Scope	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	In Implementation	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	In Implementation	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	In Implementation	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	SCMS PoC out of Scope	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-980	SCMS PoC out of Scope	Misbehavior report: eeAuthenticationFailed	EE shall initiate a misbehavior report to MA with the observed error, if RA-to-EE authentication fails.	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1065	In Implementation	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-1163	SCMS PoC out of Scope	OBE revoked	A revoked OBE shall not attempt to download pseudonym certificate batches/OBE identification certificate files.	To reduce resource usage, since RA will reject request anyways.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)
SCMS-1164	SCMS PoC out of Scope	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	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	On-board Equipment (OBE)

Key	Status	Summary	Description	justification	notes	Component/s
				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).	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 or next time period, the OBE is allowed to make a download attempt at any time.	
SCMS-1171	SCMS PoC out of Scope	EE revoked	EE shall not attempt to download a policy file, if it is revoked.	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	SCMS PoC out of Scope	Trust Chain Broken - EE	EE shall not attempt to request or download pseudonym certificate batches, OBE identification certificate files, or RSE application certificate files,	To reduce resources, since RA will reject request anyways.	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
			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	Tests passed	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	Tests passed	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	RA

Key	Status	Summary	Description	justification	notes	Component/s
					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	SCMS PoC out of Scope	OBE downloads .info file	OBE shall download the .info file each time OBE tries to download 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	SCMS PoC out of Scope	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)

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1282	SCMS PoC out of Scope	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-1289	SCMS PoC out of Scope	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 OBE identification certificates that are not currently verified and stored on the device. This is to prevent repeated downloads of the same content.		On-board Equipment (OBE)
SCMS-1291	SCMS PoC out of Scope	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	SCMS PoC out of Scope	EE request LCCF from RA	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	SCMS PoC out of Scope	EE uses internal certificate store	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 EEs behavior	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1377	Review	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	SCMS PoC out of Scope	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	Implemented	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	Keep track of which authorizatio	The RA shall keep track of how far into	This allows revoked devices to be removed	This is an optimization for CRL handling	RA

Key	Status	Summary	Description	justification	notes	Component/s
	of Scope	n (pseudonym, ID, application) certificates are downloaded	the future each device has downloaded its certificates.	from the CRL (or deprioritized for inclusion on the CRL) once they exhaust the set of certificates that they have downloaded.	and therefore out of scope for PoC implementation.	
SCMS-1421	SCMS PoC out of Scope	LCCF validation in EE	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-1637	Review	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 • X shall be the lower 8-bytes of the SHA-256 hash of the device request in hexadecimal (case insensitive)	There is only one OBE identification certificate allowed at any given time (except for overlap) and therefore there should only be one certificate per zip file.	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 billion-th certificate is stored in X_EE6B2800, and so on.	RA

Key	Status	Summary	Description	justification	notes	Component/s
			• i is a file iterator in hexadecimal starting at 0 (case insensitive) • Where there is no extension			
SCMS-1639	SCMS PoC out of Scope	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 of https://jira.camplc.org/browse/SCMS-547~~SCMS-547~~	On-board Equipment (OBE)

2.2.16.7.7 Design

1. Step 1: OBE will use .info file from the last certificate batch download to determine the time when certificates will be available and a download can be attempted.
2. Step 2: OBE and RA authenticate to each other.
3. Step 3: OBE downloads the local certificate chain file (LCCF) and local policy file (LPF).
   a. Step 3.1: The RA records the time stamp of the connection from the EE.
   b. Step 3.2: If pre-generation of certificates has been stopped, RA will resume pre-generation. This step is out of scope for PoC.
4. Step 4: OBE will download all or as many as possible, certificate files that it does not already have stored locally. It is the responsibility of the OBE to determine which certificate files to download (i.e. skip files that have already been successfully downloaded and processed).
5. Step 5: OBE downloads the .info file (generated and updated by RA). The .info file contains the time when the next certificate batches will be available.

2.2.16.7.8 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, 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.

3 RA - 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. Because of #1, the response from services that create resources will not contain URLs to the created resources as is customary in pure RESTful services.
3. Cacheability of responses may not be used due to the nature of the problem domain.
4. 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.

