CAMP LLC

Vehicle Safety Communications 5 (VSC5)

Security Credential Management System Proof–of–Concept Implementation

EE Requirements and Specifications Supporting SCMS Software Release 1.0

DRAFT

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

January 11, 2016

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

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

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.

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Table of Contents

Notice and Disclaimer i
1 Introduction 1
2 Requirements and Specifications 1
2.1 Document header and status 1
2.2 Common Requirements 2
2.2.1 Time Synchronization 2
2.2.2 Certificate Types 4
2.2.3 EE-SCMS Core Communication Requirements 12
2.2.4 EE-RA Communications - General Guidance 20
2.3 RA - Services View 21
2.3.1 General Notes 21
2.3.2 RA - Provision Pseudonym Certificate Batch 21
2.3.3 RA - Download .info file 23
2.3.4 Download local policy file 25
2.3.5 RA - Download global policy file 27
2.3.6 RA - Download Pseudonym Certificate Batch 28
2.3.7 RA - Retrieve Registration Authority Certificate 31
2.3.8 RA - Provision Identity Certificate 32
2.4 Requirements by Use Case 33
2.4.1 On-board Equipment (OBE) use cases 33
2.4.2 Road-side Equipment (RSE) use cases 34
2.4.3 Requirements to be updated / added with the next revision 34
2.4.4 Use Case 2: Bootstrapping 34
2.4.5 Use Case 3: Initial Provisioning of Pseudonym Certificates 35
2.4.6 Use Case 5: Misbehavior Reporting 110
2.4.7 Use Case 6: CRL Download 115
2.4.8 Use Case 8: OBE Revocation 120
2.4.9 Use Case 9: Refresh Pseudonym Certificates 181
2.4.10 Use Case 10: Update Pseudonym Certificate Request Parameters 219
2.4.11 Use Case 12: RSE bootstrapping 224
2.4.12 Use Case 13: RSE Application Certificate Provisioning 240
2.4.13 Use Case 14: RSE Misbehavior Reporting 278

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

2.4.14 Use Case 15: RSE CRL Check 282
2.4.15 Use Case 16: RSE Application and OBE Identification Certificate Revocation .. 283
2.4.16 Use Case 17: Refresh RSE Application Certificates 302
2.4.17 Use Case 18: Create / provide global, local and SCMS Manager policies 312
2.4.18 Use Case 19: OBE Identification Certificate Provisioning 342
2.5 Modifications to Crypto Primitives 402
2.5.1 Use of AES as a Derivation Function 402
2.5.2 Butterfly Expansion Function 404
2.5.3 Pseudonym Certificate Validity 405
2.5.4 Clock Time corresponding to i=0 405
2.5.5 Encryption of Pre-linkage Values by LA for PCA 406
2.5.6 Misbehavior Investigation: PCA returns encrypted pre-linkage values to MA 406
2.5.7 Crypto Primitives affecting End-Entity 406
Appendix A. EE Requirements with "EE-Handshake" label 1
Appendix B. EE Requirements Table 3
Appendix C. Glossary 11

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

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 Document header and status

All use cases and use case steps have their own header that are exported as well to show the status, authors, reviewers etc. of this sub section. All requirements have a link to JIRA issues which show their current status (e.g. SCMS-500-Firewall whitelist In Implementation):

- "Review" means the requirements is currently under review by the Software Team

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

- "In Implementation" means the requirement is currently in implementation by the Software Team
- "Implemented" means the Software Team finished the implementation as well as development / unit tests
- "Ready for Testing" means 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
- "Closed" means the requirement is implemented and successfully tested.
- "Manual Process" means 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" means 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.

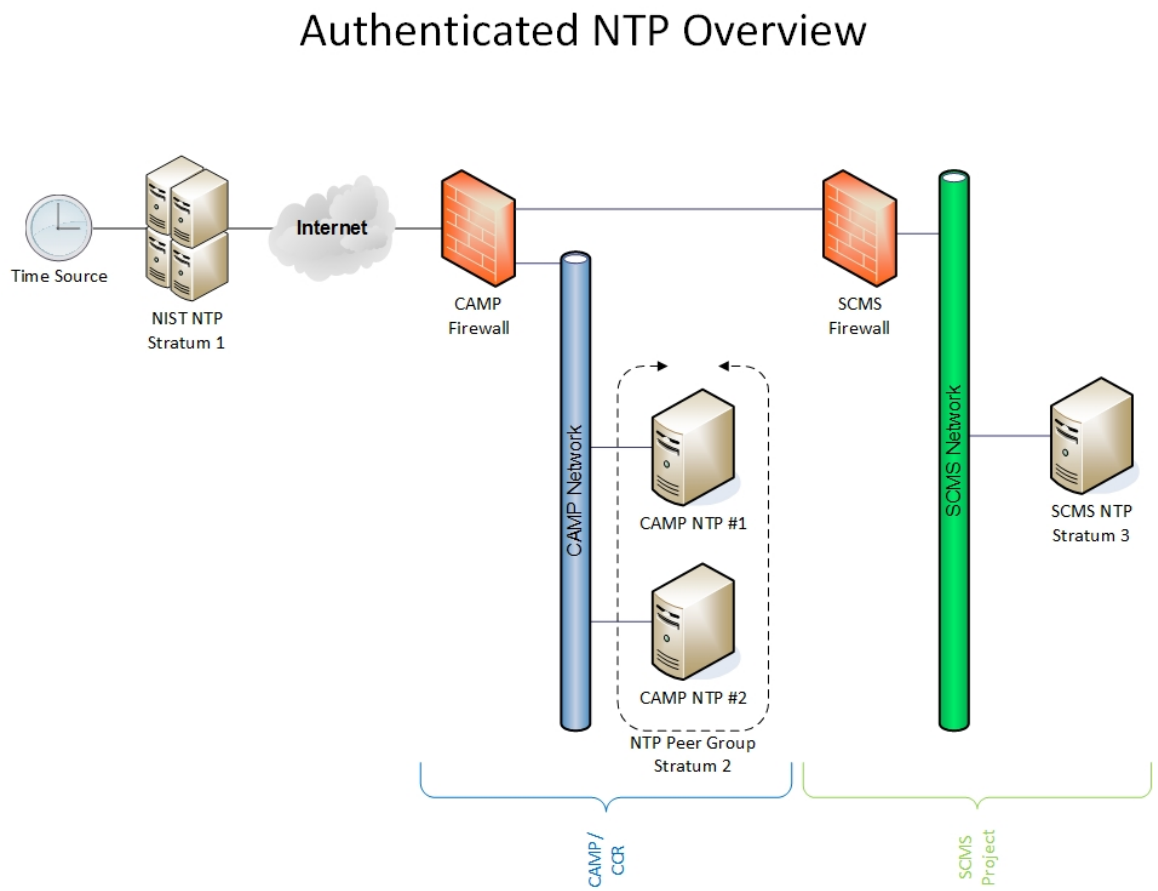
2.2 Common Requirements

2.2.1 Time Synchronization

- All servers and related devices shall use authenticated NTP as the time source.
- CAMP shall configure two servers as an NTP peer group.
- The CAMP peer group will use the NIST authenticated NTP service as its time source.
- The SCMS project shall designate one server (can be shared with other functions) as the time source.
- Under typical conditions, the SCMS server will use the CAMP peer group as its time source. For specific test cases, the SCMS server can be disconnected from the CAMP source and the time manually adjusted.
- Key infrastructure (firewall, jump server, etc) should use actual time whenever possible even if a specific test requires altering the SCMS time. For this reason, core infrastructure may need to use the CAMP servers directly.

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary



2.2.1.1 Configuration

Hostname	IP address	Auth key (M type)
NTP1.campllc.org	192.168.8.5	xxx
NTP2.campllc.org	192.168.8.6	xxx

2.2.1.2 EE time synchronization

For OBEs time synchronization is defined in J2945.1 in the following requirements:

- 6.2.4-V2V-POSTIM-SYSTIMCOORD-001
- 6.2.4-V2V-POSTIM-SYSTIMCOORD-002

For RSEs time synchronization is defined in USDOT's "DSRC Roadside Unit (RSU) Specifications Document" version 4.0 in the following requirements:

- USDOT_RSU- Req_513- v002
- USDOT_RSU- Req_514- v001

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

2.2.2 Certificate Types

There are several types of certificates that are used in the V2X system. These are generated (and in many cases can also be revoked) by SCMS components:

- **OBE**: All the OBE certificates are of **implicit** type to save storage space and over-the-air bytes.
    - **Enrollment**: **cert-profile.asn [30:88]**
      https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/cert-profile.asn?at=refs/heads/master

      Enrollment certificate is like a passport for the OBE that it uses to request other certificates: pseudonym and identification certificates. It doesn't have an encryption key. It is provided to OBE during its **bootstrap** process. Each enrollment cert has at least one PSID; however, an OBE can't have more than one enrollment cert associated with a particular (PSID, SSP) combination. In cases where an enrollment cert has more than one PSID, the corresponding apps are expected to be similar in nature. Such groupings of PSIDs in an enrollment cert are likely to be related to policy decisions to be made by the SCMS Manager. Enrollment certificates have extremely **long validity** periods (for this project it is **40 years**) expected to cover OBE's full operational lifetime. Revocation of enrollment certificate is done through **internal blacklist** at RA.
    - **Pseudonym: cert-profile.asn [91:142]**
      https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/cert-profile.asn?at=refs/heads/master

      Pseudonym certificates are used by an OBE primarily for BSM authentication and misbehavior reporting, and hence don't 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 this project, an OBE is given **3 years** worth of certificates at a time, where validity period of each certificate is **1 week**, and **20 certificates** are valid simultaneously at any time. Also, the certificates for consecutive time periods overlap for a period of **1 hour**. 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.
    - **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, so these certificates (just like enrollment and pseudonym certificates) don't have encryption keys. 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

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

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.

- **RSE**: All the RSE certificates are of **implicit** type to save storage space and over-the-air bytes.
    - **Enrollment**: Enrollment certificate is like a passport for the RSE that it uses to request application certificates. It doesn't have an encryption key. It is provided to RSE during its **bootstrap** process. Each enrollment cert has at least one PSID; however, an RSE can't have more than one enrollment cert associated with a particular (PSID, SSP) combination. In cases where an enrollment cert has more than one PSID, the corresponding apps are expected to be similar in nature. Such groupings of PSIDs in an enrollment cert are likely to be related to policy decisions to be made by the SCMS Manager. Enrollment certificates have extremely **long validity** periods (for this project it is **40 years**) 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.
    - **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.
- **SCMS Component**: The elector, Root CA, PCA, and ICA certificates, are of explicit type to support P2P distribution, and all other certificates are of implicit type. 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 .
    - **Root CA: cert-profile.asn [280:348]** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/cert-profile.asn?at=refs/heads/master

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

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 doesn't 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 the root CA can issue (or, authorize someone to issue) a CRL to revoke root CA certificate.
Root CA certificate doesn't have an encryption key, as the root CA is mostly offline and doesn't accept any incoming messages, whether encrypted or not. The root CA certificate needs to be made available to everyone in the system. For this project, root CA certificate has a validity period of **40 years**, and the certificates for consecutive periods overlap for a period of **3 years**. 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.

- **ICA: cert-profile.asn [351:438]**
  https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/cert-profile.asn?at=refs/heads/master

  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.

- **ECA: cert-profile.asn [145:210]**
  https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/cert-profile.asn?at=refs/heads/master

  As mentioned above, ECA certificates are of **implicit** type as they don't 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 don't 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 (e.g., 40 years) 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.

- **PCA: cert-profile.asn [213:278]**
  https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/cert-profile.asn?at=refs/heads/master

  PCA certificates can be used to only issue certificates to end-entities including OBEs and RSEs. These certificates don't 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

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

periods that are at least as long as the longest validity certificates issued using them, which is currently 3 years. Revocation of PCA certificate is done through **CRLs** issued by CRL Generator.

- **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, i.e. same as the CRL validity, which is currently 1 day. As CRL signing happens only once per CRL frequency (currently 1 day), there is no need for CRL Generator certificates to overlap. For a given CRACA and CRL series, there is **only 1** valid CRL Generator certificate at any time.
- **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.
- **Other**: These include LA, MA, and RA certificates. These certificates **cannot** be used to issue certificates. These certificates don't 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:
  - **LA: cert-profile.asn [507:553]** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/cert-profile.asn?at=refs/heads/master

    Can be small as LAs don't interact with end-entities (for this project it is **1 day**).
  - **RA: cert-profile.asn [441:504]** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/cert-profile.asn?at=refs/heads/master

    Must be long enough so that end-entities can successfully make a certificate provisioning request after being bootstrapped (for this project it is **1 week**).
  - MA: Needs to be long so that end-entities don't need to retrieve these certificates very often (for this project it is **10 years**).

Revocation of these certificates is done through **CRLs** issued by CRL Generator.

The following table provides an overview of the EE certificate types. 'x' describe mandatory features, and '(x)' describe optional features.

	1. OBE Enrollment Certificate	2. OBE Pseudonym Certificate	3. OBE Identification Certificate	4. RSE Enrollment Certificate	5. RSE Application Certificate

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

	1. OBE Enrollment Certificate	2. OBE Pseudonym Certificate	3. OBE Identification Certificate	4. RSE Enrollment Certificate	5. RSE Application Certificate	
					5.a RSE with connectivity	**5. b 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 certs 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. PCA shall have ability to encrypt, but the encryption is optional. The SCMS Manager approves the corresponding policy.	1 per time period, issue longer time periods than for certificate type 5a, RSE generates public/private key pair and provides public-key to RA. PCA shall have ability to encrypt, but the encryption is optional. The SCMS Manager approves the corresponding policy.
Revocation	RA blacklist	leverage linkage values	add cert digests of all issued certs (can be more than one)	RA blacklist	do not renew certificates	add cert digest of all issued certs (can be more than one)
Shuffle in		X				

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

	1. OBE Enrollment Certificate	2. OBE Pseudonym Certificate	3. OBE Identification Certificate	4. RSE Enrollment Certificate	5. RSE Application Certificate	
RA						
CRL for End-entity Devices (certificates of this type can be listed on CRL)		X	X			X
Simultaneous Validity for given PSID		X	Only allow minimal overlap to account for critical events			
Linkage Values		X				
Butterfly Keys		X	X			
Continued Generation		X	X			
Issuing Certificates for multiple time periods		X	X			
Pseudonymity	X	X				
Misbehavior reporting		X	X		X	X
Non-Traceability		X				
Encryption					X	

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

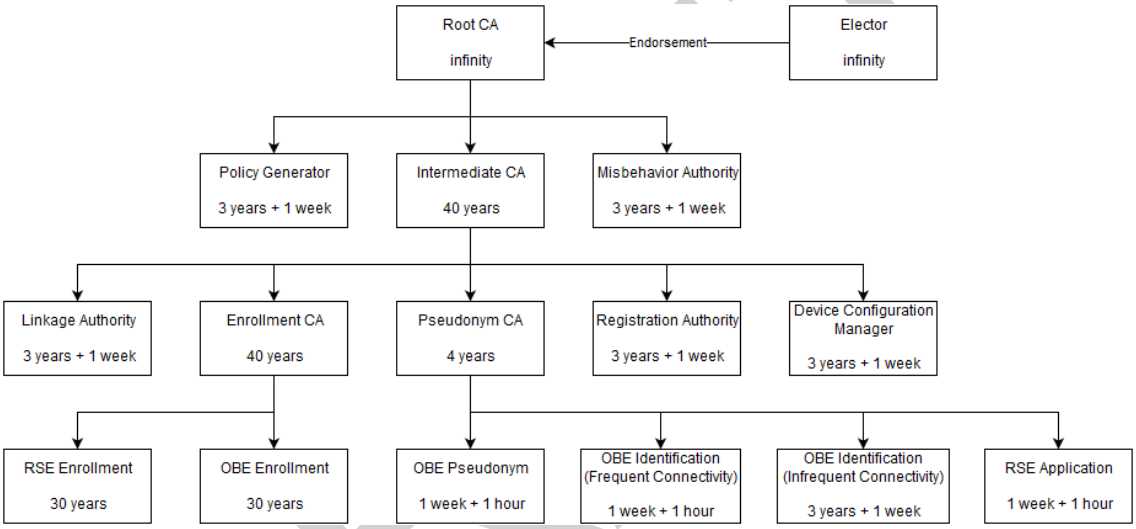
	1. OBE Enrollment Certificate	2. OBE Pseudonym Certificate	3. OBE Identification Certificate	4. RSE Enrollment Certificate	5. RSE Application Certificate	
key						

The following table provides the certificate expiration and renewal periods to be used for POC.

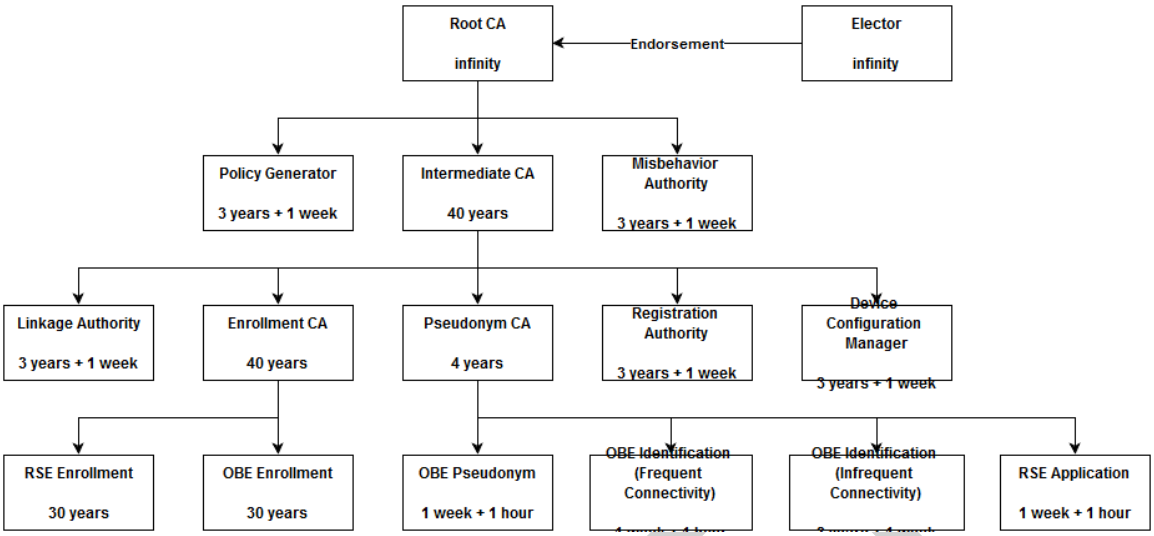
	Issuer	Expiration	Request for Renewal	Start of validity for renewal	Number of concurrently valid certificates
OBE Enrollment	ECA	30 years	N/A	N/A	1
OBE Pseudonym	PCA	1 week + 1 hour	Anytime	1 week	20 + 20 (for just 1 hour)
OBE Identification (frequent connectivity)	PCA	1 week + 1 hour	Anytime	1 week	1 + 1 (for just 1 hour)
OBE Identification (infrequent connectivity)	PCA	3 years + 1 week	Anytime	3 years	1 + 1 (for just 1 week)
RSE Enrollment	ECA	30 years	N/A	N/A	1
RSE Application	PCA	1 week + 1 hour	Anytime	1 week	1 + 1 (for just 1 hour)
DCM	ICA	3 years + 1 week	Anytime	3 years	1 + 1 (for just 1 week)
ECA	ICA	40 years	Anytime	10 years	1 + 3
RA	ICA	3 years + 1 week	Anytime	3 years	1 + 1 (for just 1 week)
LA	ICA	3 years + 1 week	Anytime	3 years	1 + 1 (for just 1 week)
PCA	ICA	4 years	Anytime	1 year	1 + 3
ICA	Root CA	40 years	Anytime	10 years	1 + 3

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

	Issuer	Expiration	Request for Renewal	Start of validity for renewal	Number of concurrently valid certificates
MA	Root CA	3 years + 1 week	Anytime	3 years	1 + 1 (for just 1 week)
Policy Generator	Root CA	3 years + 1 week	Anytime	3 years	1 + 1 (for just 1 week)
Root CA	Self	45 years	Anytime	15 years	1
Elector	Self	45 years	Anytime	15 years	1



The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary



2.2.3 EE-SCMS Core Communication Requirements

2.2.3.1 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.
- 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.

2.2.3.2 Background and strategic fit

2.2.3.2.1 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.

2.2.3.2.2 TLS Connection

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

2.2.3.2.3 1609.2 Encrypting and/or Signing

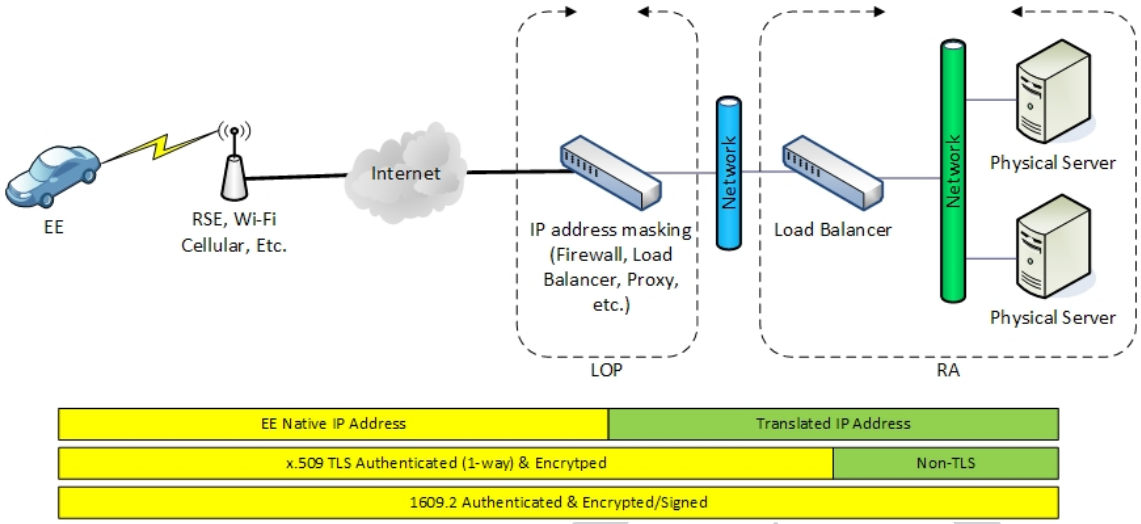
- Provides application layer security and privacy.