In the Quality of Service tables below 'Estimated Instance Latency' will be determined later based on trial implementation benchmarking. From these values, we will derive the values for 'Estimated # of instances'.

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.

3.2 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 Identity Certificate Provisioning	/provision-identity-certificate
Download Identity 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

3.3 Services Summary for RA to other SCMS Component Communications

Service Name	<PATH>
RA - Blacklist Enrollment Certificate By HPCR	/blacklist-by-hpcr
RA - Blacklist Enrollment Certificate By RIF	/blacklist-by-rif
Retrieve Linkage Chain Identifiers	/retrieve-linkage-chain-identifiers

3.4 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.

PATH	/provision-pseudonym-certificate-batch
HTTP Method	POST
HTTP Request Body	ASN1 serialized SecuredPseudonymCertProvisioningRequest

PATH	/provision-pseudonym-certificate-batch
HTTP Response Body	SecuredPseudonymCertProvisioningAck 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 of the requested batch, and a *certDLURL* property containing the URL where the batch can be downloaded.

3.4.1 Preconditions

- Policy referenced in the request message is previously known.
- PLV Cache has at least one PLV chain.
- Device is not revoked.

3.4.2 Postconditions

None

3.4.3 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 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
Maximum System Latency	2 seconds/batch request	2 seconds/batch request	2 seconds/batch request	2 seconds/batch request
Batch Preparation Time	Between 1 week and 1 month for Top Up batches. Not defined for initial batch (factory bypass).	Between 1 week and 1 month for Top Up batches. Not defined for initial batch (factory bypass).	Between 1 week and 1 month for Top Up batches. Not defined for initial batch (factory bypass).	Between 1 week and 1 month for Top Up batches. Not defined for initial batch (factory bypass).

3.4.4 Quality of Protection

- RA protects access with HTTPS (TLS V1.2) via port 8892
- 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.

3.5 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 an .info file for each device containing this information.

PATH	**/download/info**
HTTP Method	GET
HTTP Request Body	Empty
HTTP Request Headers	HTTP Header 'Download-Req' containing a Base64 encoded ASN1 serialized *SecuredScmsPDU* containing an *EndEntityRaInterfacePDU*, 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.

3.5.1 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.)

3.5.2 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.

3.5.3 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 / 604800 seconds/week = 14 requests / second	(8,500,000 new vehicles + 34,000,000 existing vehicles) / 604800 seconds/week = 70 requests / second	(8,500,000 new vehicles + 68,000,000 existing vehicles) / 604800 seconds/week = 126 requests / second	(8,500,000 new vehicles + 153,000,000 existing vehicles) / 604800 seconds/week = 267 requests / second
Maximum System Latency	A file access with validation of device enrollment certificate.	0.07 seconds / request	0.01 seconds / request	0.008 seconds / request	0.004 seconds / request
Estimated Instance Latency		TBD	TBD	TBD	TBD
Estimated # of instances		TBD	TBD	TBD	TBD

3.5.4 Quality of Protection

- RA protects access with HTTPS (TLS V1.2) via port 8892
- 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.

3.6 RA - Download local policy file

EEs use this service to download a local policy file.

PATH	**/download/policy/local**
HTTP Method	GET
HTTP Request Body	Empty
Parameters	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: If-None-Match: "lp_01_01.oer" This is used to prevent the same policy file from being downloaded by the device multiple times.
Response	File containing the local policy. The file name returned is of the form: lp_<X>_<Y>.<Z> Where: • X is the Policy Id, up to 32 octets in hexadecimal (this could be a truncated SHA-256 hash of policy file content) • Y is the i-value in hexadecimal (when the policy becomes active, for easier roll-over from an old to a new policy) • 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.

3.6.1 Preconditions

None

3.6.2 Postconditions

- Returned file contains policy that the device will use.