DRAFT

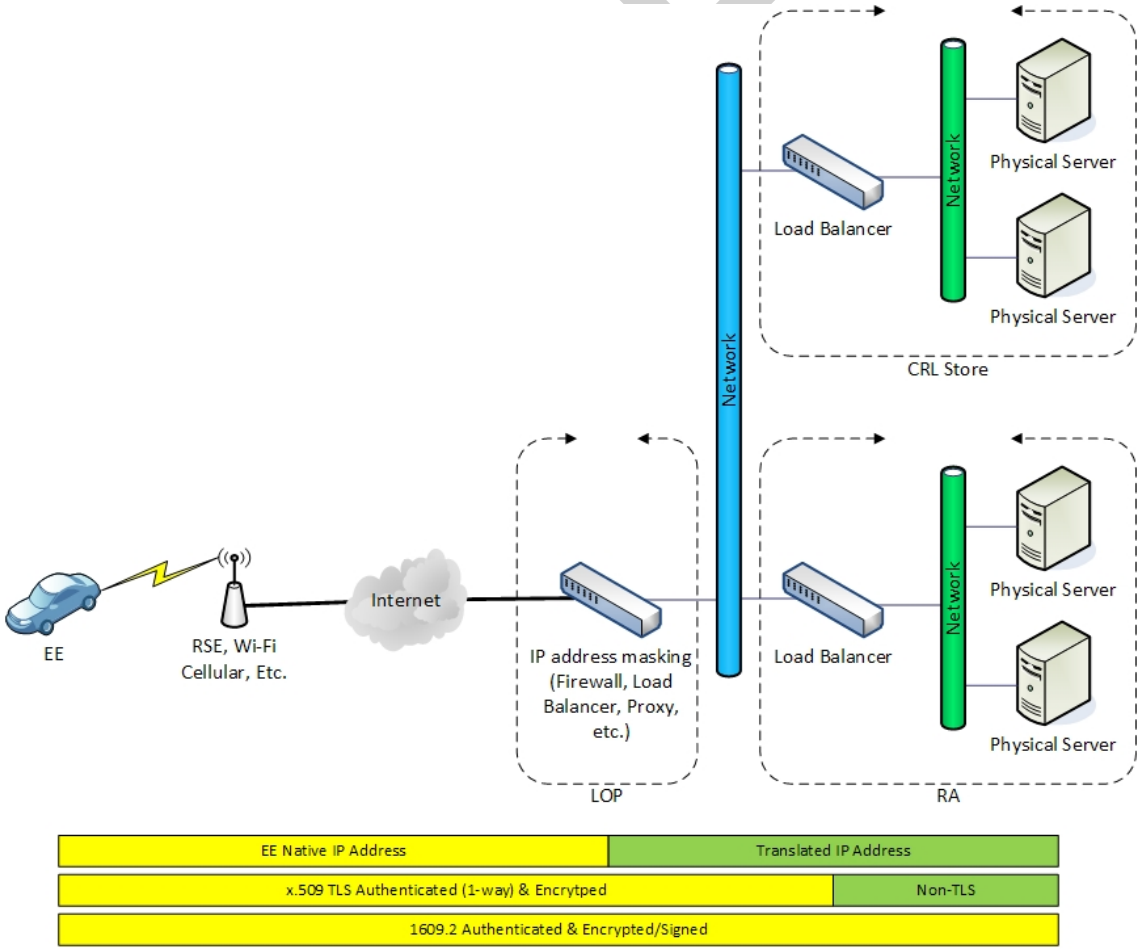
The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

2.2.3.3 Diagrams of Communications Methods

2.2.3.3.1 Overview of Methods

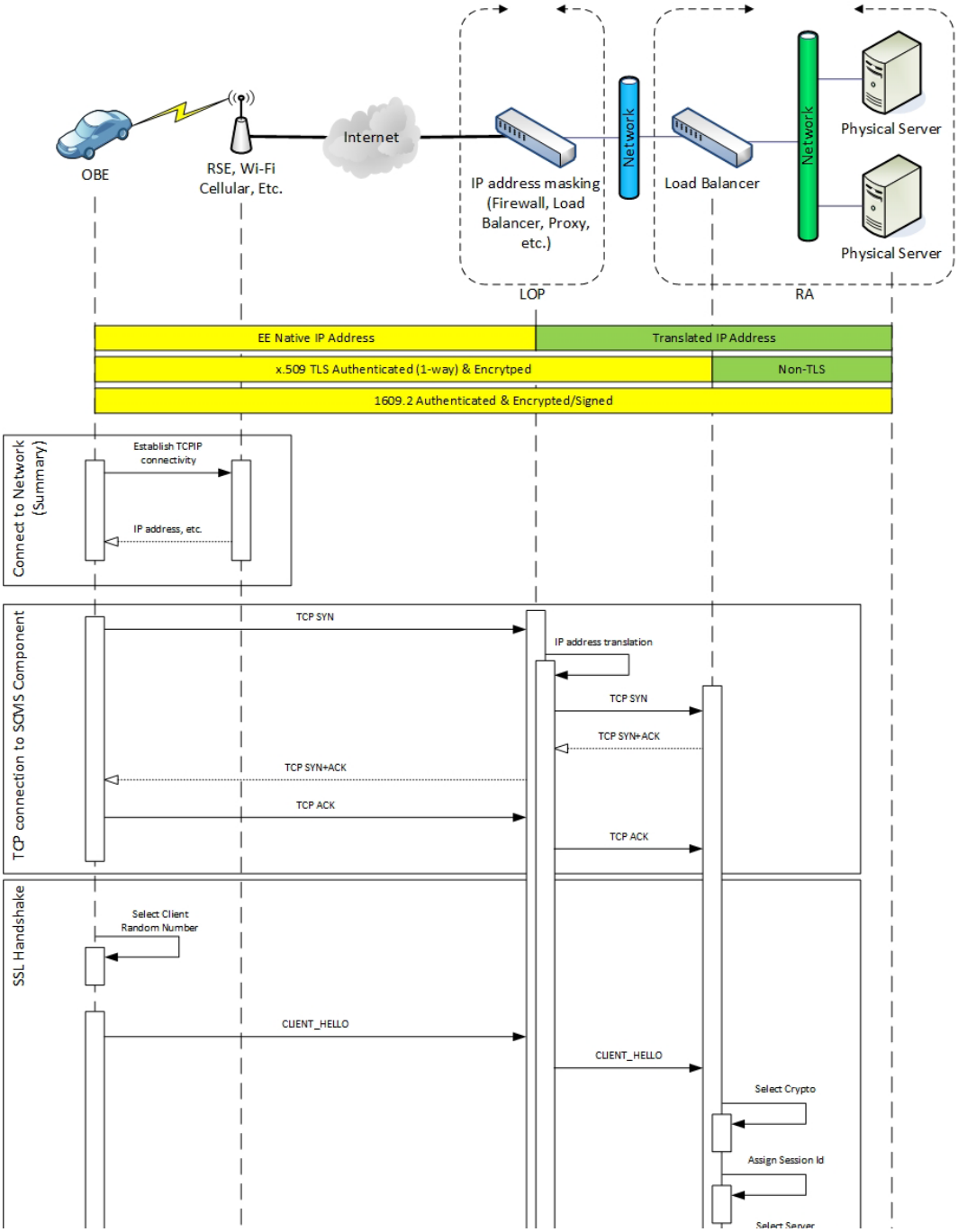


2.2.3.3.2 Overview of Multiple SCMS Components Served by Single LOP



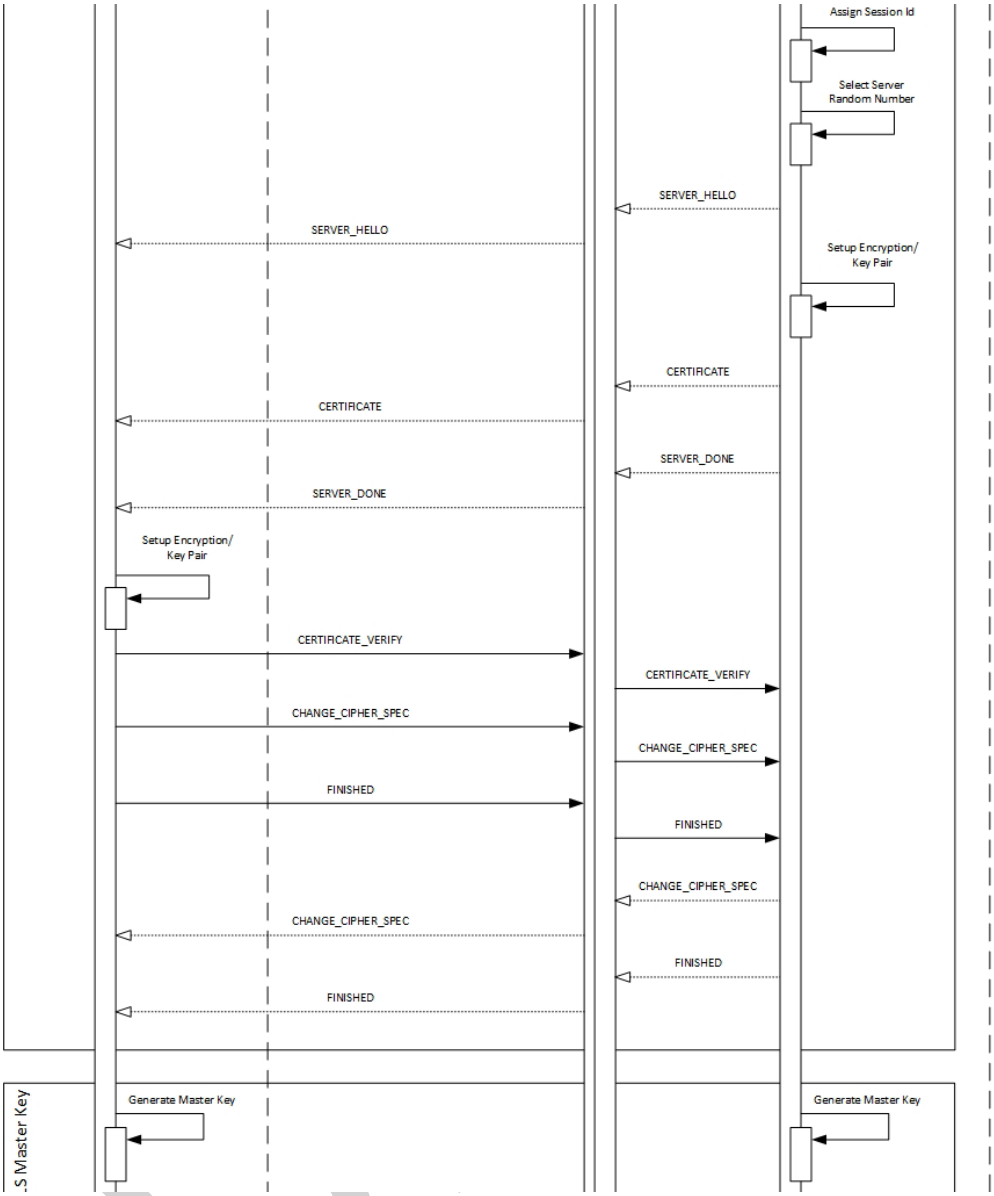
The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

2.2.3.3.3 Universal SCMS Handshake Processes



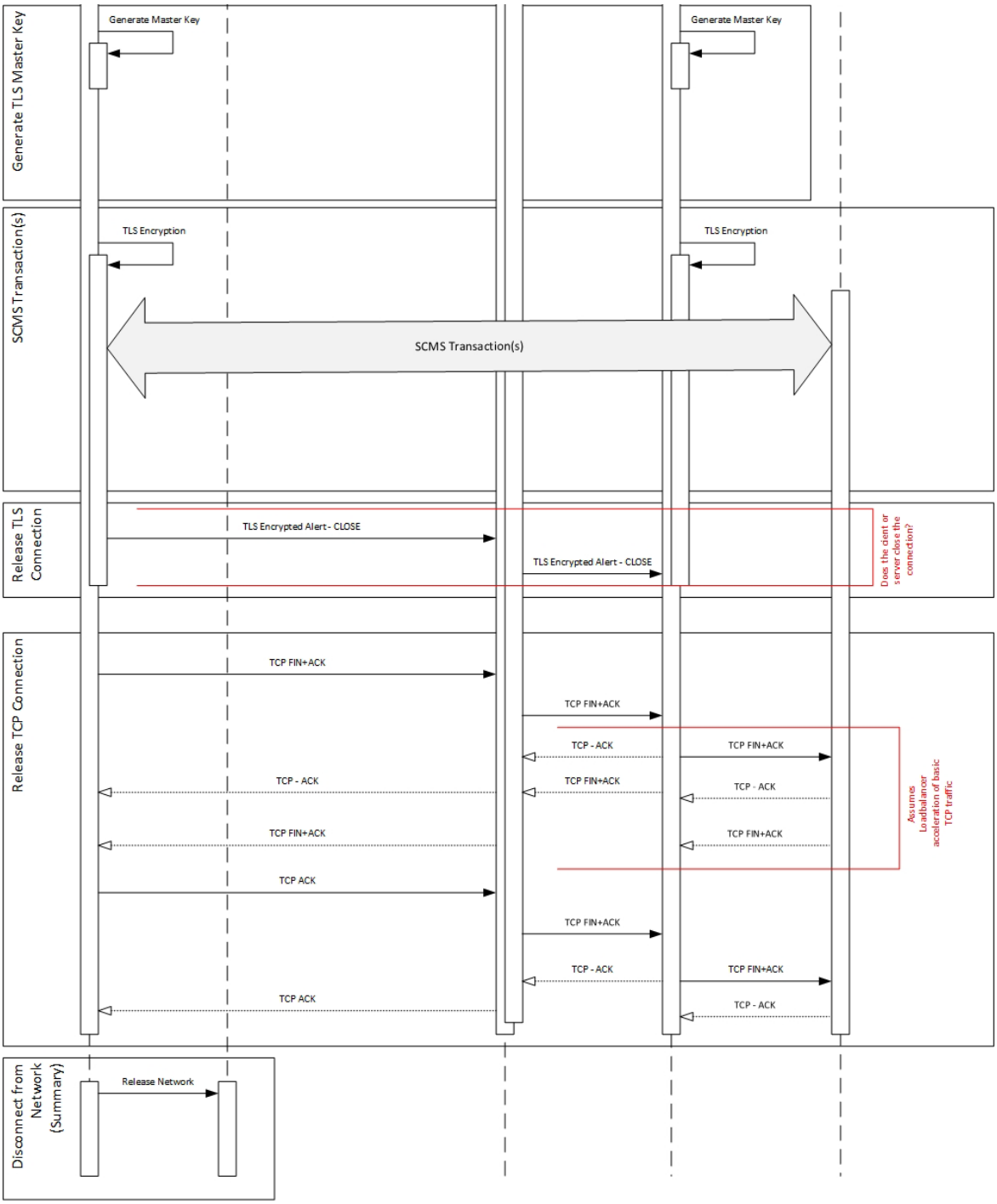
to be continued on next page

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary



to be continued on next page

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

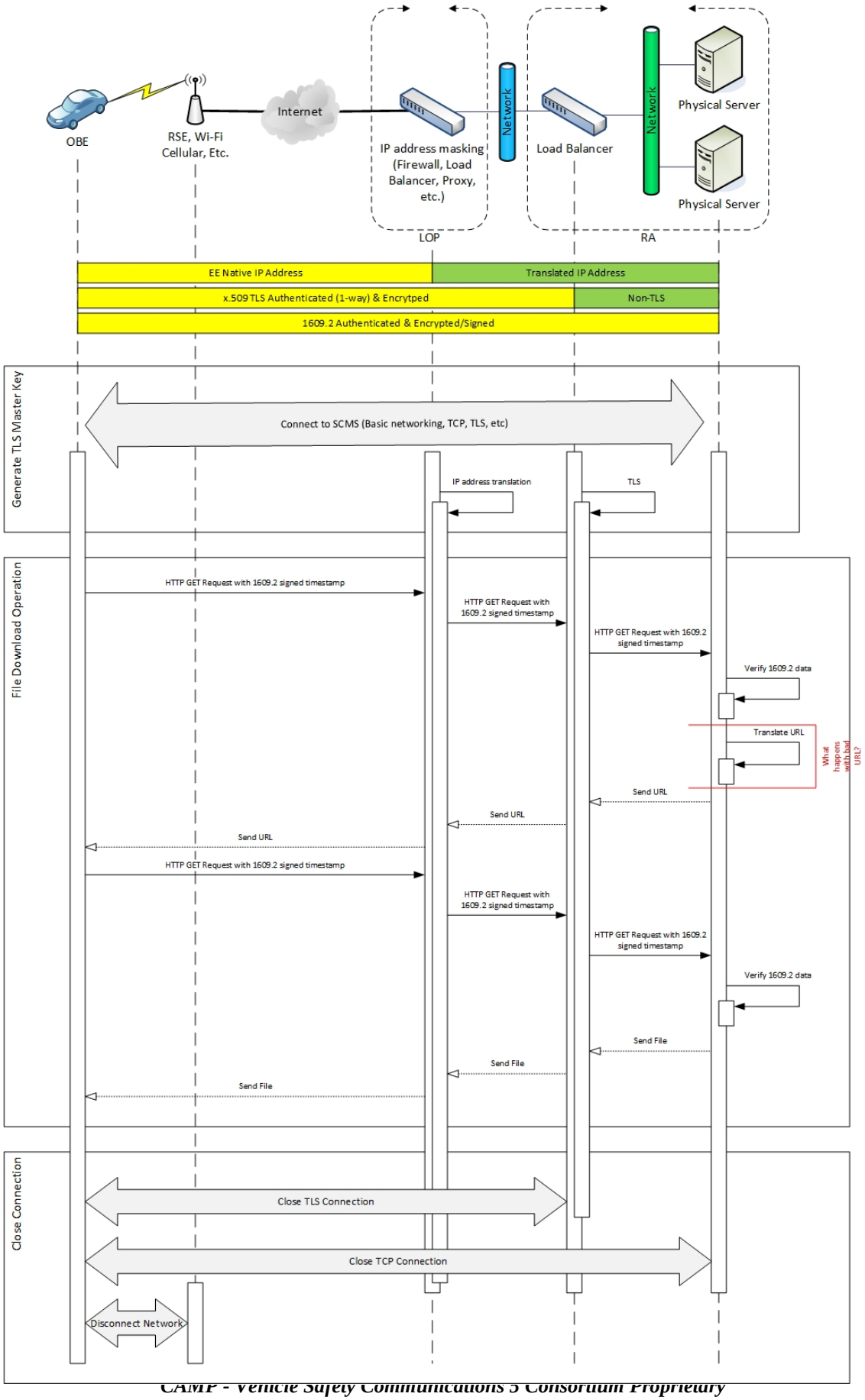


The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

2.2.3.3.4 Common Process for File Download Operations

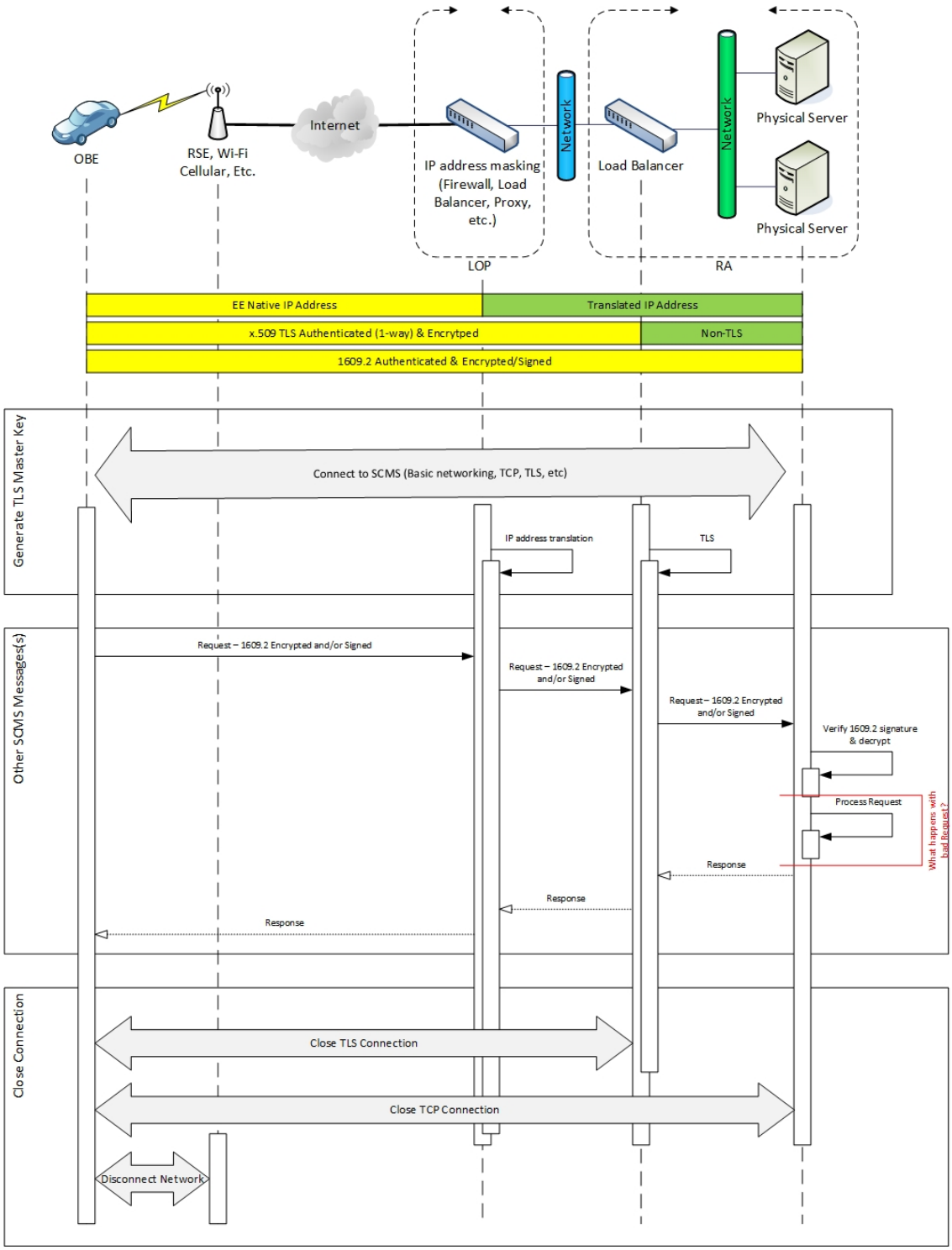
DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary



CAMP - Vehicle Safety Communications 3 Consortium Proprietary

2.2.3.3.5 Common Process for Sending SCMS Messages



2.2.3.4 Existing JIRA issues with "EE-Handshake" label

See Appendix A.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

2.2.3.5 Existing JIRA issues with OBE or RSE component

See Appendix B.

2.2.4 EE-RA Communications - General Guidance

2.2.4.1 Overview

The following is provided as general guidance for EE-RA messaging. For specific messaging refer to the RA Service Catalog provided in the RA Design Specification.

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

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.

In order to provide 1609.2 based authentication from EE-RA for Download requests an APDU named SignedAuthenticatedDownloadRequest is included in the request. The filename of the file the EE is attempting to download and the current time timestamp is included in the SignedAuthenticatedDownloadRequest. The EE uses its Enrollment Certificates signing key 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.

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

SCMS Protocol Messages

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

2.2.4.2 Requirements

- Download Requests include requests from EE to RA for the following files:
    - .info
    - Global Policy File (GPF)
    - Global Certificate Chain File (GCCF)/Local Certificate Chain File (LCCF)
    - OBE pseudonym certificate batch file
    - RSE application certificate files
    - OBE identification certificate files

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

- Download Requests shall be sent from EE to RA via HTTP GET.
- Download Request shall include a HTTP Header named 'Batch-Download-Req' with value equal to a ASN1 serialized Base64 encoded SignedAuthenticatedDownloadRequest request message.

- APDUs sent from EE to RA via HTTP POST shall include:
    - SecuredRACertRequest
    - SecuredPseudonymCertProvisioningRequest
    - SecuredIdCertProvisioningRequest

- APDUs other then 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.

2.3 RA - Services View

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

2.3.1 General Notes

1. 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.

1. For all the services, the HTTP Content-Type is set to application/octet-stream.
2. No information is returned in case of error, just an HTTP code of 500.

2.3.2 RA - Provision Pseudonym Certificate Batch

This service is used by the Device to request the initial batch of Pseudonym Certificates. After the initial batch is requested, subsequent batches are automatically provisioned.

PATH	**/provision-pseudonym-certificate-batch**

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

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

2.3.2.1 Preconditions

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

2.3.2.2 Postconditions

2.3.2.3 Quality of Service

Estimated values are per logical unit, meaning multiple individual nodes can contribute to achieve the desired level of service. A Batch of certificates is equal to 20 certificates which will be used in a week, so there will be be 52 batches per year. The number of batches that need to be generated in a year is a function of the number of years in service:

The first term of the formula captures the batches generated for vehicles added in previous years. The middle term represents the initial three years worth of certificates that are generated for new vehicles that are added on the current year, and the third term captures the ongoing top-up batch generation for new vehicles, which is needed in order to keep a backlog of three years of future batches from current date.

Quality Metric	1 Year	3 Years	5 Years	10 Years
Throughput	(52 batches/year x 3 years x 17,000,000 new vehicles + 433,500,000 top-up for new	(52 batches/year x 3 years x 17,000,000 new vehicles +433,500,000 top-up for new	(52 batches/year x 3 years x 17,000,000 new vehicles +433,500,000 top-up for new	(52 batches/year x 3 years x 17,000,000 new vehicles +433,500,000 top-up for new

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Quality Metric	1 Year	3 Years	5 Years	10 Years
	vehicles) / 31,557,600 seconds/year = **98** batch requests / second	vehicles + 52 batches x 34,000,000 existing vehicles) / 31,557,600 seconds/year = **153** batch requests / second	vehicles + 52 batches x 68,000,000 existing vehicles) / 31,557,600 seconds/year = **209** batch requests / second	vehicles + 52 batches x 153,000,000 existing vehicles) / 31,557,600 seconds/year = **350** batch requests / second
Maximum System Latency	**0.01** seconds/batch request	**0.007** seconds/batch request	**0.005** seconds/batch request	**0.003** seconds/batch request
Estimated Instance Latency	TBD	TBD	TBD	TBD
Estimated # of instances	TBD	TBD	TBD	TBD
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).

2.3.2.4 Quality of Protection

1. Incoming request and response messages are protected with TLS.
2. Incoming message is signed with the enrollment certificate of the sending device.

2.3.3 RA - Download .info file

This service is used by the device to determine the earliest date on which a new batch of pseudonym certificate will become available. There will be a .info file for each device containing this information.

PATH	/download-pseudonym-certificate-batch-info
HTTP Method	GET
HTTP Request Body	Empty
HTTP	HTTP Header 'Batch-Download-Req' containing a Base64 encoded ASN1

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

PATH	/download-pseudonym-certificate-batch-info
Request Headers	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.

2.3.3.1 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 servers time. (Controlled by the*ra.client-signature-ttl-sec* configuration setting.)

2.3.3.2 Postconditions

1. Returned file contains a single IEEE 1609 format Time32 time stamp that the device will use to schedule a subsequent "top-up" download.

2.3.3.3 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 weeks 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	**0.07** seconds / request	**0.01** seconds / request	**0.008** seconds / request	**0.004** seconds / request

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Quality Metric	Rationale	1 Year	3 Years	5 Years	10 Years
	certificate.				
Estimated Instance Latency		TBD	TBD	TBD	TBD
Estimated # of instances		TBD	TBD	TBD	TBD

2.3.3.4 Quality of Protection

1. Access is protected with HTTPS (TLS V1.2) via port 8892.
2. At a minimum support OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256
3. Access to this service is protected using certificate-based client authentication using the device enrollment certificate to establish the TLS session.

2.3.4 Download local policy file

This service is used by the device to download a local policy file.

PATH	/download-local-policy
HTTP Method	GET
HTTP Request Body	Empty
Parameters	HTTP Header 'Batch-Download-Req' containing a Base64 encoded ASN1 serialized *SecuredScmsPDU* containing an*EndEntityRaInterfacePDU*, containing an *AuthenticatedDownloadRequest* with a *filename* property of the form: lp_<X>_<Y>.<Z> Where: 1. X is the policy ID, up to 32 octets in hexadecimal (this could be a truncated SHA-256 hash of policy file content) 2. Y is the i-value in hexadecimal (when the policy becomes active, for easier roll-over from an old to a new policy) 3. Z is one of the permitted encoding formats a. oer b. xml

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

PATH	/download-local-policy
Response	File containing the local policy.

2.3.4.1 Preconditions

1. None

2.3.4.2 Postconditions

1. Returned file contains policy that the device will use.

2.3.4.3 Quality of Service

Estimated values are per logical unit, meaning multiple individual nodes can contribute to achieve the desired level of service. 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 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
Estimated Instance Latency		TBD	TBD	TBD	TBD
Estimated # of instances		TBD	TBD	TBD	TBD

2.3.4.4 Quality of Protection

- Access is protected with HTTPS (TLS V1.2) via port 8892.
- At a minimum support OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

- Access to this service is protected using certificate-based client authentication using the device enrollment certificate to establish the TLS session.

2.3.5 RA - Download global policy file

This service is used by the device to download a global policy file.

PATH	**/download-global-policy**
HTTP Method	GET
HTTP Request Body	Empty
HTTP Request Header	HTTP Header 'Batch-Download-Req' containing a Base64 encoded ASN1 serialized *SecuredScmsPDU* containing an*EndEntityRaInterfacePDU*, containing an *AuthenticatedDownloadRequest* with the *filename* property set to 'gp_latest.oer'
HTTP Response Body	File containing the global policy.

2.3.5.1 Preconditions

1. Time stamp in the request *AuthenticatedDownloadRequest* is not more than 5 seconds apart from the servers time. (Controlled by the*ra.client-signature-ttl-sec* configuration setting.)

2.3.5.2 Postconditions

1. Returned file contains global policy that the device will use.

2.3.5.3 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:

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	8,500,000 new vehicles / 604,800 seconds/week = **14** requests / second	(8,500,000 new vehicles + 34,000,000 existing vehicles) / 604,800 seconds/week = **70** requests /	(8,500,000 new vehicles + 68,000,000 existing vehicles) / 604,800 seconds/week = **126** requests	(8,500,000 new vehicles + 153,000,000 existing vehicles) / 604,800 seconds/week = **267** requests

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Quality Metric	Rationale	1 Year	3 Years	5 Years	10 Years
	global policy in the same week.		second	/ second	/ second
Maximum System Latency		**0.07** seconds / request	**0.014** seconds / request	**0.008** seconds / request	**0.004** seconds / request
Estimated Instance Latency		TBD	TBD	TBD	TBD
Estimated # of Instances		TBD	TBD	TBD	TBD

2.3.5.4 Quality of Protection

1. Access is protected with HTTPS (TLS V1.2) via port 8892.
2. At a minimum support OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256
3. Access to this service is protected using certificate-based client authentication using the device enrollment certificate to establish the TLS session.

2.3.6 RA - Download Pseudonym Certificate Batch

This service is used by the device to download a batch of Pseudonym Certificates for a specific time period.

PATH	/download-pseudonym-certificate-batch
HTTP Method	GET
HTTP Request Body	Empty
HTTP Request Headers	HTTP Header 'Batch-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}.tar 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.tar corresponds to i value 15, for device with

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

PATH	/download-pseudonym-certificate-batch
	request hash AB09281C9867DE53. **Range (optional) as defined in RFC 2616:** To support partial downloads for resuming interrupted transfers. Examples: 1. From byte offset 500 to 700: Range : bytes=500-700 2. Starting from byte offset 1000 to the end: Range : bytes=1000-
HTTP Response Body	If no Range header is present, the entire tar file corresponding to the requested batch. If a Range header is present, the specified bytes of the referenced file.

2.3.6.1 Preconditions

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

2.3.6.2 Postconditions

1. The tar file corresponding to the batch specification in the request URL is returned.
2. The content of the tar file is organized as a flat directory containing *n* files (where 0 <= *n* <= *j_max* - 1) named as in:
    a. 0.crt
    b. 1.crt
    c. ...
    d. *<n-1>*.crt

2.3.6.3 Quality of Service

Estimated values are per logical unit, meaning multiple individual nodes can contribute to achieve the desired level of service. The the number of files downloaded in a year is a function of the number of years in service:

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	With no previous year vehicles: 17m x 52 weeks * 3 years	With and two years worth of old vehicles (34 million): 17m (new) +	With four years worth of old vehicles (68 million): 17m (new) +	At the end of the first 10 years, there will be a total of 170 million cars in the

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Quality Metric	Rationale	1 Year	3 Years	5 Years	10 Years
	initial 3 year's worth of certificates (156 files) plus old cars downloading one year's worth of certificates (52 files).	= 2,652 million files Divided by the number of seconds in a year: 2,652 million files / 31,557,600seconds = **85 files per second**	34m (old) 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**	68m (old) 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**

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Quality Metric	Rationale	1 Year	3 Years	5 Years	10 Years
Maximum System Latency	A database look up and a database insert.	**0.0118**seconds / download	**0.00709** seconds / download	**0.00508** seconds / download	**0.00297** seconds / download
Estimated Instance Latency		TBD	TBD	TBD	TBD
Estimated # of instances		TBD	TBD	TBD	TBD

2.3.6.4 Quality of Protection

1. Access is protected with HTTPS (TLS V1.2) via port 8892.
2. At a minimum support OpenSSL cipher suite ECDHE-ECDSA-AES128-SHA256
3. Access to this service is protected using certificate-based client authentication using the device enrollment certificate to establish the TLS session.

2.3.7 RA - Retrieve Registration Authority Certificate

This service allows the Device to refresh its locally cached RA certificate.

PATH	/retrieve-ra-certificate
HTTP Method	POST
HTTP Request Body	ASN1 serialized *EndEntityRaInterfacePDU* containing a *EeRaCertRequestMsg*.
HTTP Response Body	Serialized IEEE X1609.2 certificate

2.3.7.1 Preconditions

None

2.3.7.2 Postconditions

- The 1609 certificate is returned to the device.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

2.3.7.3 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 vehicles likely to download the RA certificate 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 refresh their copy of the RA certificate in one 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
Estimated Instance Latency		TBD	TBD	TBD	TBD
Estimated # of instances		TBD	TBD	TBD	TBD

2.3.7.4 Quality of Protection

- Access is protected with HTTPS (TLS V1.2) via port 8892.

2.3.8 RA - Provision Identity Certificate

This service is used by the RSE to request the new identity certificates. After the initial batch is requested, subsequent batches are automatically provisioned.

PATH	/provision-identity-certificate
HTTP Method	POST
HTTP Request	ASN1 serialized SecuredIdCertProvisioningRequest

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

PATH	/provision-identity-certificate
Body	
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 IdCertProvisioningRequestAck 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 from.

2.3.8.1 Preconditions

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

2.3.8.2 Postconditions

2.3.8.3 Quality of Protection

- Incoming request and response messages are protected with TLS.
- Incoming message is signed with the enrollment certificate of the sending device.

2.4 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 be comprehend multiple steps from a system's architecture perspective that can be run without interference with each other to return a partially result of the overall use case. Normally steps need to be run in the order given to fulfill the use case. For example "Use Case 2: Bootstrapping" is a use case that includes everything to prepare an end entity to be part of the overall trust system. It comprehends two distinguished steps: Step 2.1: Initialization (Bootstrapping) and Step 2.2: Enrollment (Bootstrapping). This format was chosen to better support end to end implementation as well as testing. It also supports an easier prioritization of requirements to define an order of implementation.

2.4.1 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 EE needs to do if a Root CA is revoked or a new Root CA is introduced to the system.

- Use Case 2: Bootstrapping
- Use Case 3: Initial Provisioning of Pseudonym Certificates
- Use Case 5: Misbehavior Reporting
- Use Case 6: CRL Download

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

- Use Case 8: OBE Revocation
- Use Case 9: Refresh Pseudonym Certificates
- Use Case 10: Update Pseudonym Certificate Request Parameters

2.4.2 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 EE 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 14: RSE Misbehavior Reporting
- Use Case 15: RSE CRL Check
- Use Case 16: RSE Application and OBE Identification Certificate Revocation
- Use Case 17: Refresh RSE Application Certificates

2.4.3 Requirements to be updated / added with the next revision

- Component compromise recover strategy
- Use Case 5: Misbehavior Reporting
- CRL Generator / CRL format (within MA integration and Collaborative Distribution sub projects)

2.4.4 Use Case 2: Bootstrapping

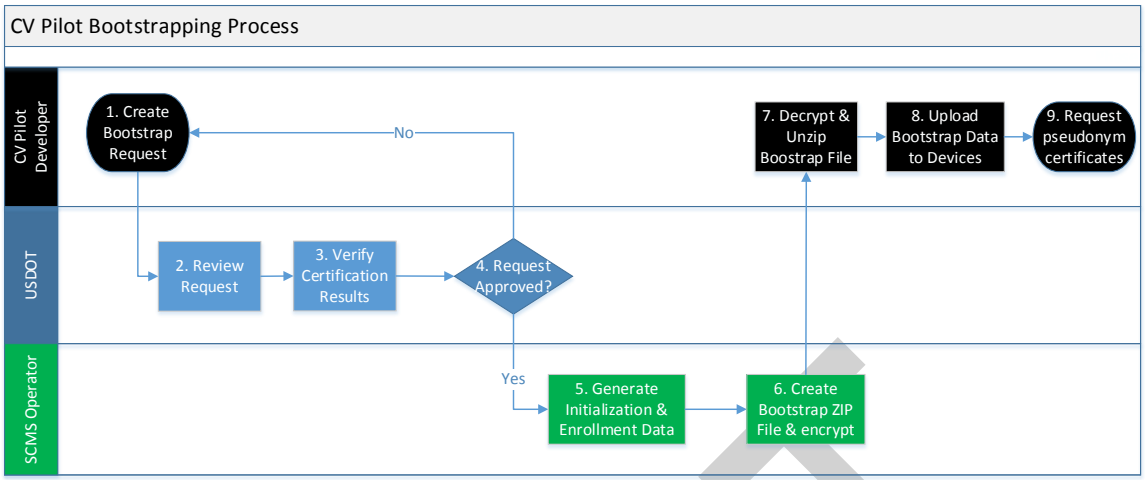
Initially a device has no certificates and no knowledge of how to contact SCMS. Bootstrapping is the process called to initialize the device in order to be ready for communication with the SCMS. Bootstrapping encompasses two distinct activities: initialization and enrollment. Initialization is the process by which a device receives keys that allow it to trust other SCMS components and credentials to connect to them. Enrollment is the process by which a device receives a long-term certificate which it can use in interactions with the SCMS to allow other devices to trust it. The overall security requirements for this process are:

- Process must protect device from receiving incorrect information
- Process must prevent SCMS from issuing certificates to unauthorized devices

Therefore it was decided that the initial version SCMS POC will only support a manual bootstrapping process; however, later versions of the system will support automatic bootstrapping. The following process flow provides an overview of the manual bootstrapping process:

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT



2.4.5 Use Case 3: Initial Provisioning of Pseudonym Certificates

Target release	Core
JIRA Task	SCMS-68-Finish document "Initial Provisioning of Pseudonym Certificates"Closed
Document owner	Virendra Kumar
Reviewer	Jeff Hahn
QA	Unknown User (administrator)

2.4.5.1 Goals

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

2.4.5.2 Background and strategic fit

The Initial Provisioning of Pseudonym Certificates is the process by which a device 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 device doesn't 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)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

- Registration Authority (RA)

At the start of this use case, the device has no pseudonym certificates. At the end of this use case, the device has 3 years worth of pseudonym certificates, and the RA has everything it needs from the device for generating and providing subsequent pseudonym certificate batches for the device.

For an explanation of time periods i and j, please refer to Time Periods.

2.4.5.3 Assumptions

- Device is assumed to have a valid enrollment certificate.
- Device is assumed to have Root CA, RA and PCA certificates.
- Device is assumed to have relevant address(s) to communicate with the RA.

2.4.5.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-505	Closed	Initial request triggers subsequent provisioning of pseudonym certificates	RA shall use the initial request by a device as a trigger for subsequent provisioning of pseudonym certificates, i.e. from this point onwards unless there is a policy change, RA shall automatically generate the desired number of pseudonym certificates and make them available for download by the device.	so that the device doesn't need to make a request every time it needs certificates		RA
SCMS-506	In Implementation	Determine right amount of	RA shall be able to determine the	so that the device's privacy is		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
		shuffling based on SCMS Manager policy	right amount of shuffling for pseudonym certificate requests based on the policy set by the SCMS Manager	maintained		
SCMS-507	Closed	Maintain an Internal Blacklist	RA shall maintain an Internal Blacklist and keep it updated based on the communications with the MA	so that revoked devices are not issued any more certificates	Every logical RA has its own internal blacklist that is not shared with anyone else.	RA
SCMS-508	SCMS PoC out of Scope	Stop pre-generating certificates for inactive device	RA shall stop pre-generating pseudonym/OBE identification certificates for a device that has not connected to RA for a given amount of time as specified by the SCMS Manager	So that computing resources are not wasted for inactive devices. If device has not connected for a certain period of time, the assumption is the device is no longer available or in service.	Stop/resume pre-generation is out of scope for PoC. Time is currently set to be 3 years. Based on the implementation, the LA may also stop pre-generating pre-linkage values.	RA
SCMS-509	Closed	Stop pre-generating pseudonym	RA shall stop pre-generating pseudonym and OBE	so that computing resources are not		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
		certificates for revoked device	identification certificates for a device that has been revoked by the MA, i.e., for a device that appears on RA's internal blacklist.	wasted for revoked devices		
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-768	In Implementation	RA - Global Certificate Chain File	RA shall provide a Global Certificate Chain File and a Local Certificate Chain File for download by EEs.	to enable EEs to verify certificates without further CA certificate downloads. If the Global Policy File indicates a new version of the Global Certificate Chain File than that existing on the EE, the EE will need to download it	For more information: Global Certificate Chain File	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				and apply it.		
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)

8 issues

2.4.5.5 Design

At a high level, this use case can be divided into 5 steps as follows.

1. Check for policy updates
2. Request for Pseudonym Certificates
3. Pseudonym Certificate Generation
4. Download of Pseudonym Certificates
5. Generate subsequent batch of Pseudonym Certificates

Having determined which RA to submit the request to, the device creates a request, signs it with the enrollment certificate, encrypts the signed request for the RA and sends it to the LOP. The LOP strips any information that could be used to determine the device's location and sends it to the RA. The RA checks to make sure that the certificate batch request is correct and authorized. 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 batch request information with linkage information from the LAs to create a series of individual certificate requests and sends those requests to the PCA, mixing the individual certificate requests with individual certificate requests generated from certificate batch requests from other devices to provide privacy against insiders at the PCA. The PCA signs the pseudonym certificates, encrypts them for the device, 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 and returns the pseudonym certificates to the device.

2.4.5.6 Step 3.1: Check for policy updates

Target release	Core
JIRA Task	SCMS-102-Finish document "Check for policy updates"Closed
Document owner	Andre Weimerskirch
Reviewer	Jeff Hahn

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

QA	Erik Schetina

2.4.5.6.1

2.4.5.6.2 Goals

- The policy download mechanism is required to ensure that the OBE is always using the latest policy for new downloaded certificates batches. Policy definition details are available at Use Case 18: Create / provide global, local and SCMS Manager policies.

2.4.5.6.3 Background and strategic fit

Whenever the SCMS manager decides to change policies for the SCMS all participating devices need to get updated. There is a Global Policy File that is signed by the Policy Generator. The OBE will request a policy download before any certificate download to ensure that the certificate batches generated by the SCMS are interpreted by the OBE correctly.

2.4.5.6.3.1 Policy Repository

The policy repository location should be the same as the RA certificate batch repository location. For example:

- https://download.ra.provider.com

Once the EE has been authenticated with the RA certificate batch repository, the RA will redirect the connection from the common URL to a location where the global policy file and certificate batches may be downloaded.

All other requirements for the policy download are the same as for the certificate batches download, specifically

- Transfer protocol method and its parameters
- Encryption scheme and its parameters
- Authentication scheme and its parameters

2.4.5.6.4 Assumptions

- Global policy identifier and current policy shall be provisioned during OBE bootstrapping process (so that RA can compare and accept/reject certificate requests).

2.4.5.6.5 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 certificat	Messages from EEs to an RA must be secure against replay attacks.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			e. These messages shall include a timestamp (which the EE will obtain from its GPS reference) to avoid replay attacks on the RA.	The signed time stamp from the EE enables the RA to validate the freshness of EE requests.		(RSE)
SCMS-512	Closed	Global Policy file	RA shall always provide a global policy file available for download by EE	There is always a global configuration available, and that configuration shall be current		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-	Closed	RA download via HTTPS	RA shall provide downloa	to utilize standard internet	Downloads could be e.g. policy file, Global Certificate Chain File,	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
514			ds over HTTPS (TLS).	protocols for the download process.	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 certs currently. Instead the OBE will use TLS to authenticate the other endpoint (as a server) and will use its SCMS cert to identify itself. EE authenticates via its IEEE 1609.2 enrollment certificate. The details of the authentication process are defined Step 3.4: Download of Pseudonym Certificates	RA
SCMS-517	In Implementation	Tunneling through LOP	RA shall provide downloads only via a LOP hardware interface,	to anonymize the location of EEs.		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			which removes all location information from the incoming request.			
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	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				defined in Step 3.4: Download of Pseudonym Certificates.		
SCMS-544	Closed	Download resume	RA shall support byte-wise resume of certificate batch, certificate file, or policy file, downloads, even if EE switches the IP address.	to improve reliability of the download protocol.		RA
SCMS-709	SCMS PoC out of Scope	Check for 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	• 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)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				definition details are available at Use Case 18: Create / provide global and local policies.		
SCMS-767	SCMS PoC out of Scope	Check for Certificate Chain Updates	EE shall check for version changes in 'certChainFileId' field of the Global Policy file. If the version is different than that of its existing file, it will take action to update it.	As CAs are added, removed, revoked, or rolled-over, new certificate chains will have to propagated to EEs and other SCMS components. For more information: Global Certificate Chain File	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-	SCMS PoC out	Error code: eeGlobalPolicyFileD	EE shall implement OEM	As the global policy	This is out of scope since it defines EE's	On-board Equipm

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
952	of Scope	ownloadFailed	defined error handling and store the error code in EE's error log file, if EE is not able to download the global policy file (e.g. because there is none or it's corrupted).	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.	behavior.	ent (OBE), Road-side Equipment (RSE)
SCMS-953	SCMS PoC out of Scope	Misbehavior reporting: eeGlobalPolicyFileDownloadFailed	If EE is not able to download the global policy file (e.g. because there is none or it's corrupted), EE shall initiate a misbehav	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)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			ior report to MA with the observed error.			
SCMS-954	SCMS PoC out of Scope	Error code: eeGlobalPolicyVerificationFailed	EE shall implement OEM defined error handling and store this error code in EE's error log file, if EE is not able to verify the digital signature of the global 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 reporting: eeGlobalPolicyVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify the digital signature of the global 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)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			file.			
SCMS-956	SCMS PoC out of Scope	Error code: eeGlobalPolicyFileParsingFailed	EE shall implement OEM defined error handling and store this error code in EE's error log file, if EE is not able to parse the successfully downloaded global policy file (e.g. because it's corrupted).	As the global 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 reporting: eeGlobalPolicyFileParsingFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to parse the successfully	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)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			downloaded global policy file (e.g. because it's corrupted).			
SCMS-958	SCMS PoC out of Scope	Error code: eeConnectionFailed	EE shall log this error in its log file, 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 this error code, 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	Error code: raNoTLS	RA shall return standard TLS error codes if TLS	in order to enable client side error handling		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			errors occur.	.		
SCMS-978	In Implementation	Error code: raAuthenticationFailed	RA shall log this error, 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 store this error code in EE's error log file, 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 reporting: 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)
SC	Impleme	Check time stamp	RA shall	If the		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
MS-1203	nted		check the signed (by EE) time-stamp and allow a tolerance of 5 seconds.	difference between the signed time-stamp and the current time is 5 seconds or less, RA will proceed with the authentication process. Otherwise RA will reject the connection.		
SCMS-1204	Implemented	Check blacklist	RA shall reject EE request, if EE is listed on its blacklist.	If EE is listed, RA will reject the connection. Otherwise RA will proceed with the authentication process. The Internal		RA

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				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 correspo		

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				nding 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 gets LCCF from RA	EE shall check for and download policy an updated	to be able to verify SCMS certificates based on their	All the certificate chains will contain certificates up to the Root CA including elector endorsement for the Root CA cert. This is out of scope	On-board Equipment (OBE), RA, Road-

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			Local Certificate Chain File (LCCF) or Global Certificate Chain File (GCCF) upon establishing communications with the RA	certificate chain.	since it defines EE's behavior	side Equipment (RSE)
SCMS-1356	SCMS PoC out of Scope	LCCF validation in EE	EE shall use the Local or Global Certificate Chain File (LCCF/GCCF) 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	EE doesn't 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 since it defines EE's behavior	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				validate the certificate chain.		

27 issues

2.4.5.6.6 ASN.1 Specification

- **scms-policy.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/scms-policy.asn?at=refs/heads/master
- **scms-base-types.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/scms-base-types.asn?at=refs/heads/master
- 1609dot2-schema.asn
- 1609dot2-base-types.asn

2.4.5.7 Step 3.2: Request for Pseudonym Certificates

Target release	Core
JIRA Task	SCMS-75-Finish document "Request for Pseudonym Certificates"Closed
Document owner	Biswajit Panja
Reviewer	Jeff Hahn
QA	Erik Schetina

2.4.5.7.1 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. A standard request is for 3,000 (3,120 to be exact) certificates and is assumed to be the default for a batch request. (20 certificates per week x 52 weeks per year x 3 years). Note: The number of requested certificates per week does change the request size since the RA sends them one-by-one to the PCA.

2.4.5.7.2 Background and strategic fit

The end-entity device decides to request pseudonym certificates from an RA, based on policy set by the DCM within the overall policy set by the SCMS Manager. The end-entity device may optionally contact the DCM through LOP to determine which RA to submit the certificate batch request to, or this information may be pre-configured.

Having determined which RA to submit the certificate batch request to, the end-entity device creates a request, signs it with the enrollment certificate, encrypts the signed request for the RA and sends it to the LOP. The LOP strips any information that could be used to determine the

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

device's location and sends it to the RA. The RA checks to make sure that the certificate batch request is correct and authorized.

Two types of requests occur in the certificate provisioning process:

1. Certificate batch request (sent from the device to the RA) requesting a batch of pseudonym certificates.
2. Individual certificate requests (sent from the RA to the PCA) which request one pseudonym certificate each.

To distinguish between these two types, the terms 'certificate batch request' and 'individual certificate request' will be used.

2.4.5.7.3 Prerequisites and Assumptions

In order to facilitate the certificate request process, the following prerequisites should be met:

- The device shall have successfully completed the bootstrap process (2. Bootstrapping)
- The device shall know the current network address of the RA (VK: provide a link when available)
- The device shall have obtained the latest device specific configurations from the DCM (VK: provide a link when available)

2.4.5.7.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-507	Implemented	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 issued any more certificates	Every logical RA has its own internal blacklist that is not shared with anyone else.	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 since it defines EE's behavior.	On-board Equipment (OBE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
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 their request was received by the RA.		RA
SCMS-522	SCMS PoC out of Scope	Retry request	If the EE doesn't receive acknowledgement (TCP ACK) within a specified amount of time, currently set to be 2 sec from the time of request, it shall retry.	to ensure that the request is received by the RA.	This is out of scope since it defines EE's 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	Certificate Provisioning Request with the RA for a minimum of 60 minute after 10 consecutive failed communication attempts resulting in no acknowledgement (TCP ACK) or no Certificate Provisionin	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				g Response		
SCMS-524	SCMS PoC out of Scope	RA certificate	EE shall dynamically acquire RA's SCMS certificate in case it has changed, see EE →RA _ RA Certificate Request, EE →RA _ RA Certificate Response	so that EE can encrypt the request to the right RA	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-529	Closed	Store enrollment certificate and butterfly parameters	RA shall store enrollment certificate and butterfly parameters for each OBE for its lifetime, that is currently assumed to be 40 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-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	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				and to verify that the certificate request is originating from a valid EE		(RSE)
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's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-986	Review	Error code: raNoInitialRequest	RA shall log "Error code: raNoInitialRequest", if this is not the OBE's initial request for pseudonym certificates and it is not a request with changed parameters.	Proper parameters are required to start the certificate provisioning process, otherwise there is already an existing request and pseudonym certificates get pre-generated.	If this is the first request by the OBE then RA shall start certificate provisioning. RA shall follow initial provisioning If a device makes a request with	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
					different parameters then RA shall begin preparing the processing of certificate. RA shall follow update pseudonym certificate provisioning	
SCMS-987	In Implementation	Error code: eeWrongParameters	RA shall log "Error code: eeWrongParameters", 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: eeRetries	RA shall log "Error code: eeRetries", if the EE retries within the time specified in SCMS-522.	to enable server side diagnostics and to avoid giving potential attackers relevant		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				information. Retry not allowed within 2 seconds		
SCMS-990	In Implementation	Error code: moreThanAllowedTries	RA shall return status code HTTP 500, if the EE makes more than n retries within the time specified in SCMS-523, and log "Error code: moreThanAllowedTries".	More than n tries not allowed		RA
SCMS-1012	In Implementation	Error code: eeWrongGlobalPolicyParameter	RA shall log "Error code: eeWrongGlobalPolicyParameter", 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 for misbehavior.	RA

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1082	In Implementation	Error code: eeInvalidSignature	RA shall log "Error code: eeInvalidSignature", if the EE doesn't 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: eeRequestNotEncrypted	RA shall log "Error code: eeRequestNotEncrypted", if the EE doesn't encrypt the certificate request using the RA's 1609 certificate.	to enable server side diagnostics and to avoid giving potential attackers relevant information	A unencrypted certificate request might be an indication for misbehavior.	RA
SCMS-1084	In Implementation	Error code: eeInvalidCredentials	RA shall log "Error code: eeInvalidCredentials", 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: eeUnauthorizedRequest	RA shall log "Error code: eeUnauthorizedRequest", if an EE makes an unauthorized request (invalid	to enable server side diagnostics and to avoid giving	An unauthorized request might be an	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			permissions)	potential attackers relevant information	indication for misbehavior.	
SCMS-1086	In Implementation	Error code: eeMalformedRequest	RA shall log "Error code: eeMalformedRequest", 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: eeRaMismatch	RA shall log "Error code: eeRaMismatch", 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: eeInvalidTime	RA shall return status code HTTP 500, if the EE has an invalid system time, and log "Error code: eeInvalidTime".	to avoid EEs using the invalid certificates		RA
SCMS-120	Implemented	Check blacklist	RA shall reject EE request, if EE is listed on its blacklist.	If EE is listed, RA will reject		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
4				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		

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				certificate of the corresponding device and put it on the internal blacklist. The RA does not send out enrollment certificates to the IBLM.		
SCMS-1397	Review	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 and not provide useful information to malicious actors.	• Standard TCP (SCMS-1090) and TLS (SCMS-977) errors shall be reported to EEs • All errors at the HTTP and	ECA, RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
					higher levels shall 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	Review	RA accept HTTP post over TCP/IP	RA shall accept HTTP post requests from authenticated EEs.	to allow the SCMS endpoint to serve everything based on HTTP protocol	RA - Services View will document the actual HTTP	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

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

25 issues

2.4.5.7.5 Design

OBE	RA
1. OBE → RA	
1.1 Generate ECC butterfly seed pair a, A= aG, and h, H=hG. Randomly select values s and e (each 16 bytes). Collect current time t, as well as start_time and end_time of requested pseudonym certificates. Sign [A, H, s, e, t, start_time, end_time, < EC >$_{ECA}$] with EC and encrypt the signed message with RA.	1.2 Decrypt all values and verify the signature with < EC >$_{ECA}$. Check freshness and validate < EC >$_{ECA}$ against internal blacklist.
	1.3 RA stores request as tuple [<EC>, start_time, end_time, flag=requested]. RA validates that OBE did not previously apply for certificates covering this time period. RA updates the time period OBE applied for.
2. RA → OBE	
	2.1 Acknowledge submission

See also Appendix D - Security Protocol Details, D.4

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

The Certificate Provisioning Request message is initiated by the EE in order to provide the RA with critical information (key parameters, security policy identifier, etc.) necessary for certificate batch generation. For new devices with no prior history of certificate requests, the RA will use the information contained within the Certificate Provisioning Request to start the certificate pre-generation process. 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

No subsequent Certificate Provisioning Request is necessary to acquire new certificate batches unless the device is instructed to change one or more critical certificate generation parameters.