3.6.3 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 policy in the same week.	8,500,000 new vehicles / 604800 seconds/week = **14** requests / second	(8,500,000 new vehicles + 34,000,000 existing vehicles) / 604800 seconds/week = **70** requests / second	(8,500,000 new vehicles + 68,000,000 existing vehicles) / 604800 seconds/week = **126** requests / second	(8,500,000 new vehicles + 153,000,000 existing vehicles) / 604800 seconds/week = **267** requests / second
Maximum System Latency		**0.07** seconds / request	**0.014** seconds / request	**0.008** seconds / request	**0.004** seconds / request

3.6.4 Quality of Protection

- RA protects access with HTTPS (TLS V1.2) via port 8892
- Supports at a minimum OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256

3.7 RA - Download Pseudonym Certificate Batch

OBEs use this service to download a batch of Pseudonym Certificates for a specific time period.

PATH	/download/batch
HTTP Method	GET
HTTP Request Body	Empty
HTTP Request Headers	HTTP Header 'Download-Req' containing a Base64 encoded ASN1 serialized *EndEntityRaInterfacePDU* containing an *AuthenticatedDownloadRequest* with a *filename* property of the form [0-9A-F]{16}_[0-9A-F]{1,8}.zip where: 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: From byte offset 500 to 700: Range : bytes=500-700 Starting from byte offset 1000 to the end: Range : bytes=1000-

PATH	/download/batch
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.

3.7.1 Preconditions

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

3.7.2 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:
   e. 37_0
   f. 37_1
   g. ...
   h. 37_12
   i. 37_13

3.7.3 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 the initial	With no previous year vehicles: 17m x 52 weeks * 3	With and two years worth of old vehicles (34 million): 17m (new) + 34m (old)	With four years worth of old vehicles (68 million): 17m (new) + 68m (old)	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
	3 year's worth of certificates (156 files) plus old cars downloading one year's worth of certificates (52 files).	years = 2,652 million files Divided by the number of seconds in a year: 2,652 million files / 31,557,600seconds = 85 files per second	Old cars only download one year's worth of certificates (52 files) while new cars download 3 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 /31,557,600seconds = ~ 141 files per second	Old cars only download one year's worth of certificates (52 files) while new cars download 3 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 /31,557,600seconds = ~ 197 files per second	system out of which, 153 million will be old vehicles: 17m (new) + 153m (old) The new cars will be downloading 3 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 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 / 31,557,600seconds = ~ 337 files per second
Maximum System Latency	A database look up and	0.0118seconds / download	0.00709 seconds / download	0.00508 seconds / download	0.00297 seconds / download

Quality Metric	Rationale	1 Year	3 Years	5 Years	10 Years
	a database insert.				

3.7.4 Quality of Protection

- RA protects access with HTTPS (TLS V1.2) via port 8892
- 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.

3.8 RA - Retrieve Registration Authority Certificate

EEs use this service to refresh its locally cached RA certificate.

PATH	/retrieve-ra-certificate
HTTP Method	POST
HTTP Request Body	ASN1 serialized *SecuredRACertRequest* PDU Message.
HTTP Response Body	Serialized IEEE 1609.2 certificate

3.8.1 Preconditions

None

3.8.2 Postconditions

- The 1609 certificate is returned to the device.

3.8.3 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	8,500,000 new vehicles / 604800 seconds/week	(8,500,000 new vehicles + 34,000,000 existing	(8,500,000 new vehicles + 68,000,000 existing	(8,500,000 new vehicles + 153,000,000 existing

Quality Metric	Rationale	1 Year	3 Years	5 Years	10 Years
	existing vehicles need to refresh their copy of the RA certificate in one week.	= 14 requests / second	vehicles) / 604800 seconds/week = 70 requests / second	vehicles) / 604800 seconds/week = 126 requests / second	vehicles) / 604800 seconds/week = 267 requests / second
Maximum System Latency		0.07 seconds / request	0.014 seconds / request	0.008 seconds / request	0.004 seconds / request

3.8.4 Quality of Protection

- RA protects access with HTTPS (TLS V1.2) via port 8892
- Supports at a minimum OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256

3.9 RA - Request Identity Certificate Provisioning

OBEs use this service to request a new identity certificates. After the initial batch is requested, subsequent batches are automatically provisioned.