2.4.5.7.6 Transmission Behavior

Assuming that the EE receives a positive acknowledgement from the RA in response to the request, the Certificate Provisioning Request message shall be sent once for each unique request. However, there are several conditions that 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 DCM /DNS for latest RA network information)
- EE possesses an invalid RA certificate and cannot establish secure communications
- RA Acknowledge message contains an error

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

For each request, the EE shall compute a hash of message for tracking/verifying responses from the RA. This hash should be maintained until the certificated request is no longer considered valid (e.g., EE submits new request due to a change in policy). The hash shall be the low order 8-bytes of the SHA-256 hash of the encoded "ToBeSigned" Certificate Provisioning Request message.

2.4.5.7.7 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.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

2.4.5.7.8 Message Contents

The EE shall use a standard format for creating the Request Certificate message. 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
- Caterpillar keys / expansion function parameters
    - One pair for signing
    - One pair for encryption
- Current device time: 32-bit denoting number of seconds since the Epoch
- Signed policy identifier that indicates the device capabilities

2.4.5.7.9 RA Response

The RA response to the Certificate Provisioning Request message may be *accept* or *reject*. The RA may *accept* a request, but choose to provide a "soft" error under certain conditions. If the RA *rejects* a request, a specific "hard" error will be provided in the Request Acknowledge. Explicit EE behaviors as a result of these errors will be described in a separate EE design specification.

Hard Errors

- certificate_revoked
- certificate_unknown
- access_denied

Soft Errors (May lead to hard error)

- Device policy identifier out-of-date

EE →RA _ Certificate Provisioning Request

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 a "hard" 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 repository URL and the time at which the first certificates batches will be available for download.

2.4.5.7.10 Transmission Behavior

Assuming that the RA receives acknowledgement that the device received the message through the transport protocol (TCP ack), the Request Acknowledge message shall be sent once in response to a Certificate Provisioning Request message. If the device is unreachable, the RA will utilize transport and application layer retransmissions for a period of time before eventually reaching a timeout limit.
Should a communication timeout occur, it is likely that the device has gone offline or has changed IP addresses. In such case, the EE will need to resend the Certificate Provisioning Request message to the RA to ensure the request has been processed. This request may contain the same parameters as the previous request.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

2.4.5.7.11 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.

2.4.5.7.12 Message Contents

The RA shall use a standard format for creating the Request Acknowledge message 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
    - Time at which the first certificate batches will be available for download (represented by Time32)
    - URL of the certificate repository (common for all devices serviced by an specific RA)
    - Soft error code (if any)
- Case: Certificate Provisioning Request *Reject*
    - Version
    - Low order 8-bytes of the SHA-256 hash of the encoded "ToBeSigned" certificate request from the device
        - In the case when RA cannot calculate hash of the original request due to an error, zero shall be returned
    - Hard error code

2.4.5.7.13 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. The EE schedules the initial download using the time specified in the RA Request Acknowledge (*accept)*.

- RA →EE _ Request Acknowledge

2.4.5.7.14 ASN.1 Specification

- **ee-ra.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/ee-ra.asn?at=refs/heads/master
- **`ee-ra-errors.asn`** `https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/ee-ra-errors.asn?at=refs/heads/master`

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

- **scms-protocol.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/scms-protocol.asn?at=refs/heads/master
- **scms-base-types.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/scms-base-types.asn?at=refs/heads/master
- **scms-error.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/scms-error.asn?at=refs/heads/master
- **scms-common-errors.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/scms-common-errors.asn?at=refs/heads/master
- 1609dot2-schema.asn
- 1609dot2-base-types.asn

2.4.5.8 Step 3.3: Pseudonym Certificate Generation

Target release	Core
JIRA Task	SCMS-76-Finish document "Pseudonym Certificate Generation"Closed
Document owner	John Turner
Reviewer	Jeff Hahn
QA	Erik Schetina

2.4.5.8.1 Goals

- Generate pseudonym certificates in a secure way while providing a high level of privacy protection from all involved entities.

2.4.5.8.2 Background and strategic fit

The overall design principle is that no SCMS element knows the complete set of pseudonym certificates belonging to a vehicle, or exactly which vehicle the pseudonym certificates have been sent to. The RA knows the enrollment certificate of the OBE that requested pseudonym certificates, but the RA does not know the actual certificates delivered to the OBE. The PCA knows each individual pseudonym certificate but the PCA does not know which pseudonym certificate will be in which OBE, nor does the PCA know which pseudonym certificates are used in the same OBE. This is achieved by appropriately dividing the whole process among several components including the LAs, the PCA and the RA. At a very high level, processing valid pseudonym certificate requests consists of the following steps:

- RA obtains (individual and group) pre-linkage values from 2 LAs. The EncryptedPrelinkageValue Data Structure was changed as of 2015-12-14 to be two distinct data structures, EncryptedIndividualPLV and EncryptedGroupPLV, defined in scms-base-types.asn.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

- **scms-base-types.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/scms-base-types.asn?at=refs/heads/master
- RA completes the butterfly key expansion and generate individual certificate requests to be sent to the PCA
- RA collects a sufficiently large number of individual certificate requests, shuffles them, and then sends them one by one to the PCA
- For each individual certificate request, PCA generates a valid pseudonym certificate, encrypts the certificate for the device specified in the request, signs the encrypted packet, and sends it to RA
- RA collates the individual encrypted-and-signed pseudonym certificates for each device by week, and makes them available for download by the device
- PCA stores the pre-linkage values, the linkage value, certificate and hash of the RA-PCA individual certificate request for future misbehavior investigation purposes

Pseudonym certificate provisioning is illustrated in Figure 13. The different steps in Figure 13 are elaborated below.

- The pseudonym certificate batch request is sent to the RA, and the pseudonym certificate response is returned to the vehicle through a Location Obscurer Proxy (LOP). The LOP obscures the physical location of the endpoints. The LOP obscures the vehicle's IP address as well as any other traceable signaling information. Without the LOP, the RA would be able to associate an enrollment certificate with a physical location, perhaps revealing information about the certificate holder.
- The pseudonym certificate batch request contains two seed public keys from the device. The RA uses the butterfly expansion function to compute two sets of public keys: one set of public keys will be used to encrypt the pseudonym certificates (k_e, one key per certificate) to the device and the other set will be used in the pseudonym certificates (k_s, one key per certificate). The RA sends an individual certificate request to the PCA for each pseudonym certificate requested. The PCA modifies each individual k_s by adding a random offset, c, prior to issuing each pseudonym certificate. The PCA includes the offset c in its response to the device which is encrypted with k_e. The device uses each offset c to adapt its private key to match the change made to the public key k_s by the PCA. See Section 2.4.2 of SCMS paper for details of butterfly keys.
- The generated pseudonym certificate is encrypted by the PCA for the OBE. The RA cannot read the contents of the pseudonym certificate, so it does not know which pseudonym certificates were issued in response to a request signed by a particular enrollment certificate.
- The PCA also signs the encrypted package. Otherwise, the RA could perform a man-in-the-middle attack and be capable of reading all the pseudonym certificates passed from the PCA to the device.
- The RA does not pass pseudonym certificate batch requests directly to the PCA. Instead, it aggregates certificate batch requests from many OBEs, creates individual certificate requests, and "shuffles" them together before sending them to the PCA. If the RA did not shuffle, the PCA would know that a particular collection of pseudonym certificates, issued in

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

sequence likely belong to the same OBE. The shuffling ensures that the CA cannot be sure that two pseudonym certificates issued at the same time belong to the same device.

- The LVs included in the pseudonym certificate are generated as described in Section 2.4.3 of SCMS paper. This ensures that the RA and each single LA do not know the LVs that appear in the finally issued pseudonym certificates. Note: The statement in Figure 14, saying that LAs are only needed if external CRLs are implemented, is currently considered as the default case. If no external CRLs are implemented, revocation must be done by internal blacklisting and denial of further pseudonym certificates. This is only effective if pseudonym certificates are preloaded for a relatively short period of time and the user frequently reloads. This, in turn, is impractical even under frequent connectivity. Appendix B of the SCMS paper elaborates on this topic.

Figure 1 Pseudonym Certificate Provisioning

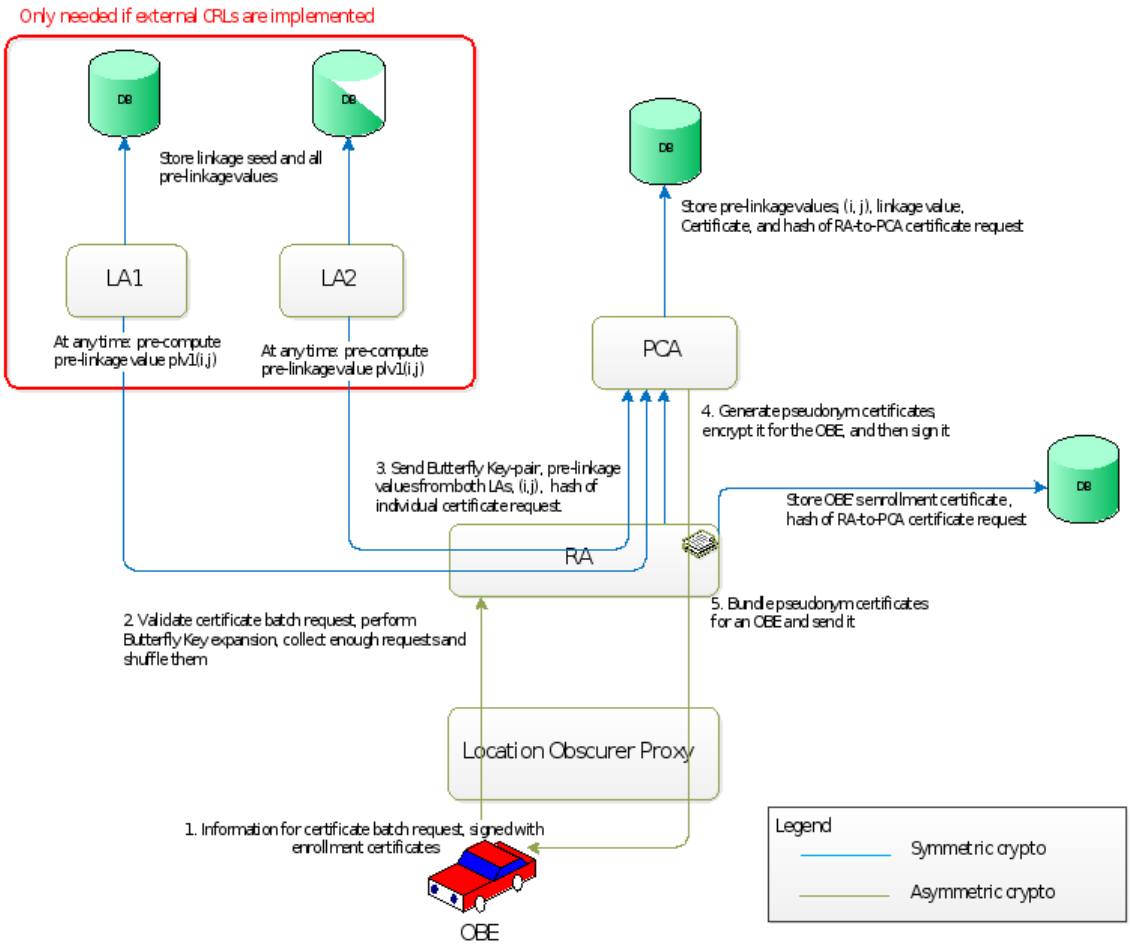


Figure 13: Pseudonym Certificate Provisioning

Below is a step by step description of the pseudonym certificate provisioning process.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

At any time: LA1 and LA2 calculate sets of PLVs plv1(i,j) and plv2(i,j), respectively, for a period (i,j) (see Section 2.4.1 of the SCMS paper for an explanation of time periods). PLV plv1(i,j) is derived from an LS value ls(i) (which is basically a hash-chain value) and index j as plv1(i,j) = $AES_{ls(i)}(j)$. The other PLV plv2(i,j) is derived in a similar way using different LS values. Note: In the following description, plv1 will be substituted for plv1(i,j) if the context is clear. The hashing algorithm SHA-256 is used for forward hashing and its output (32 bytes) is truncated to 16 bytes. The subsequent AES encryption operation has an output of 16 bytes and is truncated to nine bytes. The result of the AES encryption operation is the LVs, which are then encrypted for the PCA and sent to the RA where they will be used in a certificate request.

Request

- Step 1: The OBE creates a certificate batch request signed with the enrollment certificate, and gives it to the LOP. The certificate batch request includes a public butterfly key seed and the requested time period. This certificate batch request is encrypted to the RA. The LOP obscures the vehicle's identifiers (e.g., IP address) and forwards the certificate batch request to the RA.
- Step 2: The RA checks that the signature is valid, that the enrollment certificate was not revoked (via RA's internal blacklist), and that the same vehicle didn't already request pseudonym certificates for the same time period.
- Step 2.1: The RA sends a certificate batch request response to the OBE with estimated time the batch will be ready.

Generation

- Step 3: The RA performs the butterfly key mechanism detailed in Section 2.4.2 of the SCMS paper to expand a sequence of public keys and create a series of individual certificate requests.
- Step 4: The RA collects individual certificate requests, each with its expanded sequence of butterfly keys and sets of encrypted PLVs. Once enough such individual certificate requests are available, RA shuffles all individual certificate requests. Details are displayed in Figure 14. Note: The RA cannot obtain LVs by XORing the PLVs as the latter are encrypted for the PCA. Furthermore, there is integrity information in place to prevent the RA from including its own LVs. This could include signing the linkage information (by the LAs) for asymmetric cryptography or using an MAC for symmetric cryptography.
- Step 5: The RA forwards an individual certificate request consisting of butterfly key, plv1(i,j) and plv2(i,j) to the PCA. This communication is encrypted.
- Step 6: The PCA generates a pseudonym certificate with linkage value lv(i,j) = plv1(i,j) XOR plv2(i,j). The PCA adds a random offset, c, to the butterfly key (to prevent the RA from knowing the certificate public key and being able to correlate these with the enrollment certificate).
- Step 7: The PCA sends the encrypted (for OBE) and signed (by PCA) pseudonym certificate and random offset c to RA.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

- Step 7.1: RA determines next time OBE should come back to retrieve the NEXT batch of certificates. This time is put into an info file.
- Step 8: The RA bundles the encrypted pseudonym certificates and random offsets into a Certificate Batch Download with the .info file for a given OBE.
- Step 9: RA Stores bundle and .info file at the OBE download location (see Step 3.4: Download of Pseudonym Certificates).

Figure 2 Shuffling Certificate Requests

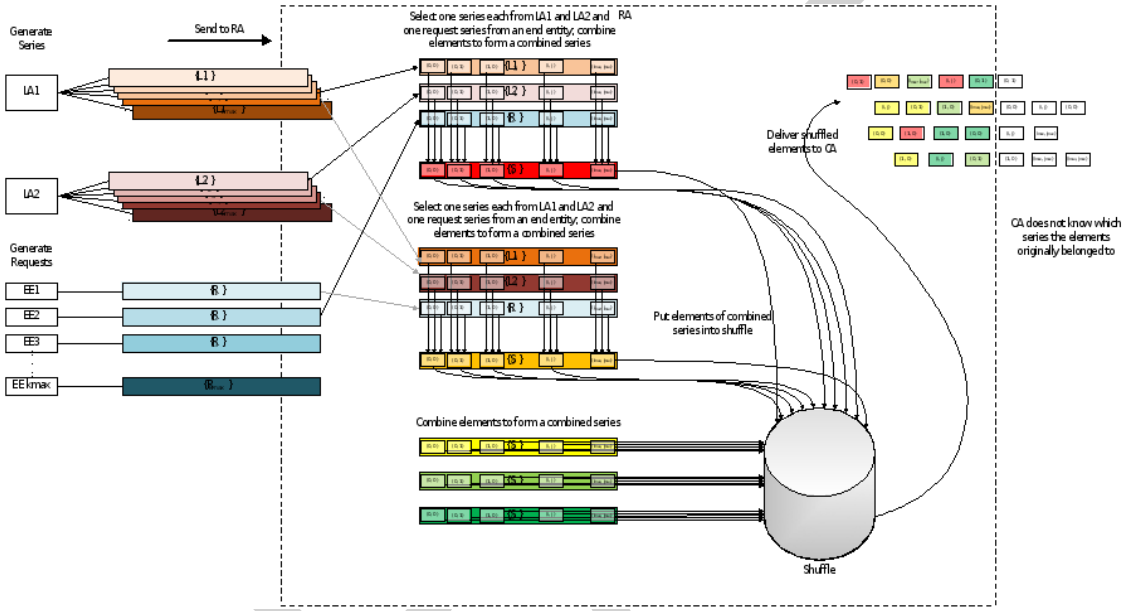


Figure 14: Shuffling Certificate Requests

The process of shuffling certificate requests is illustrated in Figure 14. In advance of this process, the RA builds chains of objects which consist of consecutive individual requests from a specific OBE and values of a given value chain from LA1 and LA2. The shuffling is then performed on the objects of this chain. With this, it can be guaranteed that despite the shuffling, the successive LVs corresponding to one OBE can be found by forward-hashing of the hash-chain values corresponding to the LVs. The RA additionally cannot derive the geographic location of the requester from the networking headers, such as the IP address, because the origin IP address is obscured by the LOP.

The entities LA1, LA2, the PCA and the RA store all information in a database. This information is only required for revocation and differs from one entity to another. Any information that is stored for revocation needs to be stored for 10 years. Any information that needs to be stored for device's lifetime will be stored for 40 years. For the POC, information for 17 million vehicles should be stored for 3 years.This information is briefly listed in detail below and will henceforth be referred to as "all information."
The PCA stores:

- LV

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

- PLVS plv1 and plv2 (to enable retrieving values from LA1 and LA2, respectively; only in the instance of misbehavior investigation, which is not covered in this paper)
- A hash of the individual certificate request (to enable internal blacklisting at the RA)
- A hash of the certificate truncated to eight bytes, CertID8 (to allow the MA to request something from the PCA even if it gets only the digest of the certificate.)
- Validity period of the certificate (start and end times)
- The value i that describes the position in the hash chain

The RA stores:

- Encrypted PLVs plv1 and plv2 (discarded after the certificate batch request is fulfilled)
- A hash of the individual certificate request. This value will be used by the MA to instruct the RA which enrollment certificate to put on the internal blacklist.
- LCIs, which can be used to request LSs from each of the LAs in the revocation process. LCIs are "pointers" to a linkage chain known at the RA and the LA. Using this information, the LA can identify the linkage chain and reveal the corresponding LS. (See Appendix D, Section D.3 for information on LCIs)
- The corresponding enrollment certificate
- Validity periods for requests for a given enrollment certificate

The LA stores:

- Chains of PLVs plv1 or plv2, depending on the LA. These are used for misbehavior investigation only, which is not covered in this paper.
- LCIs, pointing to linkage chains
- Revocation value, i.e., the ILS used for forward hashing

The PCA needs to perform efficient look-up of PLVs based on LVs and look-ups of "hash of individual certificate request" based on LVs. The LA needs to perform efficient look-up of LSs based LCIs and information on linkage based on PLVs. In both cases, the data being looked up should be considered restricted and should not be stored unencrypted. The following database layout is suggested for the PCA:

Index	Payload 1	Payload 2	Payload 3	Payload 4
LV	Encrypted Hash of individual certificate request	Encrypted PLVs	Truncated hash of certificate, CertID8	Validity period and position i in hash chain

The situation at the LA is slightly different: the look-up needs to be performed based on the PLV. Using the PLVs as index and encrypted LSs as payload has a significant drawback. In case of a breach, an attacker would learn which PLVs map to the same encrypted LS. Instead, the hash of the PLV is used. Consequently, the following database layout is suggested for the LA:

Index	Payload

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Hash(PLV)	Encrypted LS

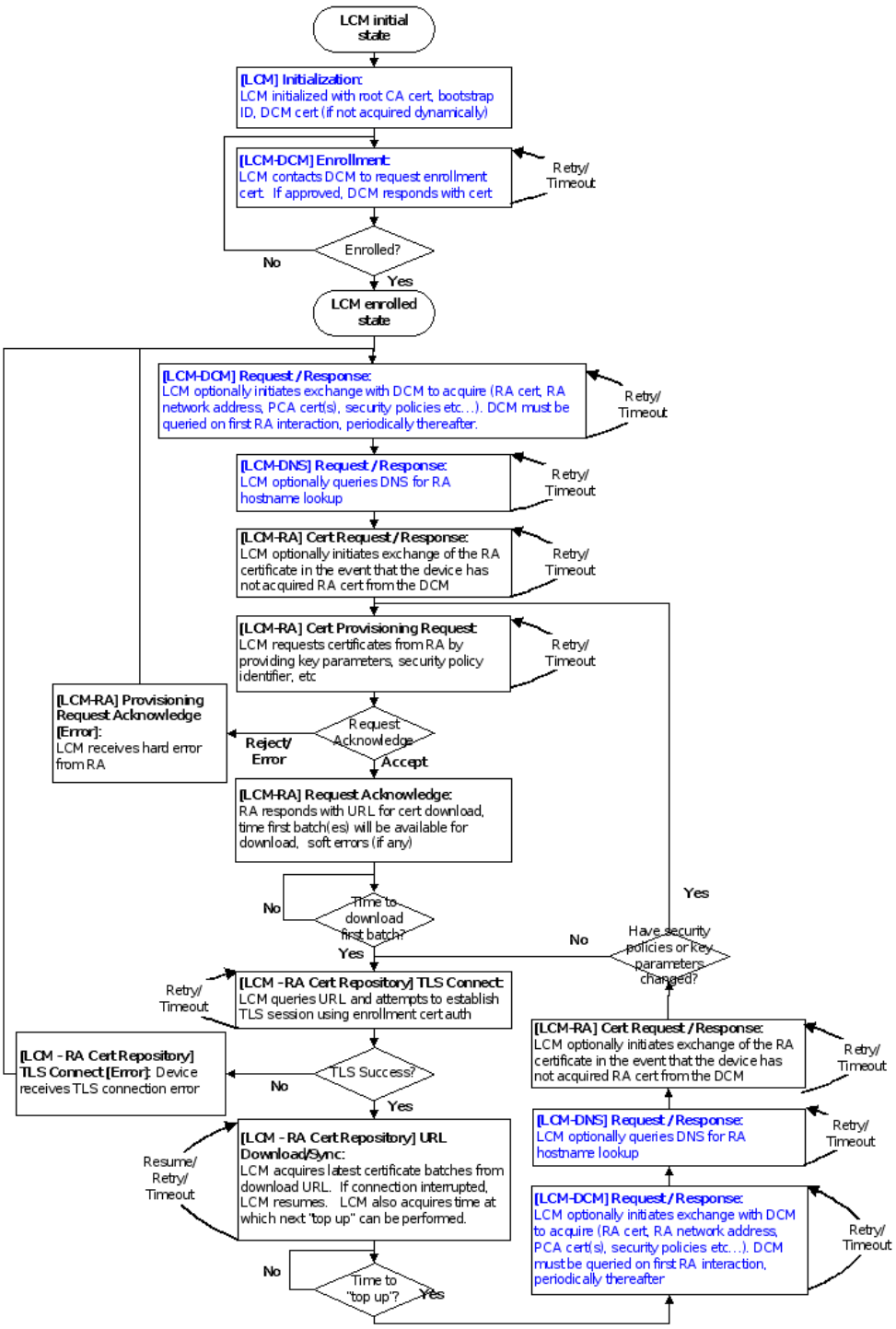
Index	Payload
LCI	Encrypted LS

In order to reduce data rate requirements between OBEs and the SCMS, butterfly keys are used. The butterfly key mechanism is in place between OBEs, the RA and the PCA. See Section 2.4.2 of the SCMS paper for details of butterfly keys.
Further details of shuffling at the RA are discussed in sections 4.2.3.2 and 8.1.2 along with the continuation of existing hash chains in follow up certificate batch requests.

Below is a device's lifecycle flowchart to further assist in understanding the pseudonym certificate provisioning process.

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary



2.4.5.8.3 Assumptions

- LA and PCA shall establish a symmetric encryption key via LA-PCA key exchange (see la-pca.asn).

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

- RA and PCA complete all necessary sanity checks and signature verification before fulfilling with certificate provisioning request.
- Requested certificate uses a public key derived from a butterfly key and is valid within the specified constraints such as time period, geographic region, etc.)