PATH	/provision-identity-certificate
HTTP Method	POST
HTTP Request Body	ASN1 serialized SecuredIdCertProvisioningRequest
HTTP Response Body	SecuredIdCertProvisioningRequestAck 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 of the requested batch, and a *certDLURL* property containing the URL where the batch can be downloaded.

3.9.1 Preconditions

- Policy referenced in the request message is previously known.
- EE is not revoked.

3.9.2 Postconditions

None

3.9.3 Quality of Protection

- RA protects access with HTTPS (TLS V1.2) via port 8892
- 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.

3.10 RA - Download Identity Certificate

OBEs use this service to download a previously requested Identity Certificate.

PATH	**/download/identity-certificate**
HTTP Method	GET
HTTP Request Body	Empty
HTTP Request Headers	HTTP Header 'Download-Req' containing a Base64 encoded ASN1 serialized *EndEntityRaInterfacePDU* containing an *AuthenticatedDownloadRequest* with a *filename* property of the form "*X_i.zip*" where X shall be the lower 8-bytes of the SHA-256 hash of the device request in hexadecimal, and i is a file iterator in hexadecimal starting at 0 (both are case insensitive). 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: From byte offset 500 to 700: Range : bytes=500-700 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.

3.10.1 Preconditions

- The requested certificate has already been generated.
- The requesting device has not been previously revoked.

3.10.2 Postconditions

- The tar file corresponding to the certificate specified in the request URL is returned.
- The content of the tar file is organized as a flat directory containing 1 file named as in:
  - X_i.crt

3.10.3 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.

3.10.4 Quality of Protection

- RA protects access with HTTPS (TLS V1.2) via port 8892
- 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.

3.11 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.

PATH	**/provision-application-certificate**
HTTP Method	POST
HTTP Request Body	ASN1 serialized SecuredAppCertProvisioningRequest
HTTP Response Body	SecuredAppCertProvisioningRequestAck 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 of the requested batch, and a *certDLURL* property containing the URL where the batch can be downloaded.

3.11.1 Preconditions

- Policy referenced in the request message is previously known.
- EE is not revoked.

3.11.2 Postconditions

None

3.11.3 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.

3.11.4 Quality of Protection

- RA protects access with HTTPS (TLS V1.2) via port 8892
- 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.

3.12 RA - Download Application Certificate

RSEs use this service to download a previously requested Application Certificate.

PATH	**/download/application-certificate**
HTTP Method	GET
HTTP Request Body	Empty
HTTP Request Headers	HTTP Header 'Download-Req' containing a Base64 encoded ASN1 serialized *EndEntityRaInterfacePDU* containing an *AuthenticatedDownloadRequest* with a *filename* property of the form "*X.zip"* where X shall be the lower 8-bytes of the SHA-256 hash of the device request in hexadecimal. 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 zip file corresponding to the requested batch. If a Range header is present, the specified bytes of the referenced file.

3.12.1 Preconditions

- The requested certificate has already been generated.
- The requesting device has not been previously revoked.

3.12.2 Postconditions

1. The file corresponding to the certificate specified in the request URL is returned.
2. Contents 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.
   a. X
   b. X shall be the lower 8-bytes of the SHA-256 hash of the device request in hexadecimal (case insensitive)
   c. Where there is no extension

3.12.3 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.

3.12.4 Quality of Protection

- RA protects access with HTTPS (TLS V1.2) via port 8892
- 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.

3.13 RA - Download Local Certificate Chain File

EEs use this service to download a local certificate chain file.

PATH	**/download/local-certificate-chain**
HTTP Method	GET
HTTP Request Body	Empty
Parameters	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 or file extension. For example: If-None-Match: "local_certificate_chains_01_03" This is used to prevent the same file from being downloaded by the device multiple times.
Response	File containing the local certificate chains. The file name returned is of the form: local_certificate_chains_<X>_<Y>.<Z> Where: • X is the global version, i.e., the *cert_chain_file_id* parameter found in the Global Policy File. • 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.