2.4.5.8.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-526	Tests failed	Certificate validity	RA shall request PCA to generate certificates with validity overlap for any 2 consecutive weeks by a time $t_{overlap}$, which is currently set to be 1 hour.	The original value for $t_{overlap}$ was 1 minute but there are safety concerns with such a small overlap. For example a device could be in an alert state for more than 1 minute. Extending $t_{overlap}$ to 1 hour (60 minutes) reduces the risk of a vehicle operating without a valid certificate.		RA
SC	In	RA global	RA shall implement the	Standard		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
MS-527	Implementation	policy	following from the Global policy: • certGenTimePeriod • validityModel • multCertsPerWeek • singleCertsOverlappingInSeconds	parameters required for certificate generation, defined by SCMS Manager as global policy items.		
SCMS-528	Closed	Reduced privacy-preservation mode	RA shall provide a reduced privacy-preservation mode for OBE manufacturers that eliminates the delay introduced in standard mode caused by waiting to accumulate a threshold of certificate requests to shuffle.	Manufacturer may be unable to wait for the certificate request threshold to be reached. For example, a manufacturing process can't be delayed waiting for the RA to have enough requests.	For PoC: reduced privacy mode means no shuffling and all initial request are fulfilled in reduced privacy mode	RA
SCMS-530	Closed	Store RA information	RA shall store information specified above (RA-stores) for a duration currently set to	so that EE can be revoked	PoC will only store 3	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			be 10 years	properly. 10 chosen as number of years of certificates (3) plus 7 years for historical purposes (law enforcement, legal, etc.).	years	
SCMS-531	Closed	Store LA information	LA shall store information specified above (LA-stores) for a duration currently set to be 10 years	10 chosen as number of years of certificates (3) plus 7 years for historical purposes (law enforcement, legal, etc.).	PoC will only store 3 years	LA
SCMS-532	Closed	Store PCA information	PCA shall store information specified at PCA-stores for a duration currently set to be 10 years	10 chosen as number of years of certificates (3) plus 7 years for historical purposes	PoC will only store 3 years	PCA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				(law enforcement, legal, etc.).		
SCMS-617	In Implementation	Change in certs per week	RA shall handle a change in allowed certs per week based on global policy file. For example, a change from 20 certs per week to 40 certs per week.	SCMS Manager may update global policy file parameter for number of certs per week.		RA
SCMS-1304	Review	PCA issues implicit certificates	PCA shall issue implicit OBE enrollment, pseudonym, and OBE identification certificates, rather than explicit certificates.	To save storage space and over-the-air bytes		PCA
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
SC	Review	PSID/SSP	PCA/RA shall read the	PSID/SS		PCA,

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
MS-1372		assignment to certificates	set of PSID/SSP values of the enrollment certificate that was used for the certificate request and use the exact same set to OBE and RSE certificates during provisioning.	Ps shall be assigned in groups such that corresponding applications are similar in nature.		RA

10 issues

2.4.5.8.5 ASN.1 Specification

- **la-ra.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/la-ra.asn?at=refs/heads/master
- **la-ra-errors.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/la-ra-errors.asn?at=refs/heads/master
- **pca-ra.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/pca-ra.asn?at=refs/heads/master
- **pca-ra-errors.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/pca-ra-errors.asn?at=refs/heads/master
- **scms-protocol.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/scms-protocol.asn?at=refs/heads/master
- **scms-base-types.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/scms-base-types.asn?at=refs/heads/master
- **scms-error.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/scms-error.asn?at=refs/heads/master
- **scms-common-errors.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/scms-common-errors.asn?at=refs/heads/master
- 1609dot2-schema.asn
- 1609dot2-base-types.asn

2.4.5.9 Step 3.4: Download of Pseudonym Certificates

Target release	Core

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

JIRA Task	SCMS-77-Finish document "Download of Pseudonym Certificates"Closed
Document owner	Andre Weimerskirch
Reviewer	Jeff Hahn
QA	Erik Schetina

2.4.5.9.1 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, to the greatest extent possible, prevent a certified device (that has not been revoked) from running out of credentials required for critical safety systems to operate.

2.4.5.9.2 Background and strategic fit

The purpose of this exchange is to provide a defined method that a certified EE 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) a .info file that includes the time when certificates will be available and (3) a global certificate chain file containing all PCA certificate chains required to validate the pseudonym certificates, but not the policy file.

2.4.5.9.3 Assumptions

1. The EE will abandon further interactions with the RA after a certain number of failed communication attempts resulted in critical errors.
2. The EE will not attempt to execute the certificate provisioning process if it finds itself on the latest CRL (assumes that the device has not been compromised by a willful violator). The device will need to execute the certification/bootstrap process again to exit a revoked state.
3. The EE may terminate the certificate batch download process if sufficient storage is not available for subsequent batches.
4. RA issued certificates and stored them in a folder on RA for EE to download.
5. The Step 18.5: Generate Global and Local Certificate Chain File has been downloaded and processed into the trust-store of the EE (necessary for PCA Certificate Validations).
6. The Step 18.5: Generate Global and Local Certificate Chain File is being actively monitored by the EE for updates as described in Step 3.1: Check for policy updates.

2.4.5.9.4 Requirements

This is an extension to Certificate Provisioning Requirements:

Key	Status	Summary	Description	justification	notes	Component/s
SCMS	SCMS PoC out	EE Authentication	The EE shall authenticate	Messages from	This is out of scope since it defines EE's	On-board

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
- 411	of Scope	to RA for Request	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.	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.	behavior.	Equipment (OBE), Road-side Equipment (RSE)
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	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

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				process.	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 certs currently. Instead the OBE will use TLS to authenticate the other endpoint (as a server) and will use its SCMS cert to identify itself. EE authenticates via its IEEE 1609.2 enrollment certificate. The details of the authentication process are defined Step 3.4: Download of Pseudonym Certificates	RA
SCMS-517	In Implementation	Tunneling through LOP	RA shall provide downloads only via a LOP hardware interface, which removes all location information	to anonymize the location of EEs.		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			from the incoming request.			
SCMS-534	Closed	Certificate Batch	RA shall store certificates to be downloaded by EE in a specific folder known to EE.	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 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	On-board Equipment (OBE), RA, Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				pseudonym certificates, that an adversary is able to read PCA-encrypted pseudonym certificates (adversary might extract Butterfly encryption keys from junked vehicle at a later stage and is then able to identify all EE certificates).	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 communicatio	EE checks whether it talks to	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE),

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			n starts.	proper RA before communication starts and to avoid sending its enrollment certificate to a malicious RA. RA authenticates via its TLS X.509 certificate. The details of the authentication process are defined in Step 3.4: Download of Pseudonym Certificates.		Road-side Equipment (RSE)
SCMS-	In Implementation	OCSP stapling - RA	The RA shall support OSCP stapled	This is as a means	OCSP stapling provides improved performance	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
540			certificate response to OBE.	to react to RA's revocation. In case the RA is compromised, and the DNS server is compromised or spoofed, then a revocation mechanism will prevent further damage.	compared to CRLs. OCSP stapling is specified in RFC 6066, Section 8. 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). The RA will be able to respond to the OBE's request for an OSCP stapled certificate. The RA itself will be able to request OCSP certificate currency from an OCSP server in order that it (the RA) is assured of the other components TLS cert currency, so it will require the OCSP request URL and credentials.	
SCMS-541	SCMS PoC out of Scope	OCSP stapling - EE	The EE may use the TLS Certificate Status Request extension (OCSP stapling) to verify RA revocation	Revocation is optional and it's up to the OEMs support it.	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	On-board Equipment (OBE), Road-side Equipment

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			status.		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.	(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
SCMS-544	Closed	Download resume	RA shall support byte-wise resume of certificate batch,	to improve reliability of the downlo		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			certificate file, or policy file, downloads, even if EE switches the IP address.	ad protocol.		
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 life-time of the SCMS. It might even vary for different EEs.		RA
SCMS-548	Closed	X.info file	RA shall provide an .info file for download by EE.	The .info file provides information when new pseudonym certificates, or identification certificates, can be downlo	see Certificate Batch Download for more information.	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				aded.		
SCMS-549	Closed	Keep Certs	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-958	SCMS PoC out of Scope	Error code: eeConnectionFailed	EE shall log this error in its log file, 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 provide this error code to EE, if certificate batch is not available.	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.	to enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			because there is none or it's corrupted), OBE shall implement OEM defined error handling and store the error code in OBE's error log file.			
SCMS-966	SCMS PoC out of Scope	Misbehavior reporting: 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's 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 implement OEM defined error handling and store the error code in EE's error log file, 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-	SCMS PoC out of	Misbehavior reporting: eeCertFileVerificati	EE shall initiate a misbehavior report to MA	to enable server side	This is out of scope since it defines EE's behavior.	On-board Equipment

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
968	Scope	onFailed	with the observed error, if EE is not able to verify the digital signature of an encrypted certificate.	misbehavior detection.		(OBE), Road-side Equipment (RSE)
SCMS-969	SCMS PoC out of Scope	Error code: eeCertificateFileDecryptionFailed	EE shall implement OEM defined error handling and store the error code in EE's error log file, 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 reporting: 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 implement OEM defined error handling and store the error code in EE's error log file, if EE is not able to	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

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			verify a certificate.			(RSE)
SCMS-972	SCMS PoC out of Scope	Misbehavior reporting: 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 implement OEM defined error handling and store the error code in EE's error log file, 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 reporting: 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	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)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			content.			
SCMS-976	In Implementation	Error code: raInvalidURL	RA shall log this error code, 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	Error code: raNoTLS	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 this error, if EE-to-RA authentication fails.	to enable server side diagnostics and to avoid giving potential attackers relevant information.		RA
SC	SCMS	Error code:	EE shall store	to	This is out of scope	On-

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
MS-979	PoC out of Scope	eeAuthenticationFailed	this error code in EE's error log file, if RA-to-EE authentication fails.	enable EE side diagnostics.	since it defines EE's behavior. This is part of TLS handshake. OEM defines EE error handling.	board Equipment (OBE), Road-side Equipment (RSE)
SCMS-980	SCMS PoC out of Scope	Misbehavior reporting: 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 this error, if Global Certificate Chain File is not available.	to enable client side error handling.		RA
SCMS-982	Implemented	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 this error code, if it is not able to	to enable EE side error	This information is probably provided by an entry in the .info file	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			provide a current .info file.	handling.		
SCMS-984	SCMS PoC out of Scope	Error code: eeInfoFileDownloadFailed	OBE shall implement OEM defined error handling and store the error code in its error log file, if OBE is not able to download the .info file (e.g. because there is none or it's 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 reporting: eeInfoFileDownloadFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to download the .info file (e.g. because there is none or it's corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)
SCMS-1090	In Implementation	Error code: rseRaTcpErrors	RA shall return standard TCP error codes if TCP errors occur.	in order to enable client side error handling.		RA
SCMS	SCMS PoC out	EE certificate download via	EE shall use HTTPS (TLS)	in order to use	This is out of scope since it defines EE's	On-board

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
-1201	of Scope	HTTPS over TCP/IP	over TCP/IP to download files from the SCMS.	standard internet technology	behavior.	Equipment (OBE), Road-side Equipment (RSE)
SCMS-1203	Implemented	Check time stamp	RA shall check the signed (by EE) time-stamp and allow a tolerance of 5 seconds.	If the difference between the signed time-stamp and the current time is 5 seconds or less, RA will proceed with the authentication process. Otherwise RA will reject the connection.		RA
SCMS-1204	Implemented	Check blacklist	RA shall reject EE request, if EE is listed on its blacklist.	If EE is listed, RA will reject the connection.		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				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 informa		

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				tion, 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 certificates.	The .info file lists the time when pseudonym certificates will be	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				available next time. EE downloads that file each time it tries to download pseudonym certificates.		
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.	Whenever EE tries to download certificates, it also downloads the .info file. EE will contact RA again to download certificates after the time listed in the .info file.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS	SCMS PoC out	EE download	EE shall try byte-wise	This will		On-board

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
-1263	of Scope	resume	resume of CRL downloads from the CRL store, certificate batches, certificate files, or policy files from RA in case a previous download failed.	improve reliability of the download process and reduce communication cost.		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)

45 issues

2.4.5.9.5 Design

- Step 0: EE and RA authenticate to each other, see below.
- Step 1: EE downloads the global certificate chain file (see file definition in Step 18.5: Generate Global and Local Certificate Chain File).

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

- Step 2: EE downloads all certificate files X_Y.tar, 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). EE downloads either all available files X_Y.tar, or as many as possible.
- Step 3: EE 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 EE to determine the earliest time which new certificate batches will be available for download, the RA shall maintain a signed 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 1609 format Time32 timestamp that the EE will use to schedule a subsequent "top-up" download.

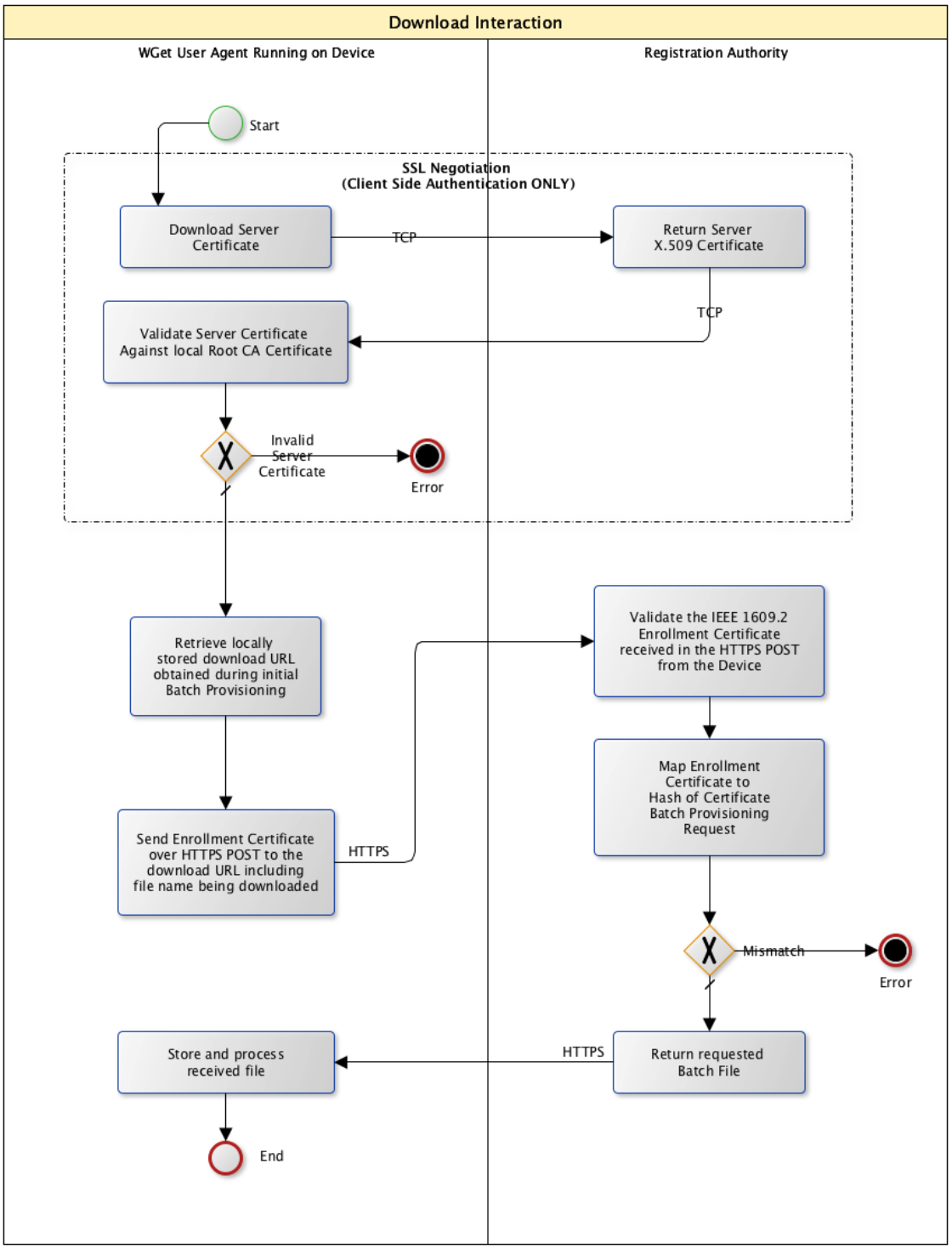
For more details: See Sections 6.6.2.3 and 6.6.2.4 in V2V-SE Minimum Performance Requirements (SAE J2945) - Word File.

2.4.5.9.5.1 EE-RA Authentication and RA-EE Authentication

1. If necessary, EE first requests RA's X.509 certificate
2. EE then establishes a secure TLS connection with RA (RA authenticates to EE).
3. EE then digitally signs the current time of type IEEE 1609.2 time32 with EE's enrollment certificate
4. EE uses POST to include the IEEE 1609.2 enrollment certificate, the current time of type time32, the digital signature over the current time, and the file to download. Note that this payload is TLS protected.
5. RA validates the enrollment certificate against the internal blacklist, and then verifies the enrollment certificate.
6. RA validates the time-stamp against a configurable time tolerance (default value is 5 seconds), and then digitally verifies the signature of the current time.
7. 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 4, and the verification of Step 6.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary



2.4.5.9.5.2 RA Revocation

RA's X.509 certificate is issued by an X.509 Root CA certificate that is known by EE. EE will perform the following check before Step 2 in above EE-RA mutual authentication:

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

- EE validates whether RA's X.509 certificate was issued by the X.509 Root CA, 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.

2.4.5.10 Step 3.5: Schedule generation of subsequent batch of Pseudonym Certificates

Target release	Core
JIRA Task	SCMS-78-Finish document "Generate subsequent batch of Pseudonym Certificates"Closed
Document owner	John Turner
Reviewer	Jeff Hahn
QA	Erik Schetina

2.4.5.10.1 Goals

- This use case differs from initial pseudonym certificate generation in that it is just scheduling. Once scheduling is done, follow the steps from Step 3.3: Pseudonym Certificate Generation for generating certificates.

2.4.5.10.2 Background and strategic fit

Once a device has made an initial request for pseudonym certificate provisioning, the RA starts pre-generating certificates for as long as the device is still operational.

2.4.5.10.3 Assumptions

1. The RA will retain certificates from the current date to the maximum duration set by the security policy (e.g., three years).
2. The RA will 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. This feature may help devices recover from a loss of certificates at the device level (e.g., disk corruption).

2.4.5.10.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS--	SCMS Po	Stop pre-generat	RA shall stop pre-generatin	So that computing	Stop/resume pre-generation is out of scope for PoC. Time is currently set to be 3 years. Based on	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
508	C out of Scope	ing certificates for inactive device	g pseudonym/OBE identification certificates for a device that has not connected to RA for a given amount of time as specified by the SCMS Manager	resources are not wasted for inactive devices. If device has not connected for a certain period of time, the assumption is the device is no longer available or in service.	the implementation, the LA may also stop pre-generating pre-linkage values.	
SCMS-509	Closed	Stop pre-generating pseudonym certificates for revoked device	RA shall stop pre-generating pseudonym and OBE identification certificates for a device	so that computing resources are not wasted for revoked devices		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			that has been revoked by the MA, i.e., for a device that appears on RA's internal blacklist.			
SCMS-553	SCMS PoC out of Scope	Resume pre-generating certificates	RA shall resume pre-generation of pseudonym/OBE identification certificates if an OBE submits a new request after a silent period where RA had stopped pre-generating	If the OBE submits a valid request, it is a signal that the OBE is participating again regardless of the length of the silent period.	Stop/resume pre-generation is out of scope for PoC.	RA
SCMS-1293	Review	Schedule pre-generation of OBE pseudo	RA shall schedule pre-generation of certificat	Certificate requests may vary. The	For pseudonym certificates, the availability requirement is specified in http://wiki.campllc.org/display/SP/3.4.+Download+of+Pseudonym+Certificates. For identification certificates, a certificate for the next time period shall always be	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
		nym and OBE identification certificates	es to meet the availability requirements of certificate download defined by the SCMS Manager.	SCMS must ensure that certificates are available before the current certificate expires.	available.	

4 issues

2.4.6 Use Case 5: Misbehavior Reporting

Target release	Release 1.1
JIRA Task	SCMS-137-Finish document "Misbehavior Reporting"QA
Document owner	Biswajit Panja
Reviewer	
QA	

2.4.6.1 Goals

- Maintain the trust in the system
- Identify and remove bad actors

2.4.6.2 Background and strategic fit

OBEs send misbehavior reports to the MA. 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 OBE for the MA. Note: The OBEs' misbehavior detection algorithms (also called local misbehavior detection) are not defined yet.

The following steps are executed:

- Step 1: OBE creates a misbehavior report, encrypts it to the MA, and submits it to the RA.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

- Step 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. RA shuffles misbehavior report and send to MA. 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).
- Note: Misbehavior report older than one week not required to be stored in OBE(not requirement, for informational purposes)
- No separate ACK, RA to OBE.

2.4.6.3 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
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 be used to identify the location of the OBE before forwarding the misbehavior report to the RA.	to protect the identity of the sending OBE.	This does not apply to misbehavior reports send by RSEs.	LOP, RA
SCMS-686	In Implementation	Shuffle	RA shall shuffle misbehavior reports before	Shuffling ensures MA cannot be sure that two misbehavior reports coming at the same time are from same OBE.	Amount of shuffle and/or maximu	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			sending them to MA.		m delay decided by SCMS manager.	
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-1013	SCMS PoC out of Scope	Error code: eeEncryptionFailed	EE shall store this error in its error log file, 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 store this error in its error log file, if MA encounters an error when decrypting a	to enable server side diagnostics.		MA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			misbehavior report.			
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 and include liability.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)
SCMS-1339	Review	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 misbehavior report	MA shall verify a misbehavior report by (1) checking the	This is MA's counterpart to https://jira.campllc.org/browse/SCMS-1308~~SCMS-1308~~	This is for POC only, and might need revision	MA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			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.		for deployment.	
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	Review	RA accept HTTP post over TCP/IP	RA shall accept HTTP post requests	to allow the SCMS endpoint to serve everything based on	RA - Services View will	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			from authenticated EEs.	HTTP protocol	document the actual HTTP post details This is out of scope as it defines EE behavior.	

2.4.6.4 ASN.1 Specification

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

- **ee-ma.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/ee-ma.asn?at=refs/heads/protocols
- **ee-ma-errors.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/ee-ma-errors.asn?at=refs/heads/master

2.4.7 Use Case 6: CRL Download

Target release	Release 1.0
JIRA Task	SCMS-138-Finish document "CRL Download"In Review
Document owner	Rob Lambert
Reviewer	Benedikt Brecht
QA	Erik Schetina

2.4.7.1 Goals

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

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

2.4.7.2 Background and strategic fit

EE must be made aware of revoked entities.

2.4.7.3 Assumptions

- A CRL file has been successfully generated and signed by the CRL Generator, and has been made available to the CRL Store (these are both components of the MA).
- The CRL Store is able to cryptographically validate the signature on the CRL file prior to making it available for EEs to download.
- The EE has already been provisioned and is able to readily communicate with the CRL Store.
- The EE is able to download the CRL by issuing a CRL wget request to the CRL Store.
- The CRL Store will not authenticate the EE, i.e., CRL Store will not require that EE authenticates by EE's enrollment certificate.
- The EE is able to download the components CRL by issuing a CRL wget request to the CRL Store.

2.4.7.4 Requirements

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-1264	Review	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		CRL Store

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				cost.		
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-997	In Implementation	CRL Store validates CRLs	An updated CRL shall be cryptographically verified before it is entered into the CRL Store. This will ensure that new CRL changes take effect immediately and EEs always receive the newest CRL when requests are made.	To ensure that invalid CRLs are not distributed.		CRL Store
SCMS-995	SCMS PoC out of Scope	Error code: eeCRLVerificationFailed	EE shall store this error in its log file, if EE's 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	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
					misbehavior.	
SCMS-994	SCMS PoC out of Scope	Error code: eeCRLDownloadFailed	EE shall store this error and the reason in its log file, 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-991	SCMS PoC out of Scope	Error code: eeCRLStoreAuthenticationFailed	EE shall store this error in its log file, 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-342	In Implementation	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	The CRL Store does not authenticate EE before download of the CRL starts, i.e., EE does not authenticate by using	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				be valid).	its enrollment certificate to CRL Store but EE can download the CRL without authentication to CRL Store.	
SCMS-341	In Implementation	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	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-340	In Implementation	CRL availability	There shall be at any given time a CRL available for download at the CRL store.	To ensure that an EE can always download a CRL.		CRL Store
SCMS-	SCMS PoC out	EE issues a CRL Request	An EE shall issues a HTTP get to the CRL Store to	The EE needs to be	This is out of scope	On-board Equipm

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
335	of Scope		obtain the latest CRL.	provided with current CRLs so that the EE can be informed of revoked components.	since it defines EE's behavior.	ent (OBE), Road-side Equipment (RSE)

11 issues

2.4.7.5 ASN.1 Specification

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

2.4.8 Use Case 8: OBE Revocation

Target release	Release 1.0
JIRA Task	SCMS-140-Finish document "OBE Revocation"Open
Document owner	Andre Weimerskirch
Reviewer	
QA	

2.4.8.1 Goals

- Perform misbehavior investigation and eventually revocation of OBEs.

2.4.8.2 Step 8.1: OBE Misbehavior Analysis

Target release	Release 1.0
JIRA Task	SCMS-141-Finish document "Misbehavior Analysis"In Review
Document owner	Andre Weimerskirch
Reviewer	
QA	

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

OBE Misbehavior Analysis will be defined by CAMP's VSC6 Communications Research (CR) project and integrated with the to be awarded "Misbehavior Authority Integration" sub project.

OBE Misbehavior Analysis is out of scope of POC. For POC, this is a "black box" that determines whether an EE misbehaved or not. The MA misbehavior analysis algorithm (aka Global Misbehavior Detection) will leverage the Investigation methods described in Step 8.2: OBE Misbehavior Investigation.

A potential model for OBE Misbehavior Analysis is a black box that upon input of all misbehavior reports outputs certificates together with the label 'misbehavior detected'. The OBE Misbehavior Analysis leverages the OBE Misbehavior Investigation functions for this task. After the OBE Misbehavior Analysis outputs the labeled certificates, it passes those certificates to the OBE Revocation (Step 8.3: OBE Revocation (CRL, blacklist)).