3.13.1 Preconditions

None

3.13.2 Postconditions

1. Returned file contains SCMS certificates chains that the device will use.

3.13.3 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 / 604800 seconds/week = 14 requests / second	(8,500,000 new vehicles + 34,000,000 existing vehicles) / 604800 seconds/week = 70 requests / second	(8,500,000 new vehicles + 68,000,000 existing vehicles) / 604800 seconds/week = 126 requests / second	(8,500,000 new vehicles + 153,000,000 existing vehicles) / 604800 seconds/week = 267 requests / second
Maximum System Latency		0.07 seconds / request	0.014 seconds / request	0.008 seconds / request	0.004 seconds / request

3.13.4 Quality of Protection

- RA protects access with HTTPS (TLS V1.2) via port 8892
- 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.

3.14 RA - Submit Misbehavior Report

EEs use this service to submit a Misbehavior Report (MBR) that RA will forward to the Misbehavior Authority.

PATH	/process-misbehavior-report
HTTP Method	POST
HTTP Request Body	ASN1 serialized SecuredMisbehaviorReport
HTTP Response Body	Empty

3.14.1 Preconditions

1. EE is not revoked.

3.14.2 Postconditions

None

3.14.3 Quality of Service

For PoC the volume for this interface will be estimated by the currently underway CR - GMBD project, but is not expected to have significant impact on system throughput requirements.

3.14.4 Quality of Protection

- RA protects access with HTTPS (TLS V1.2) via port 8892
- 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.

4 MA - Services View

Please refer to the Common - Services View section for an introduction of the Services View.

4.1 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.

4.2 Services Summary for EE-MA Communications

Service Name	<PATH>
Download CRL	/download-crl/

4.3 Services Summary for MA to other SCMS Component Communications

Service Name	<PATH>
Download GCCF File	/download-gccf/

4.4 MA - Download CRL

EEs use this service to download the CRL File.

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

4.4.1 Preconditions

- CRL has been generated by the CRL Generator and stored in the CRL Store

4.4.2 Postconditions

1. Returned file contains ASN.1 Serialized Composite CRL File as defined by the CompositeCrl ASN.1 definition

4.4.3 Quality of Protection

- RA protects access with HTTPS (TLS V1.2) via port 8892
- 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.

5 Test Vectors

5.1 Purpose

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.

5.2 Test Vectors Location

Test vectors are located at http://stash.campllc.org/projects/SCMS/repos/crypto-test-vectors/

5.3 Overview

The following is the README in that Stash repository (https://stash.campllc.org/projects/SCMS/repos/crypto-test-vectors/browse/README.md?at=refs/heads/master):

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.

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

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

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

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

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

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

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

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

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

Other files:

- radix.py:
- array.py: utility scripts for printing the output
- ecc.py: Elliptic Curve Cryptosystems core computations

5.3.1 Hash-based functions:

5.3.1.1 Key Derivation Function, KDF2

- This function is used to expand/derive keys from a 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

5.3.1.2 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

5.3.2 AES-based functions:

5.3.2.1 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

5.3.3 ECC functions:

5.3.3.1 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

5.3.3.2 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

5.3.3.3 Implicit Certificate Generation and Public/Private Keys Reconstruction

- Implicit certificates are employed for pseudonym certificates, enrollment certificates, ... (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.