The steps are as follows:

1. Misbehavior reports are provided by EE to SCMS
2. SCMS invokes Misbehavior Analysis and passes all misbehavior reports
3. Misbehavior Analysis runs the Global Misbehavior Detection and utilizes OBE Misbehavior Investigation.
4. Misbehavior Analysis continuously outputs certificates that were identified as 'misbehaving'.
5. The SCMS invokes OBE Revocation with certificates identified as 'misbehaving'

2.4.8.2.1 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-611	In Implementation	Revoke all reported certs	The MA shall revoke each reported certificate directly.	For testing purposes the PoC needs to have a simple mechanism to create CRLs.	Requirement for PoC only.	MA

1 issue

2.4.8.2.2 Not Doing

- Implementation of Misbehavior Analysis. This will be implemented by CAMP CR project.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

2.4.8.3 Step 8.2: OBE Misbehavior Investigation

Target release	Release 1.0
JIRA Task	SCMS-142-Finish document "OBE Misbehavior Investigation"In Review
Document owner	Andre Weimerskirch
Reviewer	
QA	

Changes to misbehavior investigation are currently discussed and changes might be introduced. Those changes will not be part of the first version but might be implemented in a later version.

2.4.8.3.1 Goals

- The Misbehavior Investigation is a set of functions that support Misbehavior Analysis (see Step 8.1: OBE Misbehavior Analysis).

2.4.8.3.2 Background and strategic fit

- To support Misbehavior Analysis.

2.4.8.3.3 Assumptions

Overall Assumptions and Requirements, if any, are provided below. Specific Assumptions and Requirements, if any, are provided in the sub-sections 8.2.1 MA-PCA: linkage value -> pre-linkage value, LA's host name and 8.2.2 LA - MA: pre-linkage value -> LinkageInformation.

2.4.8.3.4 Design

Misbehavior Investigation

Misbehavior Investigation is also named Misbehavior Detection in prior documents. The Misbehavior Investigation is a new concept introduced in the Study 3 report. Misbehavior Investigation comprises two main functions that are listed below.

The natural flow is that (1) MA will map a linkage value to an encrypted pre-linkage value (an encrypted pre-linkage value that matches the value LA originally encrypted to PCA during pseudonym certificate provisioning) and LA's hostname using PCA, and then (2) query LA with the encrypted pre-linkage values to receive additional related information (such as "do the two input pre-linkage values belong to the same linkage chain").

Note that interface functions allow for batch handling, i.e., rather than a single value typically an array of values is input and returned. For ease of explanation, the basic case is explained below.

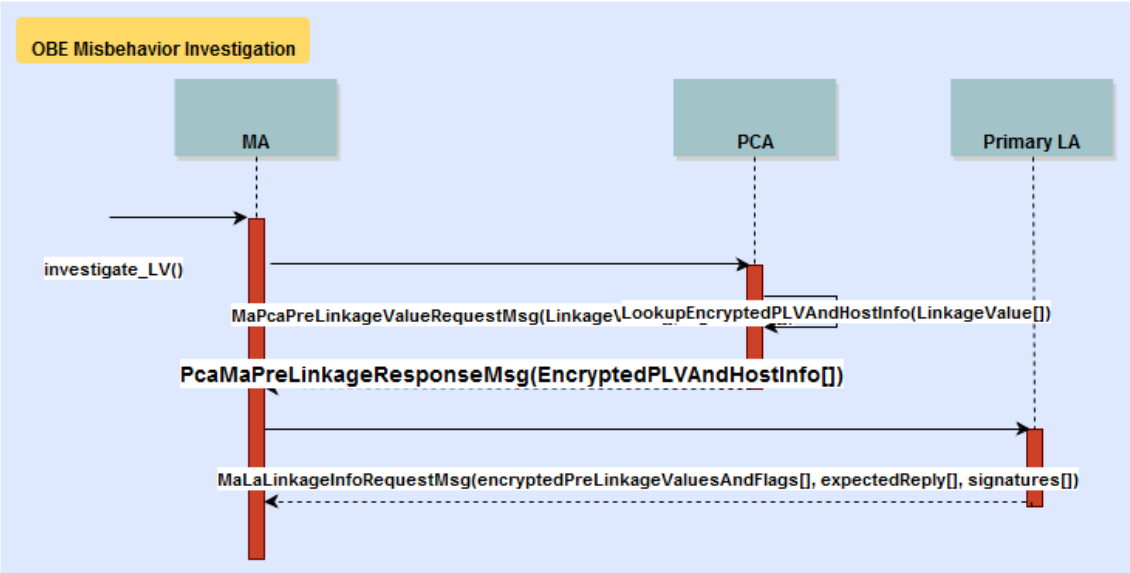
1. MA - PCA: Maps a linkage value to an encrypted pre-linkage value (encrypted using symmetric key shared between LA and PCA) and corresponding LA's host name. Note that there is the concept of a primary LA, and that the returned value is the same as created by the primary LA (also see Assumptions2). **Alsonote that the return value is a set of encrypted pre-linkage values. PCA simply returns an encrypted pre-linkage value (encrypted using symmetric key shared between LA and PCA) that matches the value that PCA received during pseudonym certificate provisioning.**

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

a. MA → PCA _ MA requests pre-linkage values from PCA (Misbehavior Detection)

b. PCA → MA _ PCA replies to pre-linkage values request (Misbehavior Detection): PCA responds with a set of **encrypted** pre-linkage values.

2. LA - MA: Maps a set of encrypted pre-linkage values to LinkageInformation. LinkageInformation provides valuable information, such as "how many of the input pre-linkage values belong to the same linkage seed chain". See LA → MA _ LA replies with linkage information (Misbehavior Detection) for a description of LinkageInformation. This interface is complex and powerful, and future modifications are likely.



2.4.8.3.5 ASN.1 Specification

- **ma-pca.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/ma-pca.asn?at=refs/heads/master
- **`ma-pca-errors.asn`** `https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/ma-pca-errors.asn?at=refs/heads/master`
- **`la-ma.asn`** `https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/la-ma.asn?at=refs/heads/master`
- **`la-ma-errors.asn`** `https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/la-ma-errors.asn?at=refs/heads/master`

2.4.8.3.6 Step 8.2.1: MA-PCA: linkage value -> encrypted pre-linkage value, LA's host name

Target release	Release 1.0
JIRA Task	SCMS-494-Finish document "MA-PCA: linkage value -> pre-linkage value, LA's host name"In Review

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Document owner	Andre Weimerskirch
Reviewer	
QA	

2.4.8.3.6.1 Assumptions

- There is a mechanism in place that allows MA to prove that MA is authorized to request this information. For the purpose of POC, this is a digital signature.
- There is the concept of a primary LA. PCA provides information related to the primary LA only.

2.4.8.3.6.2 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-407	In Implementation	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 a OCSP service at the technical component of the SCMS manager shall be deployed for revocation. See SCMS-406 for information about the cipher suite, SCMS-1016 for information about OCSP, and https://jira.campllc.org/browse/SCMS-938~~SCMS-938~~ for TLS certificate management.	CRL Store, CRLG, DCM, ECA, IBLM, LA, MA, PCA, PG, RA
SCMS-789	In Implementation	Error code: internalTimeout	LA, PCA, RA shall return and log this error code, if there is	to enable server side error handling.		LA, PCA, RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			an internal timeout within the component such that it cannot correctly process the request in time but can still respond to the MA.			
SCMS-791	In Implementation	Verify MA request authorization	LA, PCA and RA shall verify the MA requests in terms of authorization. If the verification fails, it shall return an error to MA and add an entry to its error log. Otherwise it shall	LA, PCA, RA only accepts requests from MA that use a valid format and that are authorized. The authorization process is done by signature.	There is a set (sequence) of countersignatures per request. These countersignatures are provided by some trusted authority, and only if the signatures verify successfully, the the command will be executed. It's a policy decision which authorities need to sign the requests. For instance, it could be as simple as MA, or as difficult as some real-world legal entity (e.g. NHTSA).	LA, PCA, RA

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			start its computation.			
SCMS-792	In Implementation	Error code: noMaAuthorizationSignature	LA, PCA and RA shall return this error code and add an error entry to its log file, if a request from the MA does not have a signature.	to enable server side error handling.	LA, PCA and RA only accept requests that use a valid format and that are authorized. The authorization process is done by signature.	LA, PCA, RA
SCMS-793	In Implementation	Error code: invalidMaAuthorizationSignature	PCA shall return this error code and add an error entry to its log file, if the MA authorization signature is invalid.	to enable server side error handling.	PCA only accepts requests that use a valid format and that are authorized. The authorization process is done by signature	PCA
SCMS-	In Implementation	PCA linkage value request limit	PCA shall be able to process a	Set a maximum value to allow		PCA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
802			request input of up to a configurable amount of linkage values	proper sizing of IT.		
SCMS-803	In Implementation	Request limit: POC	For POC, PCA shall be able to process a request of up to 10,000 linkage values.	upper performance limit		PCA
SCMS-874	In Implementation	Validation	PCA shall validate the input. If the validation fails, PCA shall return an error to MA. Otherwise PCA shall starts its computation.	PCA only accepts properly formatted requests with a valid value.		PCA
SCMS-	In Impleme	Error code: pcaInvalidInputValue	If the input values	To enable error		PCA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
875	ntation	Format	are improperly formatted, PCA shall provide this error code	handling.		
SCMS-876	In Implementation	Error code: pcaInvalidLinkageValue	If an invalid linkage value is input, PCA shall provide this error code	To enable error handling.		PCA
SCMS-880	In Implementation	PCA return encrypted pre-linkage values	PCA shall provide an interface to return an array of encrypted pre-linkage values (one per input linkage value) and corresponding primary LA's host name	Ensure correctness.		PCA

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			given an array of linkage values as detailed in MA → PCA_MA requests pre-linkage values from PCA (Misbehavior Detection) (request) and PCA → MA_PCA replies to pre-linkage values request (Misbehavior Detection) (response). Contrary to the description, encrypted linkage values shall be applied as			

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			described in Modifications to Crypto Primitives v0.2-2015-08-18.			
SCMS-881	In Implementation	Extract linkage value and PCA ID	MA shall extract linkage value and PCA's ID from the considered certificate and then send the request to that PCA	MA needs to recover the input values and further information from the considered certificate.R		MA
SCMS-884	In Implementation	Error code: pcaNumberOfLinkageValuesExceeded	If more than the threshold number of linkage values are input, PCA shall provide this error code.	If upper performance limit is exceeded.		PCA
SCMS	In Impleme	Performance	The SCMS	There must be		LA, PCA,

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
- 921	ntation		component shall respond with the correct response or an error message in time to support system throughput requirements	a defined time-out.		RA
SCMS - 923	In Implementation	Error code: maRequestTimeout	MA shall log this timeout error, if the RA, PCA or LA does not respond within the defined threshold time	to enable server side error handling and for diagnosis purposes MA should log this error.		MA
SCMS - 930	In Implementation	Log	APDU requests and responses shall be stored for a configurable amount of time	To allow proper auditing.		LA, MA, PCA, RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			in an encrypted database.			
SCMS-931	In Implementation	Log: POC	For POC, at least 10,000 APDU requests and 10,000 responses shall be stored in an encrypted database.	To allow proper auditing.		LA, MA, PCA, RA

17 issues

2.4.8.3.6.3 ASN.1 Specification

- **ma-pca.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/ma-pca.asn?at=refs/heads/master
- **`ma-pca-errors.asn`** `https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/ma-pca-errors.asn?at=refs/heads/master`

2.4.8.3.7 Step 8.2.2: LA - MA: encrypted pre-linkage value -> LinkageInformation

Target release	Release 1.0
JIRA Task	SCMS-495-Finish document "LA - MA: pre-linkage value -> LinkageInformation"In Review
Document owner	Andre Weimerskirch
Reviewer	

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

QA	

2.4.8.3.7.1 Assumptions

- There is a mechanism in place that allows MA to prove that MA is authorized to request this information. For the purpose of POC, this is a digital signature.

2.4.8.3.7.2 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-407	In Implementation	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 a OCSP service at the technical component of the SCMS manager shall be deployed for revocation. See SCMS-406 for information about the cipher suite, SCMS-1016 for information about OCSP, and https://jira.campllc.org/browse/SCMS-938~~SCMS-938~~ for TLS certificate management.	CRL Store, CRLG, DCM, ECA, IBLM, LA, MA, PCA, PG, RA
SCMS-789	In Implementation	Error code: internalTimeout	LA, PCA, RA shall return and log this error code, if there is an internal timeout within the component such that it cannot correctly process the	to enable server side error handling.		LA, PCA, RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			request in time but can still respond to the MA.			
SCMS-791	In Implementation	Verify MA request authorization	LA, PCA and RA shall verify the MA requests in terms of authorization. If the verification fails, it shall return an error to MA and add an entry to its error log. Otherwise it shall start its computation.	LA, PCA, RA only accepts requests from MA that use a valid format and that are authorized. The authorization process is done by signature.	There is a set (sequence) of countersignatures per request. These countersignatures are provided by some trusted authority, and only if the signatures verify successfully, the the command will be executed. It's a policy decision which authorities need to sign the requests. For instance, it could be as simple as MA, or as difficult as some real-world legal entity (e.g. NHTSA).	LA, PCA, RA
SCMS-792	In Implementation	Error code: noMaAuthorizationSignature	LA, PCA and RA shall return this error code and add an error entry to its log file, if a request from the MA does not have a	to enable server side error handling.	LA, PCA and RA only accept requests that use a valid format and that are authorized. The authorization process is done by signature.	LA, PCA, RA

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			signature.			
SCMS-793	In Implementation	Error code: invalidMaAuthorizationSignature	PCA shall return this error code and add an error entry to its log file, if the MA authorization signature is invalid.	to enable server side error handling.	PCA only accepts requests that use a valid format and that are authorized. The authorization process is done by signature	PCA
SCMS-891	In Implementation	Validation	LA shall validate the input. If the validation fails, LA shall return an error to MA. Otherwise LA shall starts its computation.	LA only accepts properly formatted requests with a valid value.		LA
SCMS-892	In Implementation	Error code: laInvalidInputValueFormat	LA shall return and log this error code, if the input values are improperly formatted.	to enable server side error handling.		LA
SCMS-893	In Implementation	Error code: laInvalidPrelinkageValuePresented	If an invalid encrypted pre-	To enable error handlin		LA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			linkage value is input, LA shall provide this error code	g.		
SCMS-897	In Implementation	LA return linkageInformation	LA shall provide an interface to return an array of linkageInformation values given an array of encrypted pre-linkage values as detailed in MA → LA_ MA requests linkage information from LA (Misbehavior Detection) (request) and LA → MA_ LA replies with linkage information (Misbehavior Detection)	Ensure correctness.	LinkageInformation is described at LA → MA_ LA replies with linkage information (Misbehavior Detection).	LA, MA

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			(response). Contrary to the description, encrypted linkage values shall be applied as described in Modifications to Crypto Primitives v0.2-2015-08-18.			
SCMS-898	In Implementation	LA encrypted pre-linkage value request limit	LA shall be able to process a request input of up to a configurable amount of encrypted pre-linkage values	Set a maximum value to allow proper sizing of IT.		LA
SCMS-899	In Implementation	Request limit: POC	For POC, LA shall be able to process a request of up to 10,000 linkage values.	Set a maximum value to allow proper sizing of IT.		LA
SCMS	In Impleme	Error code: laNumberOfLinkage	If more than the	To enable		LA

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
-900	ntation	ValuesExceeded	threshold number of linkage values are input, LA shall provide this error code.	error handling.		
SCMS-901	In Implementation	Derive pre-linkage value	MA shall derive the proper encrypted pre-linkage values from the function call 8.2.1 MA-PCA: linkage value -> pre-linkage value, LA's host name	MA needs to recover the input values and further information from a previous service request.		MA
SCMS-921	In Implementation	Performance	The SCMS component shall respond with the correct response or an error message in time to support system throughput requireme	There must be a defined time-out.		LA, PCA, RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			nts			
SCMS-923	In Implementation	Error code: maRequestTimeout	MA shall log this timeout error, if the RA, PCA or LA does not respond within the defined threshold time	to enable server side error handling and for diagnosis purposes MA should log this error.		MA
SCMS-930	In Implementation	Log	APDU requests and responses shall be stored for a configurable amount of time in an encrypted database.	To allow proper auditing.		LA, MA, PCA, RA
SCMS-931	In Implementation	Log: POC	For POC, at least 10,000 APDU requests and 10,000 responses shall be stored in an encrypted	To allow proper auditing.		LA, MA, PCA, RA

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			database .			

17 issues

2.4.8.3.7.3 ASN.1 Specification

- **la-ma.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/la-ma.asn?at=refs/heads/master
- **`la-ma-errors.asn`** `https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/la-ma-errors.asn?at=refs/heads/master`

2.4.8.4 Step 8.3: OBE Revocation (CRL, blacklist)

Target release	Release 1.0
JIRA Task	SCMS-143-Finish document "OBE Revocation (CRL, blacklist)"In Review
Document owner	Andre Weimerskirch
Reviewer	Jeff Hahn
QA	Erik Schetina

2.4.8.4.1 Goals

- The OBE Revocation is a set of functions to revoke an EE after Misbehavior Analysis determined that EE shall be revoked. The main output is
    - Blacklist EE in RA
    - Determine linkage seeds from LA1 and LA2 so that it can be added to the CRL

2.4.8.4.2 Assumptions

Overall Assumptions and Requirements, if any, are provided below. Specific Assumptions and Requirements, if any, are provided in the sub-sections 8.3.1 MA-PCA: linkage value -> hash of RA-PCA request, RA's host name, 8.3.2 MA-RA: hash of RA-PCA request -> blacklist entry, 8.3.3 MA-RA: hash of RA-PCA request -> LCI1/2, LA1/2's hostname, group, 8.3.4 LA-MA: LCI -> linkage seed.

2.4.8.4.3 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-747	Review	Group Revocation: group linkage seeds	LA shall offer a web-based user interface that outputs	No automatic interfaces are offered		LA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			the currently valid group linkage seed after input of a groupIdentifier.	for group revocation.		
SCMS-852	Review	Group Revocation: MA user interface	The web-based user interface offered by MA for group revocation shall only be accessible to a dedicated local user "group revocation" on MA.	User access control		MA
SCMS-853	Review	Group Revocation: LA user interface	The web-based user interface offered by LA for group revocation shall only be accessible to a dedicated local user "group revocation" on LA.	User access control		MA
SCMS-854	Review	Group Revocation: groupIdentifier Look-Up	MA shall offer a web-based user interface that outputs the groupIdentifier after input of	No automatic interfaces are offered for group revocation.		MA

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			a certificate.			
SCMS-855	Review	Group Revocation: add to CRL	MA shall offer a web-based user interface that adds a group to the CRL after input of the group linkage seeds.	No automatic interfaces are offered for group revocation.		MA
SCMS-856	Review	Group Revocation: remove entry from CRL	The MA shall offer a web-based user interface that removes a group entry from the CRL after input of the currently valid corresponding group linkage seed.	No automatic interfaces are offered for group revocation.	Note that this is for PoC testing only but not a feature for a production SCMS.	MA
SCMS-857	In Implementation	Linkage seeds to CRL Generator	MA shall provide the linkage seeds of revoked EEs to the CRL Generator.	After an EE has been revoked, MA needs to provide the linkage seeds to its internal sub-component CRL Generator.	CRL Generator is a sub-component of MA. Therefore this is an internal function within MA and no explicit interface has been defined.	MA
SCMS	In	CRL	The CRL	An	Nice to	MA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
-858	Implementation	Generator Update of Revoked Linkage Values	generator shall be capable of updating the linkage seeds that are used on the CRL to reflect the current time period by hashing the linkage seeds before signing the updated CRL. The EEs then save the hashing of linkage seeds to reflect the current time period, but EEs receive the linkage seeds as part of the CRL that reflects the current time period.	optimization to save the OBEs effort when checking other OBEs against CRLs.	have only.	
SCMS-921	In Implementation	Performance	The SCMS component shall respond with the correct response or an error message in time to support system throughput requirements	There must be a defined time-out.		LA, PCA, RA

9 issues

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

2.4.8.4.4 Design

OBE Revocation

OBE Revocation comprises four functions that are listed below.

The natural flow is that MA will (1) map a linkage value to the "hash of RA-PCA request" and RA's hostname using PCA, (2) ask RA with the "hash of RA-PCA request" to add EE to RA's blacklist, (3) query RA with the "hash of RA-PCA request" to learn LCI1/2, LA1/2's hostname, and EE's group ID (if available), and (4) query LA1/2 to map LCI1/2 to linkage seed 1/2.

Note that interface functions allow for batch handling, i.e., rather than a single value typically an array of values is input and returned. For ease of explanation, the basic case is explained below.

1. MA - PCA: Maps a linkage values to a "hash of RA-PCA request" and RA's host name.
    a. MA → PCA_ MA requests Hash(PCReqRA) values from PCA (Revocation)
    b. PCA → MA_ PCA replies to Hash(PCReqRA) Request (Revocation)
2. MA - RA: Inputs the "hash of RA-PCA request" and asks RA to add corresponding enrollment certificate to RA's internal blacklist.
    a. MA → RA_ MA instructs RA to add entry to blacklist (Revocation)
    b. RA → MA_ RA replies to MA blacklisting instruction (Revocation)
3. MA - RA: Maps the "hash of RA-PCA request" to LCI1/2, LA1/2's host name, and EE's groupIdentifier
    a. MA → RA_ MA requests linkage chain identifiers from RA (Revocation)
    b. RA → MA_ RA replies to linkage chain identifier request (Revocation)
4. LA - MA: Maps LCI1/2 to linkage seed 1/2
    a. MA → LA_ MA requests linkage seed from LA (Revocation)
    b. LA → MA_ LA replies with linkage seed (Revocation)
5. MA - CRL Generator:
    a. MA provides the linkage seeds to CRL Generator.
    b. CRL Generator adds linkage seeds to CRL

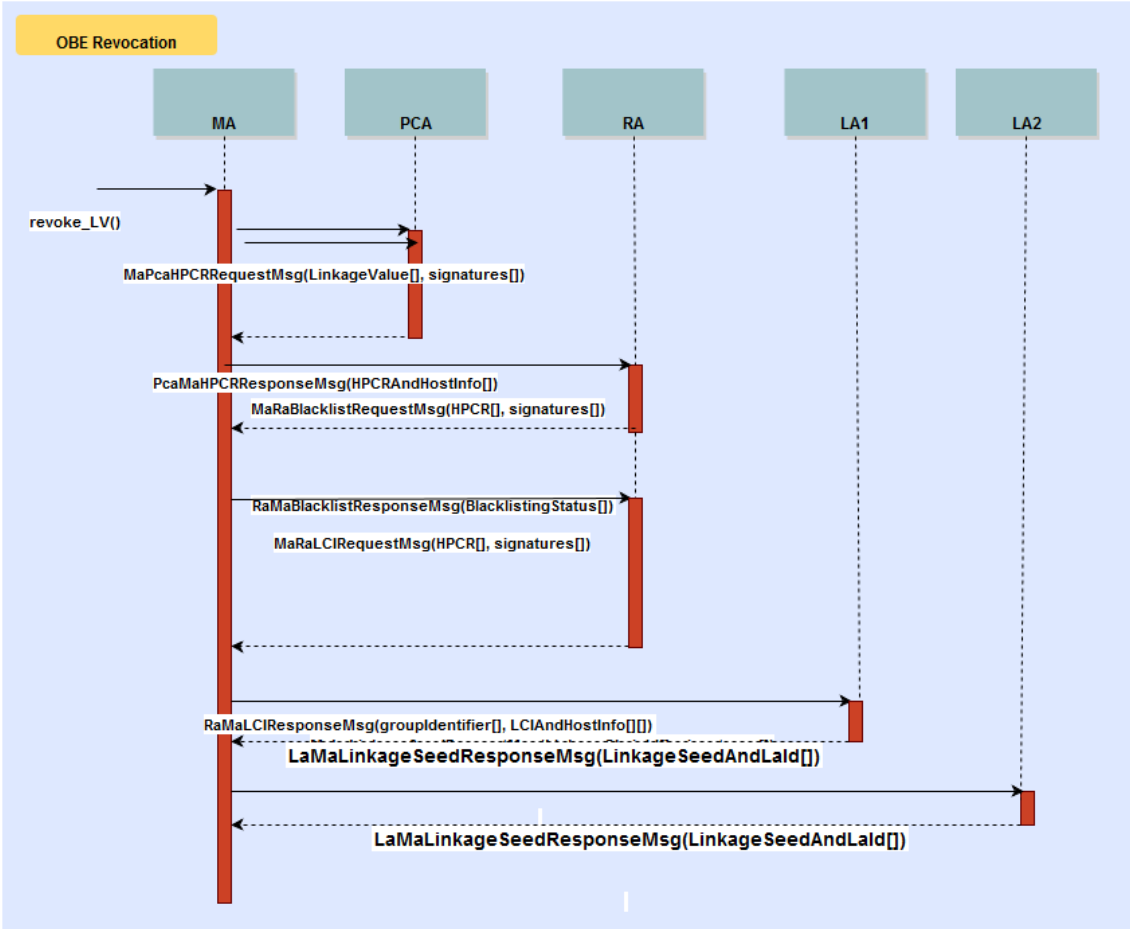
2.4.8.4.5 Group Revocation

Note that group revocation is planned as a manual process to avoid faulty group revocation, and there is no automated function available nor are there component interfaces defined.

RA defines a groupIdentifier and provides it to LA when group linkage chains are generated. This is described in http://wiki.campllc.org/display/SP/Group+Linkage+Values+-+SCMS+Paper (note that it's called "group chain identifier" and "index k" in that document). Later RA provides the groupIdentifier to MA after an EE is revoked. This is done in Step 3 above. MA uses this information to investigate whether any group is particularly susceptible to revocation. Note that groupIdentifier does not appear in certificates, it's only a "virtual" identifier used by RA, LA and MA.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT



To revoke, MA provides the groupIdentifier to LA1 and LA2 which then provide the corresponding group linkage seed. Those are then added to the CRL.

2.4.8.4.6 ASN.1 Specification

- **ma-pca.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/ma-pca.asn?at=refs/heads/master
- **ma-pca-errors.asn** master SCMS/scms-asnhttps://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/ma-pca-errors.asn?at=refs/heads/master
- **ma-ra.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/ma-ra.asn?at=refs/heads/master
- **ma-ra-errors.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/ma-ra-errors.asn?at=refs/heads/master
- **la-ma.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/la-ma.asn?at=refs/heads/master
- **la-ma-errors.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/la-ma-errors.asn?at=refs/heads/master

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

2.4.8.4.7 Step 8.3.1: MA-PCA: linkage value -> hash of RA-PCA request, RA's host name

Target release	Release 1.0
JIRA Task	SCMS-496-Finish document "MA-PCA: linkage value -> hash of RA-PCA request , RA's host name"In Review
Document owner	Andre Weimerskirch
Reviewer	
QA	

2.4.8.4.7.1 Assumptions

- There is a mechanism in place that allows MA to prove that MA is authorized to request this information. For the purpose of POC, this is a digital signature.

2.4.8.4.7.2 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-407	In Implementation	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 a OCSP service at the technical component of the SCMS manager shall be deployed for revocation. See SCMS-406 for information about the cipher suite, SCMS-1016 for information about OCSP, and https://jira.campllc.org/browse/SCMS-938~~SCMS-938~~ for TLS certificate management.	CRL Store, CRLG, DCM, ECA, IBLM, LA, MA, PCA, PG, RA
SCMS	In Implem	Error code: internalTimeout	LA, PCA, RA shall	to enable		LA, PCA,

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
-789	entation		return and log this error code, if there is an internal timeout within the component such that it cannot correctly process the request in time but can still respond to the MA.	server side error handling.		RA
SCMS-791	In Implementation	Verify MA request authorization	LA, PCA and RA shall verify the MA requests in terms of authorization. If the verification fails, it shall return an error to MA and add an entry to its error log. Otherwise it shall start its computation.	LA, PCA, RA only accepts requests from MA that use a valid format and that are authorized. The authorization process is done by signature.	There is a set (sequence) of countersignatures per request. These countersignatures are provided by some trusted authority, and only if the signatures verify successfully, the the command will be executed. It's a policy decision which authorities need to sign the requests. For instance, it could be as simple as MA, or as difficult as some real-world legal entity (e.g. NHTSA).	LA, PCA, RA
SCMS-792	In Implementation	Error code: noMaAuthorizationSignature	LA, PCA and RA shall return this error code and add an	to enable server side error	LA, PCA and RA only accept requests that use a valid format and that are authorized. The	LA, PCA, RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			error entry to its log file, if a request from the MA does not have a signature.	handling.	authorization process is done by signature.	
SCMS-793	In Implementation	Error code: invalidMaAuthorizationSignature	PCA shall return this error code and add an error entry to its log file, if the MA authorization signature is invalid.	to enable server side error handling.	PCA only accepts requests that use a valid format and that are authorized. The authorization process is done by signature	PCA
SCMS-795	In Implementation	Error code: pcaInvalidInputValueFormat	If the input values are improperly formatted, PCA shall provide this error code	to enable server side error handling.		PCA
SCMS-796	In Implementation	Error code: pcaInvalidLinkageValue	If an invalid linkage value is input, PCA shall provide this error code	to enable server side error handling.		PCA
SCMS-800	In Implementation	PCA return "hash of RA-PCA certificate request"	PCA shall provide an interface to return an array of "hash of RA-PCA request" values given	To support MA processes to get corresponding enrollm		PCA

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			an array of linkage values as detailed in MA → PCA_ MA requests Hash(PCReq RA) values from PCA (Revocation) (request) and PCA → MA_ PCA replies to Hash(PCReq RA) Request (Revocation) (response).	ent certificates		
SCMS-801	In Implementation	Extract linkage value and PCA ID	MA shall extract linkage value and PCA's ID from the considered certificate and then send the request to that PCA	MA needs to recover the input values and further information from the considered certificate.		MA
SCMS-802	In Implementation	PCA linkage value request limit	PCA shall be able to process a request input of up to a configurable amount of	Set a maximum value to allow proper sizing		PCA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			linkage values	of IT.		
SCMS-803	In Implementation	Request limit: POC	For POC, PCA shall be able to process a request of up to 10,000 linkage values.	upper performance limit		PCA
SCMS-804	In Implementation	Error code: pcaNumberOfLinkageValuesExceeded	If more than the threshold number of linkage values are input, PCA shall provide this error code.	For error handling.		PCA
SCMS-874	In Implementation	Validation	PCA shall validate the input. If the validation fails, PCA shall return an error to MA. Otherwise PCA shall starts its computation.	PCA only accepts properly formatted requests with a valid value.		PCA
SCMS-923	In Implementation	Error code: maRequestTimeout	MA shall log this timeout error, if the RA, PCA or LA does not respond within the defined threshold	to enable server side error handling and for diagnos		MA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			time	is purposes MA should log this error.		
SCMS-930	In Implementation	Log	APDU requests and responses shall be stored for a configurable amount of time in an encrypted database.	To allow proper auditing.		LA, MA, PCA, RA
SCMS-931	In Implementation	Log: POC	For POC, at least 10,000 APDU requests and 10,000 responses shall be stored in an encrypted database .	To allow proper auditing.		LA, MA, PCA, RA

16 issues

2.4.8.4.8 Step 8.3.2: MA-RA: hash of RA-PCA request -> blacklist entry

Target release	Release 1.0
JIRA Task	SCMS-497-Finish document "MA-RA: hash of RA-PCA request -> blacklist entry"In Review
Document owner	Andre Weimerskirch
Reviewer	
QA	

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

2.4.8.4.8.1 Assumptions

- There is a mechanism in place that allows MA to prove that MA is authorized to request this information. For the purpose of POC, this is a digital signature.

2.4.8.4.8.2 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-407	In Implementation	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 a OCSP service at the technical component of the SCMS manager shall be deployed for revocation. See SCMS-406 for information about the cipher suite, SCMS-1016 for information about OCSP, and https://jira.campllc.org/browse/SCMS-938~~SCMS-938~~ for TLS certificate management.	CRL Store, CRLG, DCM, ECA, IBLM, LA, MA, PCA, PG, RA
SCMS-789	In Implementation	Error code: internalTimeout	LA, PCA, RA shall return and log this error code, if there is an	to enable server side error handling.		LA, PCA, RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			internal timeout within the component such that it cannot correctly process the request in time but can still respond to the MA.			
SCMS-791	In Implementation	Verify MA request authorization	LA, PCA and RA shall verify the MA requests in terms of authorization. If the verification fails, it shall return an error to MA and add an entry to its	LA, PCA, RA only accepts requests from MA that use a valid format and that are authorized. The authorization process is done by	There is a set (sequence) of countersignatures per request. These countersignatures are provided by some trusted authority, and only if the signatures verify successfully, the the command will be executed. It's a policy decision which authorities need to sign the requests. For instance, it could be as simple as MA, or as difficult as some real-world legal entity (e.g. NHTSA).	LA, PCA, RA

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			error log. Otherwise it shall start its computation.	signature.		
SCMS-792	In Implementation	Error code: noMaAuthorizationSignature	LA, PCA and RA shall return this error code and add an error entry to its log file, if a request from the MA does not have a signature.	to enable server side error handling.	LA, PCA and RA only accept requests that use a valid format and that are authorized. The authorization process is done by signature.	LA, PCA, RA
SCMS-793	In Implementation	Error code: invalidMaAuthorizationSignature	PCA shall return this error code and add an error entry to its log file, if the MA	to enable server side error handling.	PCA only accepts requests that use a valid format and that are authorized. The authorization process is done by signature	PCA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Components
			authorization signature is invalid.			
SCMS-812	In Implementation	Error code: raInvalidHashRequest	If an invalid "hash of RA-PCA request" is input, RA shall return this error code to MA	For error handling		RA
SCMS-816	Implemented	Remove Blacklist Entry: POC	There shall be a feature to remove a blacklist entry manually.	If an EE is revoked, there needs to be a mechanism to remove the blacklist entry, e.g. for testing purposes. Blacklist entries are on the	This is only for POC. It needs to be reconsidered later whether this feature can stay or should be removed.	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				level of enrollment certificates. This needs to be considered on the level of certificate types though, i.e., for pseudonym certificates, OBE identification certificates, and RSE application certificates.		
SCMS-817	Implemented	RA add to blacklist	RA shall provide an interface that upon input of an array	To support MA processes of revoking OBE certificates by	The details are described in https://wiki.campllc.org/pages/viewpage.action?pageId=1081819 and https://wiki.campllc.org/pages/viewpage.action?pageId=1081820	RA

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Components
			of "hash of RA-PCA request" values adds the corresponding enrollment certificates to RA's internal blacklist.	avoiding an OBE to get new pseudonym certificates with its current enrollment certificate.		
SCMS-818	In Implementation	RA hash RA-PCA request values request limit	RA shall be able to process a request input of up to a configurable amount of "hash of RA-PCA request" values	Set a maximum value to allow proper sizing of IT.		RA
SCMS-820	In Implementation	Error code: raNumberOfRequestsExceeded	RA shall return this error code, if more	to enable server side error handlin		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			than the threshold number of linkage values are input.	g.		
SCMS-919	In Implementation	Request limit: POC	For POC, RA shall be able to process a request of up to 10,000 request identifier field (RIF) values.	For performance reasons. This upper performance limit is used in POC.		RA
SCMS-921	In Implementation	Performance	The SCMS component shall respond with the correct response or an error message in time to support system through	There must be a defined time-out.		LA, PCA, RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			put requirements			
SCMS-923	In Implementation	Error code: maRequestTimeout	MA shall log this timeout error, if the RA, PCA or LA does not respond within the defined threshold time	to enable server side error handling and for diagnosis purposes MA should log this error.		MA
SCMS-927	In Implementation	Validation	RA shall validate the input. If the validation fails, RA shall return an error to MA. Otherwise RA shall starts its computation.	RA only accepts properly formatted requests with a valid value.		RA
SCMS	In Implem	Log	APDU requests	To allow		LA, MA,

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
-930	entation		and responses shall be stored for a configurable amount of time in an encrypted database.	proper auditing.		PCA, RA
SCMS-931	In Implementation	Log: POC	For POC, at least 10,000 APDU requests and 10,000 responses shall be stored in an encrypted database .	To allow proper auditing.		LA, MA, PCA, RA

16 issues

2.4.8.4.9 Step 8.3.3: MA-RA: hash of RA-PCA request -> LCI1/2, LA1/2's hostname, groupIdentifier

Target release	Release 1.0

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

JIRA Task	SCMS-498-Finish document "MA-RA: hash of RA-PCA request -> LCI1/2, LA1/2's hostname, groupIdentifier"In Review
Document owner	Andre Weimerskirch
Reviewer	
QA	

2.4.8.4.9.1 Assumptions

- There is a mechanism in place that allows MA to prove that MA is authorized to request this information. For the purpose of POC, this is a digital signature.

2.4.8.4.9.2 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-407	In Implementation	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 a OCSP service at the technical component of the SCMS manager shall be deployed for revocation. See SCMS-406 for information about the cipher suite, SCMS-1016 for information about OCSP, and https://jira.campllc.org/browse/SCMS-938~~SCMS-938~~ for TLS certificate management.	CRL Store, CRLG, DCM, ECA, IBLM, LA, MA, PCA, PG, RA
SCMS-789	In Implementation	Error code: internalTimeout	LA, PCA, RA shall return and log this error code, if	to enable server side error handling.		LA, PCA, RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			there is an internal timeout within the component such that it cannot correctly process the request in time but can still respond to the MA.			
SCMS-791	In Implementation	Verify MA request authorization	LA, PCA and RA shall verify the MA requests in terms of authorization. If the verification fails, it shall return an error to MA and add an entry to its error log. Otherwise it shall	LA, PCA, RA only accepts requests from MA that use a valid format and that are authorized. The authorization process is done by signature.	There is a set (sequence) of countersignatures per request. These countersignatures are provided by some trusted authority, and only if the signatures verify successfully, the the command will be executed. It's a policy decision which authorities need to sign the requests. For instance, it could be as simple as MA, or as difficult as some real-world legal entity (e.g. NHTSA).	LA, PCA, RA

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			start its computation.			
SCMS-792	In Implementation	Error code: noMaAuthorizationSignature	LA, PCA and RA shall return this error code and add an error entry to its log file, if a request from the MA does not have a signature.	to enable server side error handling.	LA, PCA and RA only accept requests that use a valid format and that are authorized. The authorization process is done by signature.	LA, PCA, RA
SCMS-793	In Implementation	Error code: invalidMaAuthorizationSignature	PCA shall return this error code and add an error entry to its log file, if the MA authorization signature is invalid.	to enable server side error handling.	PCA only accepts requests that use a valid format and that are authorized. The authorization process is done by signature	PCA
SCMS-820	In Implementation	Error code: raNumberOfRequestsExceeded	RA shall return this error code, if more	to enable server side error		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			than the threshold number of linkage values are input.	handling.		
SCMS-829	In Implementation	Error code: raInvalidLinkageValue	If an invalid linkage value is input, RA shall provide this error code	For error handling		RA
SCMS-833	In Implementation	RA return linkage chain identifiers	RA shall provide an interface to return an array of linkage chain identifiers (one per LA), linkage authority hostname (one per LA), and groupIdentifiers for a given array of certificate request hash values as	To support MA processes to put OBE's current pseudonym certificates on the CRL by granting the MA the feasibility to get the required linkage seeds.		RA

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			detailed in MA → RA_ MA requests linkage chain identifiers from RA (Revocation) (request) and RA → MA_ RA replies to linkage chain identifier request (Revocation) (response).			
SCMS-910	In Implementation	Error code: raInvalidInputValueFormat	RA shall return this error code and add an error entry to its log file, if the input values are improperly formatted.	to enable server side error handling.		RA
SCMS-	In Impleme	Request limit: POC	For POC, RA shall	For perform		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
919	ntation		be able to process a request of up to 10,000 request identifier field (RIF) values.	ance reasons. This upper performance limit is used in POC.		
SCMS-921	In Implementation	Performance	The SCMS component shall respond with the correct response or an error message in time to support system throughput requirements	There must be a defined time-out.		LA, PCA, RA
SCMS-923	In Implementation	Error code: maRequestTimeout	MA shall log this timeout error, if the RA, PCA or LA does not respond within the defined threshold	to enable server side error handling and for diagnosis purposes MA should log this		MA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			time	error.		
SCMS-927	In Implementation	Validation	RA shall validate the input. If the validation fails, RA shall return an error to MA. Otherwise RA shall starts its computation.	RA only accepts properly formatted requests with a valid value.		RA
SCMS-930	In Implementation	Log	APDU requests and responses shall be stored for a configurable amount of time in an encrypted database.	To allow proper auditing.		LA, MA, PCA, RA
SCMS-931	In Implementation	Log: POC	For POC, at least 10,000 APDU requests and 10,000 responses shall be	To allow proper auditing.		LA, MA, PCA, RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			stored in an encrypted database.			

15 issues

2.4.8.4.10 Step 8.3.4: LA-MA: LCI -> linkage seed

Target release	Release 1.0
JIRA Task	SCMS-499-Finish document "LA-MA: LCI -> linkage seed"In Review
Document owner	Andre Weimerskirch
Reviewer	
QA	

2.4.8.4.10.1 Assumptions

- There is a mechanism in place that allows MA to prove that MA is authorized to request this information. For the purpose of POC, this is a digital signature.

2.4.8.4.10.2 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-407	In Implementation	TLS Mutual Authentication	Communication transactions between SCMS components shall be client-server mutually authenticated and encrypte	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 a OCSP service at the technical component of the SCMS manager shall be deployed for revocation. See SCMS-406 for information about the cipher suite, SCMS-	CRL Store, CRLG, DCM, ECA, IBLM, LA, MA, PCA, PG, RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			d with TLS (except EE-RA).		1016 for information about OCSP, and https://jira.campllc.org/browse/SCMS-938~~SCMS-938~~ for TLS certificate management.	
SCMS-789	In Implementation	Error code: internalTimeout	LA, PCA, RA shall return and log this error code, if there is an internal timeout within the component such that it cannot correctly process the request in time but can still respond to the MA.	to enable server side error handling.		LA, PCA, RA
SCMS-791	In Implementation	Verify MA request authorization	LA, PCA and RA shall verify the MA requests in terms of authoriza	LA, PCA, RA only accepts requests from MA that use a valid	There is a set (sequence) of countersignatures per request. These countersignatures are provided by some trusted authority, and only if the signatures verify successfully, the	LA, PCA, RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			tion. If the verification fails, it shall return an error to MA and add an entry to its error log. Otherwise it shall start its computation.	format and that are authorized. The authorization process is done by signature.	the command will be executed. It's a policy decision which authorities need to sign the requests. For instance, it could be as simple as MA, or as difficult as some real-world legal entity (e.g. NHTSA).	
SCMS-792	In Implementation	Error code: noMaAuthorizationSignature	LA, PCA and RA shall return this error code and add an error entry to its log file, if a request from the MA does not have a signature.	to enable server side error handling.	LA, PCA and RA only accept requests that use a valid format and that are authorized. The authorization process is done by signature.	LA, PCA, RA
SCMS-793	In Implementation	Error code: invalidMaAuthorizationSignature	PCA shall return this error code and add an error entry to	to enable server side error handling.	PCA only accepts requests that use a valid format and that are authorized. The authorization process is done by signature	PCA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			its log file, if the MA authorization signature is invalid.			
SCMS-844	In Implementation	Error code: laInvalidLinkageValue	If an invalid linkage chain identifier (LCI) is input, LA shall provide this error code	For error handling.		LA
SCMS-848	In Implementation	LA return linkage seed	LA shall provide an interface to return an array of corresponding linkage seeds to a given array of linkage chain identifiers as detailed in MA → LA_ MA requests linkage seed	To support MA processes to put OBE's current pseudonym certificates on the CRL.		LA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			from LA (Revocation) (request) and LA → MA_LA replies with linkage seed (Revocation) (response).			
SCMS-849	In Implementation	LA LCI values request limit	LA shall be able to process a request input of up to a configurable amount of LCI values	Set a maximum value to allow proper sizing of IT.		LA
SCMS-851	In Implementation	Error code: laNumberOfLciValuesExceeded	If more than the threshold number of LCI values are input, LA shall provide this error code.	For error handling.		LA
SCMS-891	In Implementation	Validation	LA shall validate the input. If the	LA only accepts properly formatte		LA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			validation fails, LA shall return an error to MA. Otherwise LA shall starts its computation.	d requests with a valid value.		
SCMS-892	In Implementation	Error code: laInvalidInputValueFormat	LA shall return and log this error code, if the input values are improperly formatted.	to enable server side error handling.		LA
SCMS-899	In Implementation	Request limit: POC	For POC, LA shall be able to process a request of up to 10,000 linkage values.	Set a maximum value to allow proper sizing of IT.		LA
SCMS-921	In Implementation	Performance	The SCMS component shall respond with the correct response	There must be a defined time-out.		LA, PCA, RA

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			or an error message in time to support system throughput requirements			
SCMS-923	In Implementation	Error code: maRequestTimeout	MA shall log this timeout error, if the RA, PCA or LA does not respond within the defined threshold time	to enable server side error handling and for diagnosis purposes MA should log this error.		MA
SCMS-930	In Implementation	Log	APDU requests and responses shall be stored for a configurable amount of time in an encrypted database.	To allow proper auditing.		LA, MA, PCA, RA
SCMS-	In Impleme	Log: POC	For POC, at least	To allow proper		LA, MA,

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
931	ntation		10,000 APDU requests and 10,000 responses shall be stored in an encrypted database.	auditing.		PCA, RA

16 issues

2.4.8.5 Step 8.4: OBE CRL Check

Target release	
JIRA Task	
Document owner	Andre Weimerskirch
Reviewer	
QA	

2.4.8.5.1 Goals

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

2.4.8.5.2 Assumptions

- The OBE received a CRL
- OBE checks all received BSMs against the CRL using the mechanism described in IEEE 1609.2-v3-D12, in the following clauses:
    - Clause 5.1.3.4
    - Clause 6.4.10 and 6.4.11
    - Clause 7

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

2.4.8.5.3 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1216	SCMS PoC out of Scope	OBE calculates linkage values	OBE shall calculate the currently valid linkage values for each CRL entry that describes a set of pseudonym certificates and store temporarily for further use.	Calculating the linkage values is a requirement to then check received BSMs against the list of all linkage values belonging to revoked OBEs.	The algorithm to calculate linkage values is described in Modifications to Crypto Primitives (see "Use of AES as a Derivation Function"). This is out of scope since it defines OBE's behavior.	On-board Equipment (OBE)
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	OBE updates linkage value list	OBE shall update the list of revoked	OBE is able to update the linkage values for each time period. It is left to the OEM/supplier, when the values	Linkage values are updated by hashing the	On-board Equipment (OBE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
	of Scope		linkage values for each time period (week). OBE shall either update the linkage value or remove the linkage value.	are updated. The updated values are needed when a new time period starts.	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	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 time 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 week of buffer.	This is out of scope since it defines OBE's behavior.	On-board Equipment (OBE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			(week).			
SCMS-1221	SCMS PoC out of Scope	OBE processes CRL	OBE 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 OBE must always update its stored CRL in a timely fashion.	This is out of scope since it defines OBE's behavior.	On-board Equipment (OBE)
SCMS-1222	SCMS PoC out of Scope	Removed CRL entry	OBE shall apply a missing CRL entry (from a previous CRL) for at least one more time period (week) if 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 OBE's behavior.	On-board Equipment (OBE)
SCMS-1223	SCMS PoC out of	OBE checks against CRL for other	EEs shall check all received sender certificate	EEs also checks against CRL for RSE and OBE identification certificates. These are checks based on the hash value of the sender's	These checks are specified in IEEE 1609.2.	On-board Equipment (OBE), Road-side Equipment

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
	Scope	certificate types	s against the most recent CRL. If the sender certificate is listed, OBE shall discard the received message.	certificate.	This is out of scope since it defines EE's behavior.	(RSE)
SCMS-1224	SCMS PoC out of Scope	OBE stops sending	OBE shall stop sending over-the-air DSRC messages, if it detects that it has been listed on the CRL.	If OBE has been revoked, it stops sending. OBE might still receive DSRC messages.	This is out of scope since it defines OBE's behavior.	On-board Equipment (OBE)
SCMS-1285	SCMS PoC out of Scope	OBE stops sending: revoked ECA for OBE's enrollment certificate	OBE shall stop sending over-the-air messages, if it detects (via CRL) that it's ECA, or any ICA between it's ECA and the Root CA, has been	In this case, OBE's enrollment certificate also has been revoked.	This is out of scope since it defines EE behavior.	On-board Equipment (OBE)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			revoked.			
SCMS-1286	SCMS PoC out of Scope	OBE stops sending: revoked PCA for OBE's pseudonym certificates	OBE shall stop using all pseudonym certificates issued by a certain PCA, if OBE detects (via CRL) that this PCA, or any ICA between PCA and Root CA, has been revoked.	If the PCA was revoked, all pseudonym certificates are also revoked.	This is out of scope since it defines EE behavior.	On-board Equipment (OBE)
SCMS-1302	SCMS PoC out of Scope	OBE check received BSMs against CRL	OBE shall check all received BSMs against the CRL using the mechanism described in IEEE 1609.2-v3-D12: • Clause 5.1.3.4 • Clause	This is to test whether SCMS issued a proper CRL for OBEs.	This is out of scope since it defines EE behavior.	On-board Equipment (OBE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			6.4.10 and 6.4.11 • Clause 7			

11 issues

2.4.9 Use Case 9: Refresh Pseudonym Certificates

Target release	Release 1.0
JIRA Task	SCMS-144-Finish document "Refresh Pseudonym Certificates"QA
Document owner	Roger Motz
Reviewer	
QA	

2.4.9.1 Goals

- The goal of refreshing the pseudonym certificates is ensure that the EE has a constant supply of certificates and related policy information. This is accomplished by periodically connecting to the RA to download policy updates and pseudonym certificates.
- See sub-sections for specific details.

2.4.9.2 Background and strategic fit

EEs are not assumed to have constant or frequent connection to the SCMS system. Therefore, certificates will be pre-generated and available to download for a significant amount of time into the future.

2.4.9.3 Assumptions

- The EE has successfully completed the enrollment process.
- The EE has the .info file from a previous download from the RA.

2.4.9.4 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	Messages from EEs to an RA must be	This is out of scope since it defines EE's behavior.	On-board Equipment

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			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.	secure against replay attacks. The signed time stamp from the EE enables the RA to validate the freshness of EE requests.		(OBE), Road-side Equipment (RSE)
SCMS-416	In Implementation	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-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-	Closed	RA download	RA shall provide	to utilize standard	Downloads could be e.g. policy file, Global	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
514		via HTTPS	downloads over HTTPS (TLS).	internet protocols for the download process.	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).	
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 certs currently. Instead the OBE will use TLS to authenticate the other endpoint (as a server) and will use its SCMS cert to identify itself. EE authenticates via its IEEE 1609.2 enrollment certificate. The details of the authentication process are defined Step 3.4: Download of Pseudonym Certificates	RA
SCMS-517	In Implementation	Tunneling through LOP	RA shall provide downloads only via a LOP hardware interface, which removes all location	to anonymize the location of EEs.		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			information from the incoming request.			
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 (adversary might extract Butterfly encryption keys from junked vehicle at a later stage and is then	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)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				able to identify all EE certificates).		
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 in Step 3.4: Download of Pseudonym	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				Certificates.		
SCMS-540	In Implementation	OCSP stapling - RA	The RA shall support OSCP stapled certificate response to OBE.	This is as a means to react to RA's revocation. In case the RA is compromised, and the DNS server is compromised or spoofed, then a revocation mechanism will prevent further damage.	OCSP stapling provides improved performance compared to CRLs. OCSP stapling is specified in RFC 6066, Section 8. 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). The RA will be able to respond to the OBE's request for an OSCP stapled certificate. The RA itself will be able to request OCSP certificate currency from an OCSP server in order that it (the RA) is assured of the other components TLS cert currency, so it will require the OCSP request URL and credentials.	RA
SCMS-541	SCMS PoC out of Scope	OCSP stapling - EE	The EE may use the TLS Certificate Status Request extension (OCSP stapling)	Revocation is optional and it's up to the OEMs support it.	This is out of scope since it specifies EE's behavior If EE does not support this feature, the following might happen: An adversary that extracted the RA's private key and that successfully spoofed	On-board Equipment (OBE), Road-side Equipme

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			to verify RA revocation status.		DNS is able to learn EE's enrollment certificate (but not EE's private key). OCSP stapling is specified in RFC 6066, Section 8.	nt (RSE)
SCMS-544	Closed	Download resume	RA shall support byte-wise resume of certificate batch, certificate file, or policy file, downloads, even if EE switches the IP address.	to improve reliability of the download protocol.		RA
SCMS-958	SCMS PoC out of Scope	Error code: eeConnectionFailed	EE shall log this error in its log file, 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 this error code, if EE requests invalid	to enable server side diagnostics and to avoid giving	This is not in ASN.1 but http 404	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			URL.	potential attackers relevant information		
SCMS-977	In Implementation	Error code: raNoTLS	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 this error, 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 store this error code in EE's error log file, 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 reporting: eeAuthenticationFailed	EE shall initiate a misbehavior report to MA with the	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			observed error, if RA-to-EE authentication fails.			side Equipment (RSE)
SCMS-1090	In Implementation	Error code: rseRaTcpErrors	RA shall return standard TCP error codes if TCP errors occur.	in order to enable client side error handling.		RA
SCMS-1196	SCMS PoC out of Scope	Stored .info file	OBE shall have a .info file stored from the previous connection to the RA.	The .info file is used to determine the next allowed connection attempt.	This is out of scope since it defines OBE's behavior.	On-board Equipment (OBE)
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 since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1203	Implemented	Check time stamp	RA shall check the signed (by EE) time-stamp and allow a tolerance of 5	If the difference between the signed time-stamp and the		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			seconds.	current time is 5 seconds or less, RA will proceed with the authentication process. Otherwise RA will reject the connection.		
SCMS-1204	Implemented	Check blacklist	RA shall reject EE request, if EE is listed on its blacklist.	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		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				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.		
SC	SCMS	EE download	EE shall	This will		On-

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
MS-1263	PoC out of Scope	resume	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.	improve reliability of the download process and reduce communication cost.		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)

24 issues

2.4.9.5 Step 9.1: Request updated policy(/ies)

Target release	Release 1.0
JIRA Task	SCMS-145-Finish document "Request updated policies"Closed
Document owner	Roger Motz

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Reviewer	
QA	

2.4.9.5.1 Goals

- The policy download mechanism is required to ensure that the OBE is always using the latest policy for new downloaded certificate batches. The ongoing download of the policy files is identical to the initial policy download process as described in Step 3.1: Check for policy updates from the SCMS point of view.