5.3.4 Linkage Values and Butterfly Key Expansion Functions

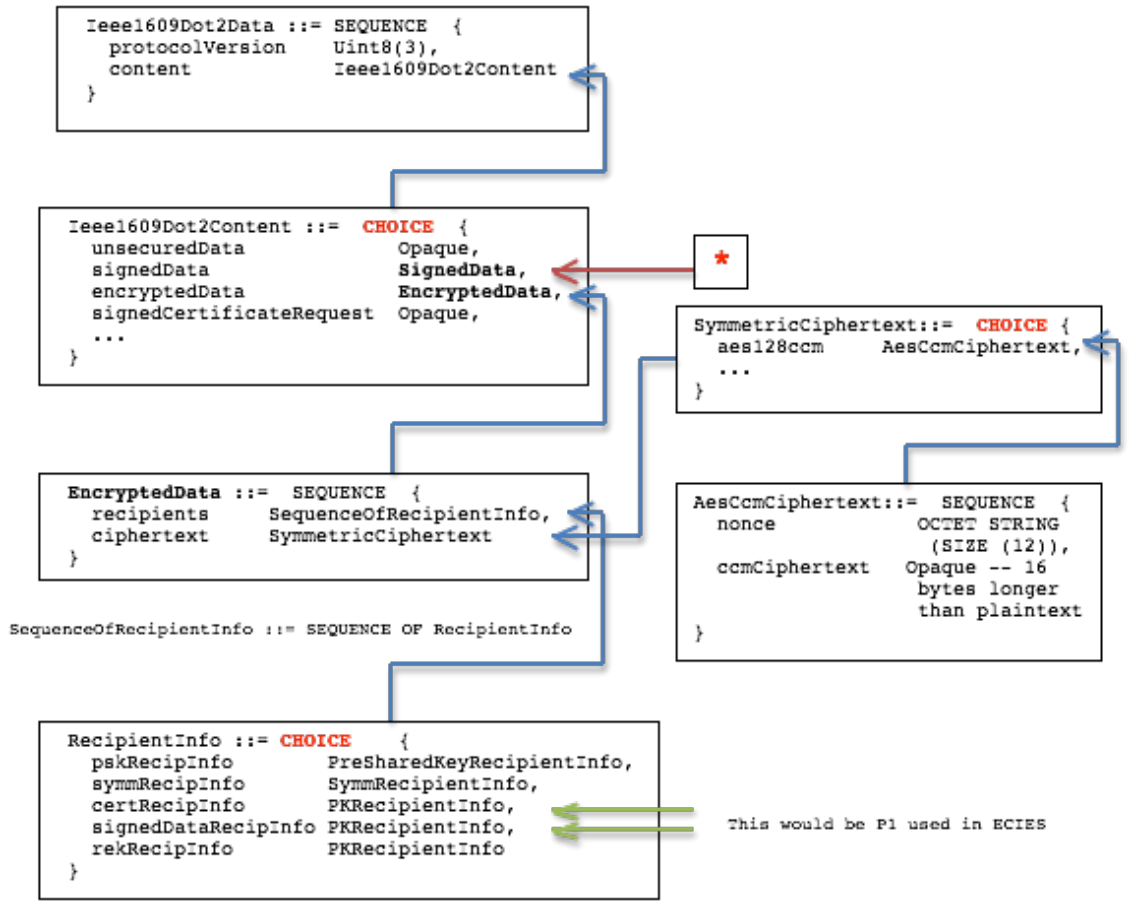
- These are as specified in Cryptographic Primitives

5.4 1602.2 and SCMS ASN.1 Objects

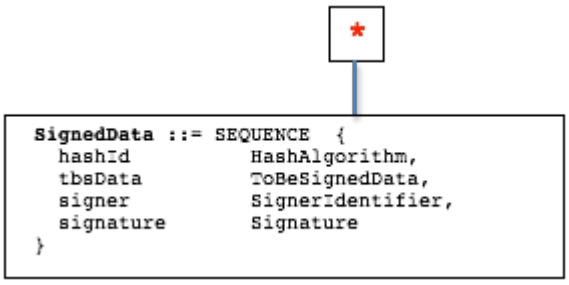
scms-protocol.asn

```
SecuredScmsPDU ::= Ieee1609Dot2Data
```

1609.2-schema.asn



See ECIES diagram and Notes on Encrypted Data below as well as PKRecipientInfo and EciesNistP256EncryptedKey ASN.1 objects in 1609dot2-schema.asn and EciesNistP256EncryptedKey in 1609dot2-base-types.asn to see how the outputs of ECIES are encoded in the RecipientInfo.



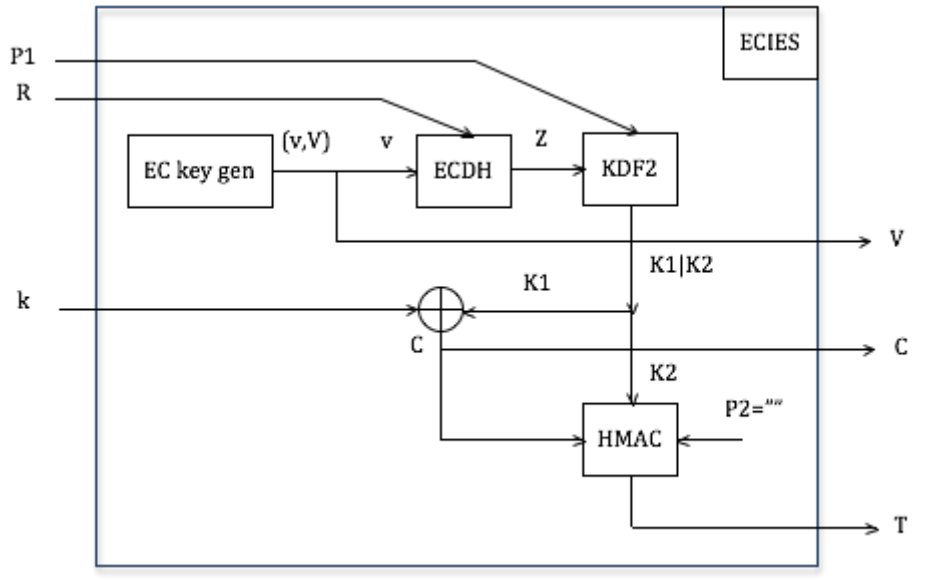
Example of SignedData from scms-protocol.asn:

```
SignedPseudonymCertProvisioningAck ::= SecuredScmsPDU (WITH COMPONENTS {...,
  content (WITH COMPONENTS {...,
    signedData  (WITH COMPONENTS {...,
      tbsData (WITH COMPONENTS {...,
        payload (WITH COMPONENTS {...,
          data (WITH COMPONENTS {...,
             content (WITH COMPONENTS {
                unsecuredData (CONTAINING ScopedPseudonymCertProvisioningAck)
            })
          })
        }),
        headerInfo (WITH COMPONENTS {...,
          psid (SecurityMgmtPsid),
          generationTime ABSENT,
          expiryTime ABSENT,
          generationLocation ABSENT,
          certLearningRequest ABSENT,
          missingCrlIdentifier ABSENT,
          encryptionKey ABSENT
        })
      })
    })
  })
})
```

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

Defined in ee-ra.asn:
See EndEntityRaInterfacePDU and
RaEePseudonymCertProvisioningAckMsg

5.5 ECIES Encryption as in 1609.2, Sec 5.3.5



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.

Appendix A. Glossary

Acronym	Full form / description
3D	Three-Dimensional
AES	Advanced Encryption Standard
ASD	Aftermarket Safety Device
ASN.1	Abstract Syntax Notation One
BMC	Backend Management Commands
BSM	Basic Safety Message
BSS	Basic Service Set
BSW	Blind Spot Warning
C2C-CC	Car-2-Car Communication Consortium
CA	Certificate Authority
CAMP	Crash Avoidance Metrics Partnership
CAN	Controller Area Network
CCH	Control Channel
CCM	Counter with Cipher-Block-Chaining MAC (Mode for authenticated encryption)
CFR	Code of Federal Regulations
CME	Certificate Management Entity
CONVERGE	Communication Network Vehicle Road Global Extension
CPR	Certificate Provisioning Request
CPU	Central Processing Unit
CRACA	Certificate Revocation Authorizing Certificate Authority
CRLG	Certificate Revocation List Generator
CRL	Certificate Revocation List
CS	Certificate Store
CTS	Clear To Send
DCM	Device Configuration Manager
DER	Distinguished Encoding Rules
DF	Data Frame
DNPW	Do Not Pass Warning

Acronym	Full form / description
DNS	Domain Name Server
DOT	Department of Transportation
DSRC	Dedicated Short-Range Communications
DVI	Driver Vehicle Interface
ECA	Enrollment Certificate Authority
ECB	Electronic Code Book (block cipher mode of operation)
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECIES	Elliptic Curve Integrated Encryption Scheme
ECQV	Elliptic Curve Qu-Vanstone Certificate Scheme
ECU	Electronic Control Unit
EDCA	Enhanced Distributed Channel Access
EE	End-entity
EEBL	Emergency Electronic Brake Lights
EGNOS	European Geostationary Navigation Overlay Service
EK	Encryption Key
Elector	Electors together (or at least a quorum of them) have the power to change and manage the trust relationship of the PKI system by adding or revoking Root Certificate Authorities and Electors. This establishes a distributed management scheme, like a democracy, that contains within itself the power to replace an established hierarchy, and does not succumb to a single failure.
ETSI	European Telecommunications Standards Institute
FCC	Federal Communication Commission
FCW	Forward Collision Warning
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standards
FM	Frequency Modulation
FMVSS	Federal Motor Vehicle Safety Standards
FQDN	Fully Qualified Domain Name
GCCF	Global Certificate Chain File
GD	Global Detection
GHz	Gigahertz
GMBD	Global Misbehavior Detection
GNSS	Global Navigation Satellite System
GP	General Purpose
GP-CPU	General Purpose Central Processing Unit

Acronym	Full form / description
GPF	Global Policy File
HCF	Hybrid Coordination Function
HD	Hybrid-Digital
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
HV	Host Vehicle
Hz	Hertz
IBLM	Internal Blacklist Manager
ICA	Intermediate Certificate Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IEEE	IEEE (The Institute of Electrical and Electronics Engineers)
ILS	Initial Linkage Seed
IMA	Intersection Movement Assist
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
IPv6	Internet Protocol Version 6
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.
JPO	Joint Program Office
LA	Linkage Authority
LCCF	Local Certificate Chain File
LCI	Linkage Chain Identifier
LCM	Local Certificate Management
LCW	Lane Change Warning
LOP	Location Obscurer Proxy
LPF	Local Policy File
LS	Linkage Seed
LTA	Left Turn Assist
LV	Linkage Value

Acronym	Full form / description
MA	Misbehavior Authority
MAC	The Media Access Control (MAC) Layer is one of two sublayers that make up the Data Link Layer of the 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.
MD	Model Deployment
MHz	Megahertz
MIB	Management Information Base
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
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute for Standards and Technology
NMEA	National Marine Electronics Association
NTP	Network Time Protocol
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.
OTA	Over The Air
PCA	Pseudonym Certificate Authority
PDU	Protocol Data Unit
PG	Policy Generator
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.

Acronym	Full form / description
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
PP	Path Prediction
PPS	Pulse Per Second
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	Registration Authority
RCA	Root Certificate Authority
RIF	Revocation Identifier Field
RF	Radio Frequency
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
RSU	Roadside Unit
RTS	Request To Send
RV	Remote Vehicle
SAE	Society of Automotive Engineers
SAP	Service Access Point
SBAS	Satellite Based Augmentation System
SCH	Service Channel
SCMS	Security Credential Management System
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).

Acronym	Full form / description
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	Station
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.
TCotSCMSM	Technical Component of the SCMS Manager
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).
TRNG	True Random Number Generator
TSF	Time Synchronization Function
Tx	Transmit
USDOD	United States Department of Defense
USDOT	United States Department of Transportation
UTC	Coordinated Universal Time, abbreviated as UTC, is the primary time standard by which the world regulates clocks and time.
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2V-SE	Vehicle to Vehicle System Engineering and Vehicle Integration Research for Deployment (CAMP Project)
VIIC	Vehicle Infrastructure Integration Consortium (CAMP project)
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.

Acronym	Full form / description
VSA	Vendor Specific Action
VSC-A	Vehicle Safety Communication - Applications
VSC3	Vehicle Safety Communications 3 (CAMP Consortium)
VSC5	Vehicle Safety Communications 5 (CAMP Consortium)
VSCS	Vehicle Safety Communications Security (Studies)
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 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).
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	WAVE Management Entity
WSM	WAVE Short Message
WSA	WAVE Service Advertisement
WSMP	WAVE Short Message Protocol