2.4.9.5.2 Background and strategic fit

From an EE point of view the download time is controlled by the .info file that was downloaded from the RA the previous time.

2.4.9.5.3 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-512	Closed	Global Policy file	RA shall always provide a global policy file available for download by EE	There is always a global configuration available, and that configuration shall be current		RA
SCMS-709	SCMS PoC out of Scope	Check for 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	• If no policy file is available on the EE, the EE is allowed to make a download attempt at any	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				Case 18: Create / provide global and local policies.	time. • This is out of scope since it defines EE's behavior.	
SCMS-767	SCMS PoC out of Scope	Check for Certificate Chain Updates	EE shall check for version changes in 'certChainFileId' field of the Global Policy file. If the version is different than that of its existing file, it will take action to update it.	As CAs are added, removed, revoked, or rolled-over, new certificate chains will have to propagated to EEs and other SCMS components. For more information: Global Certificate Chain File	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-952	SCMS PoC out of Scope	Error code: eeGlobalPolicyFileDownloadFailed	EE shall implement OEM defined error handling and store the error code in EE's error	As the global policy file is essential for the system to work	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			log file, if EE is not able to download the global policy file (e.g. because there is none or it's corrupted).	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.		
SCMS-953	SCMS PoC out of Scope	Misbehavior reporting: eeGlobalPolicyFileDownloadFailed	If EE is not able to download the global policy file (e.g. because there is none or it's corrupted), EE 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), Road-side Equipment (RSE)
SCMS-954	SCMS PoC out of Scope	Error code: eeGlobalPolicyVerificationFailed	EE shall implement OEM defined error handling and store this error code in EE's error	to enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			log file, if EE is not able to verify the digital signature of the global policy file.			
SCMS-955	SCMS PoC out of Scope	Misbehavior reporting: eeGlobalPolicyVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify the digital signature of the global 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: eeGlobalPolicyFileParsingFailed	EE shall implement OEM defined error handling and store this error code in EE's error log file, if EE is not able to parse the successfully downloaded global policy file (e.g. because it's corrupted).	As the global 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	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				not able to read the latest version of that file.		
SCMS-957	SCMS PoC out of Scope	Misbehavior reporting: eeGlobalPolicyFileParsingFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to parse the successfully downloaded global policy file (e.g. because it's 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-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 download a policy file If any component in the trust chain of the EE is revoked.	If the EE's ECA or other CA in the chain is revoked the EE shall not attempt to establish a connection to the RA. If an attempt is	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				made, it will be unable to authenticate to the RA.		
SCMS-1353	SCMS PoC out of Scope	EE gets LCCF from RA	EE shall check for and download policy an updated Local Certificate Chain File (LCCF) or Global Certificate Chain File (GCCF) 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 cert. This is out of scope since it defines EE's behavior	On-board Equipment (OBE), RA, Road-side Equipment (RSE)
SCMS-1356	SCMS PoC out of Scope	LCCF validation in EE	EE shall use the Local or Global Certificate Chain File (LCCF/GCCF) to validate received SCMS certificates and respond to P2P certificate	EEs need to be able to validate received SCMS certificates based on their certificate chain up to the SCMS Root CA. EEs need	EE doesn't need to store all certificate chains, the LCCF provides the minimum set and EEs can learn additional	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			requests.	to respond to P2P certificate requests to enable receiving EEs to validate the certificate chain.	chains via P2P certificate request. This is out of scope since it defines EE's behavior	

13 issues

2.4.9.5.4 User interaction and design

- Step 1: EE will use .info file from the last certificate batch download to determine the time a download can be attempted.
- Step 2: EE and RA authenticate to each other.
- Step 3: EE downloads the policy file.

2.4.9.6 Step 9.2: Download new Pseudonym Certificates

Target release	Release 1.0
JIRA Task	SCMS-146-Finish document "Download new Pseudonym Certificates"In Specification
Document owner	Roger Motz
Reviewer	Jeff Hahn
QA	

2.4.9.6.1 Goals

- See Step 3.4: Download of Pseudonym Certificates for full details of the batch download process. Differences from the 3.4 process 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 3.4: 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 EE point of view the process is slightly different than the process for initial provisioning.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

- See Step 3.5: 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 EE 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 EE reestablishes a connection. The new certificates will be available for download at the time specified in the .info file.

2.4.9.6.2 Background and strategic fit

- See Step 3.4: Download of Pseudonym Certificates for full details of the batch download process.
- See Step 3.5: Schedule generation of subsequent batch of Pseudonym Certificates for full details of the process to schedule certificate pre-generation.

2.4.9.6.3 Assumptions

- See Step 3.4: Download of Pseudonym Certificates for full details of the batch download process.
- See Step 3.5: Schedule generation of subsequent batch of Pseudonym Certificates for full details of the process to schedule certificate pre-generation.

2.4.9.6.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-508	SCMS PoC out of Scope	Stop pre-generating certificates for inactive device	RA shall stop pre-generating pseudonym /OBE identification certificates for a device that has not connected to RA for a given amount of time as specified by the SCMS Manager	So that computing resources are not wasted for inactive devices. If device has not connected	Stop/resume pre-generation is out of scope for PoC. Time is currently set to be 3 years. Based on the implementation, the LA may also stop pre-generating pre-linkage values.	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Components/s
				for a certain period of time, the assumption is the device is no longer available or in service.		
SCMS-509	Closed	Stop pre-generating pseudonym 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 for revoked devices		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Components/s
SCMS-534	Closed	Certificate Batch	RA shall store certificates to be downloaded by EE in a specific folder known to EE.	Certificate batch is the basis for receiving pseudonym certificates. The use-case objective is to transfer certificate batches from RA to EE.		RA
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		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Components/s
				files, to avoid that an EE needs to download all certificates each time. This also allows easier resume of a download.		
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_availa	This might change during the life-time of the SCMS. It might even vary for different EEs.		RA

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Components/s
			ble_cert_supply in the global policy.			
SCMS-548	Closed	X.info file	RA shall provide an .info file for download by EE.	The .info file provides information when new pseudonym certificates, or identification certificates, can be downloaded.	see Certificate Batch Download for more information.	RA
SCMS-549	Closed	Keep Certs	The RA shall allow the EE to download certificates that have previously been downloaded, so long as the devices	to recover from a loss of certificates at the device level		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			credentials are still valid and the certificates are not expired.	(e.g., disk corruption).		
SCMS-553	SCMS PoC out of Scope	Resume pre-generating certificates	RA shall resume pre-generation of pseudonym/OBE identification certificates if an OBE submits a new request after a silent period where RA had stopped pre-generating	If the OBE submits a valid request, it is a signal that the OBE is participating again regardless of the length of the silent period.	Stop/resume pre-generation is out of scope for PoC.	RA
SCMS-576	Implemented	Update .info file	The RA shall update .info files for all EEs even if no new certificate	The EE uses the .info file to determine	• Timestamp in .info file is dynamically calculated base on system load. Should there be a maximum? • PoC scope will be to update .info file for active EEs only.	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Components/s
			batches are created.	when the the earliest the next download is allowed to happen.		
SCMS-964	In Implementation	Error code: raNoCertFileAvailable	RA shall provide this error code to EE, if certificate batch is not available.	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's corrupted), OBE shall implement OEM defined error handling and store the error	to enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			code in OBE's error log file.			
SCMS-966	SCMS PoC out of Scope	Misbehavior reporting: 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's 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 implement OEM defined error handling and store the error code in EE's error log file, 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-96	SCMS PoC out of	Misbehavior reporting: eeCertFileVerifi	EE shall initiate a misbehavior report to	to enable server	This is out of scope since it defines EE's behavior.	On-board Equipment

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
8	Scope	cationFailed	MA with the observed error, if EE is not able to verify the digital signature of an encrypted certificate.	side misbehavior detection.		(OBE), Road-side Equipment (RSE)
SCMS-969	SCMS PoC out of Scope	Error code: eeCertificateFileDecryptionFailed	EE shall implement OEM defined error handling and store the error code in EE's error log file, 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 reporting: 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)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-971	SCMS PoC out of Scope	Error code: eeCertificateVerificationFailed	EE shall implement OEM defined error handling and store the error code in EE's error log file, 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 reporting: 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 implement OEM defined error handling and store the error code in EE's error log file, if EE is not able to parse a	to enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			certificate, or if the certificate has wrong content.			
SCMS-974	SCMS PoC out of Scope	Misbehavior reporting: 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-981	In Implementation	Error code: raNoPcaCertificateChainFileAvailable	RA shall return this error, if Global Certificate Chain File is not available.	to enable client side error handling.		RA
SCMS-982	Implemented	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		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Components/s
				updates to EE		
SCMS-983	In Implementation	Error code: raNoInfoFileAvailable	RA shall return this error code, if it is not able to provide a current .info file.	to enable EE side error handling.	This information is probably provided by an entry in the .info file	RA
SCMS-984	SCMS PoC out of Scope	Error code: eeInfoFileDownloadFailed	OBE shall implement OEM defined error handling and store the error code in its error log file, if OBE is not able to download the .info file (e.g. because there is none or it's 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 reporting: eeInfoFileDownloadFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able	to enable server side misbehavior detect	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Components/s
			to download the .info file (e.g. because there is none or it's corrupted).	ion.		
SCMS-1163	SCMS PoC out of Scope	OBE revoked	A revoked OBE shall not attempt to download pseudonym certificate batches/OBE identification certificate files.	Once an OBE detects that it has been revoked, it shall stop attempting to download more certificates.	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	This is out of scope since it defines EE's behavior. • If no pseudonym certificates are available on the OBE for the current i_period (week), the OBE is allowed to make a download attempt at any time. • If no pseudonym certificates are available on the OBE for the next i_period (week), the OBE is allowed to make a download attempt at any time.	On-board Equipment (OBE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Components/s
				(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.	• 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	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Components/s
				current time or in the future. Certificates that are already expired should not be downloaded.		
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	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				currently verified and stored on the device. This is to prevent repeated downloads of the same content.		
SCMS-1188	SCMS PoC out of Scope	Trust Chain Broken - OBE	OBE shall not attempt to download pseudonym certificate batches/OBE identification certificate files if any component in the trust chain of the OBE is revoked.	If the OBE's ECA or other CA in the chain is revoked the OBE shall not attempt to establish a	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Components/s
				connection to the RA. If an attempt is made, it will be unable to authenticate to the RA.		
SCMS-1214	SCMS PoC out of Scope	OBE downloads .info file	OBE shall download the .info file each time OBE tries to download pseudonym certificates.	The .info file lists the time when pseudonym certificates will be available next time. EE downloads that file each time	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Components/s
				it tries to download pseudonym certificates.		
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.	Whenever EE tries to download certificates, it also downloads the .info file. EE will contact RA again to download certificates after the time listed in the .info file.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Components/s
SCMS-1293	Review	Schedule pre-generation of OBE pseudonym and OBE identification certificates	RA shall schedule pre-generation of certificates to meet the availability requirements of certificate download defined by the SCMS Manager.	Certificate requests may vary. The SCMS must ensure that certificates are available before the current certificate expires.	For pseudonym certificates, the availability requirement is specified in http://wiki.campllc.org/display/SP/3.4.+Download+of+Pseudonym+Certificates. For identification certificates, a certificate for the next time period shall always be available.	RA

33 issues

2.4.9.6.5 Design

- Step 1: EE 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: EE and RA authenticate to each other.
- Step 3: EE downloads the Step 18.5: Generate Global and Local Certificate Chain File
    - 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: EE will download all or as many as possible, certificate files that it does not already have stored locally. It is the responsibility of the EE to determine which certificate batch files to download (i.e. skip files that have already been successfully downloaded and processed).

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

- Step 5: EE downloads the .info file (generated and updated by RA). The .info file contains the time when the next certificate batches will be available.

  See Step 3.4: Download of Pseudonym Certificates for full details of the batch download process.
  See Step 3.5: Schedule generation of subsequent batch of Pseudonym Certificates for full details of the process to schedule certificate pre-generation.

2.4.9.6.6 Questions

Below is a list of questions to be addressed as a result of this requirements document:

Question	Outcome
What to do if no certificates are available for download? This would be the case if a download (communication to the RA) has not been made for more than 6 years since initial provisioning (initial 3 years + 3 years of pre-generated certificates)? • Wait for next download attempt as specified by .info file? Should reduced shuffling be allowed to decrease wait time? • Alert driver immediately?	Decision to NOT implement in PoC. For PoC requirement, DB attribute will be added to schema to enable future inclusion of such a capability. Defined in Step 3.4: Download of Pseudonym Certificates

2.4.9.6.7 Not Doing

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

2.4.10 Use Case 10: Update Pseudonym Certificate Request Parameters

Target release	Release 1.0
JIRA Task	SCMS-148-Finish document "Update Pseudonym Certificate Request Parameters"In Review
Document owner	Virendra Kumar
Reviewer	
QA	

2.4.10.1 Goals

Provide a device (that has already been bootstrapped and provisioned with pseudonym certificates) with a mechanism to update certain parameters, such as butterfly keys and batch size, of the pseudonym certificate request.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

2.4.10.2 Background and strategic fit

From a device's (and LOP's) point of view, this use case is identical to Step 3.2: Request for Pseudonym Certificates. However, from the RA's point of view, there are some important differences from Step 3.2: Request for Pseudonym Certificates as follows.

- Based on the policies set by the SCMS Manager, RA must stop generating subsequent batches with old parameters within a certain time period from the time the device makes a request for updating the parameters.
- Based on the type of update, such as batch size update, RA may need to communicate to the LAs the necessary updates to the generation of pre-linkage values.
- Instead of a plain acknowledge (see bullet 2.1 under Design in Step 3.2: Request for Pseudonym Certificates), RA needs to respond back to the device if the update request was accepted or not, and also the time when the updates will take effect.

2.4.10.3 Assumptions

- Device is assumed to be bootstrapped.
- Device is assumed to be provisioned with pseudonym certificates at least once.

2.4.10.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-669	In Implementation	check-request	RA shall check if the requested change(s) in parameters are within the allowed range(s) as per policies by the SCMS Manager	so that pseudonym certificate provisioning parameters are not assigned values outside the allowed range		RA
SCMS-670	In Implementation	stop-generating	RA shall stop generating subsequent batches with old parameters within a certain time period (as specified by	so that updates take effect in a timely fashion	For POC, the time period was decided to be 3 years and 1 week	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			the SCMS Manager) from the time the device makes a request for updating the parameters			
SCMS-671	In Implementation	other-components	RA shall communicate to other SCMS components, such as LAs and PCA, if they need to update their processes	so that pseudonym certificate provisioning process works smoothly	There will be sub-requirements for each specific change, but that will worked out when the set of policy changes are finalized. Also, RA may need to provide evidence to LA/PCA when requesting change in parameters.	RA
SCMS-672	In Implementation	accept-reject	RA shall inform the device if an update request was accepted or not	so that the device is not in an undetermined state at any time		RA
SCMS-673	In Implementation	update-time	RA shall inform the device when a particular	so that the device can get updated pseudonym	This is somewhat related to SCMS-669,	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			update will take effect	certificates in a timely fashion	in that SCMS Manager can specify a range and RA can choose to enforce a fixed value.	
SCMS-1161	SCMS PoC out of Scope	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.	On-board Equipment (OBE)
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-1404	SCMS PoC out of Scope	EE send data via HTTP post	EE shall use HTTP post to send data	to allow the SCMS endpoint to	RA - Services View will	On-board Equipment (OBE),

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
		over TCP/IP	towards the RA	serve everything based on HTTP protocol	document the actual HTTP post details This is out of scope as it defines EE behavior.	Road-side Equipment (RSE)
SCMS-1405	Review	RA accept HTTP post over TCP/IP	RA shall accept HTTP post requests 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 This is out of scope as it defines EE behavior.	RA

2.4.10.5 ASN.1 Specification

- **ee-ra.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/ee-ra.asn?at=refs/heads/master
- **ee-ra-errors.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/ee-ra-errors.asn?at=refs/heads/master
- **scms-protocol.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/scms-protocol.asn?at=refs/heads/master
- **scms-base-types.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/scms-base-types.asn?at=refs/heads/master
- **scms-common-errors.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/scms-common-errors.asn?at=refs/heads/master
- 1609dot2-schema.asn
- 1609dot2-base-types.asn

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

2.4.11 Use Case 12: RSE bootstrapping

Target release	Release 1.0
JIRA Task	SCMS-162-Finish document "RSE Bootstrapping"In Review
Document owner	Biswajit Panja
Reviewer	
QA	

2.4.11.1 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.

2.4.11.2 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:

- All Root CAs
- (Optionally) 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.
- The MA
- (Optionally) 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 enrollment certificate
- The ECA certificate (so it can verify its own enrollment certificate)
- The RA certificate (so it can encrypt the certificate batch requests to the RA)
- Any network address information necessary to allow the device to locate the RA on the network. URL is used to connect to RA. The URL remains same, however DNS server may use different IP addresses.
- The certificate policy information that indicates to the RA how many pseudonym certificates the device can store, and the required refresh rates and sizes

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

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

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 and 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.

2.4.11.3 Assumptions

- All required certificates are provided upfront to the In-production DCM.
- A “secure environment” here means that the entirety of the connection between the DCM and RSE 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.

2.4.11.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-556	SCMS PoC out of Scope	Secure process	There shall be a secure operational process for devices manufactures to inject EE firmware, enrollment certificates etc.	Physical and operational security involving EEs is crucial to their security.	Doesn't apply to POC	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-557	SCMS PoC out of Scope	Secure chain of custody	EE shall get firmware, enrollment certificates etc. injected with a secure chain of custody for device manufacturers.	Documented and audited processes are crucial to the security of EEs.	Not software testable, procedural	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
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.	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.	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 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)

5 issues

2.4.11.5 Step 12.1: RSE initialization

Target release	Release 1.0
JIRA Task	SCMS-163-Finish document "RSE Initialization"In Review
Document owner	Biswajit Panja
Reviewer	
QA	

2.4.11.5.1 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 certificates (Root CA, PCA, MA, etc)
- Initial CRL

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

- Initial policy(ies)

2.4.11.5.2 Background and strategic fit

The use case Initialization involves the following components:

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

Overview:

The In-production DCM gathers the current certificates of:

- All Root CAs
- (Optionally) 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.
- The MA
- Policy Generator
- (Optionally) 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 RSE. Only the certificate of the Root CA has to be installed in a secure environment. All other certificates can be installed in a non-secure environment as the RSE now has the certificate of the Root CA to double check whether the new certificates are genuine.

2.4.11.5.3 Assumptions

- For the given design, it is assumed that the process takes place in a secure environment.
- The DCM is In-production and only accessible from a secure environment and sets up a secure connection to the SCMS.
- Root CA, ICA, PCA, MA certs are provided to the In-production DCM beforehand.

2.4.11.5.4 Requirements

Key	Status	Summary	Description	justification	notes	Components/s
SCMS-562	In Implementation	RA certificate	DCM shall provide the EE with the RA certificate	The EE will need to communicate securely with the RA (e.g.		DCM

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Components/s
			and the URL for the RA.	to request new certificates).		
SCMS-563	In Implementation	ECA certificate	DCM shall provide the EE with the ECA certificate and the URL for the ECA.	The EE will need to communicate securely with the ECA.		DCM
SCMS-564	In Implementation	MA certificate	DCM shall provide the EE with the MA certificate and the URL for the MA.	The EE will need to communicate securely with the MA (e.g. in order to download CRLs)		DCM
SCMS-565	In Implementation	ICA certificates	DCM shall provide the EE with its own ICA certificate. Optionally, include other existing ICA certificates.	The EE needs its ICA cert, e.g. to provide this to other EE in peer-to-peer cert updates.		DCM
SCMS-566	In Implementation	PCA certificates	DCM shall provide the EE with its own PCA certificate. Optionally, include other existing PCA	The EE needs its PCA cert, e.g. to provide this to other EE in peer-to-peer cert updates.		DCM

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			certificates.			
SCMS-567	In Implementation	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	In Implementation	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	In Implementation	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		DCM

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				Authority.		
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
SCMS-949	SCMS PoC out of Scope	Error code: eeInitCertProvFailed	EE generates this code when 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 certs.	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 generates this code when 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-1096	In Implementation	DNS Server	DCM shall provide the EE with the DNS information for the SCMS	The EE will use this to connect to the SCMS.		DCM

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Components/s
			DNS.			
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 secure tamper-resistant 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.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1160	SCMS PoC out of Scope	EE securely stores Root CA certificate	EE shall store the Root CA certificate in secure tamper-	The Root CA certificate must be protected against manipulation	This is out of scope since it defines EE's	On-board Equipment (OBE), Road-side Equipment

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			resistant storage.	. 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.	behavior.	(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	In Implementation	Policy Generator certificate	DCM shall provide the EE with the Policy Generator	The EE requires this to validate the signature on Policy		DCM

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			certificate.	Files.		
SCMS-1207	SCMS PoC out of Scope	EE stores Certificate Revocation List	EE shall store the Certificate Revocation List in tamper-resistent 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-resistant storage.	The EE will need to communicate securely, at the TLS level, with the RA (e.g. in order to download pseudonym certs) 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-resistant storage.	The EE will use this in the verification process of SCMS certificates.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

21 issues

2.4.11.5.5 ASN.1 Specification

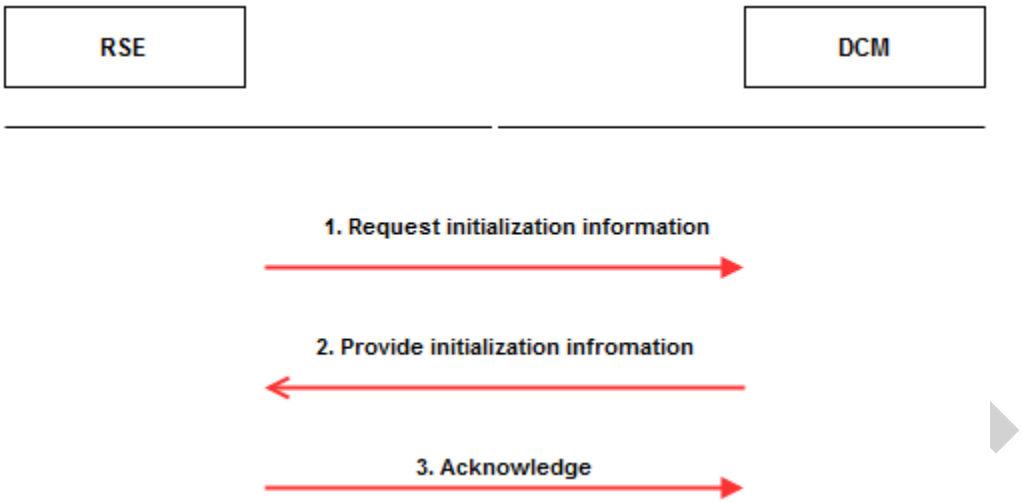
- **dcm-ee.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/dcm-ee.asn?at=refs/heads/master

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

- **dcm-ee-errors.asn**
  https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/dcm-ee-errors.asn?at=refs/heads/master

2.4.11.5.6 Design



2.4.11.6 Step 12.2: RSE enrollment

Target release	Release 1.0
JIRA Task	SCMS-164-Finish document "RSE Enrollment"In Review
Document owner	Biswajit Panja
Reviewer	
QA	

2.4.11.6.1 Goals

To provide RSEs with enrollment certificate.

2.4.11.6.2 Background and strategic fit

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

The use case Enrollment involves the following components:

- Actively involved:
  - The DCM
  - RSE being configured
  - ECA

Overview:

There must be a secure operational process and a chain of custody for RSEs, RSE firmware, and any other data to be injected to the RSE by the DCM. This is crucial to ensuring only properly certified devices can receive enrollment certificates. The operational process must involve some

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

physical protection and assurance that only certified devices are provisioned with certified software.

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 subsequently connects to the DCM through a trusted channel and performs an enrollment certificate request and receives an enrollment certificate response through the DCM. The secure environment is proprietary.
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.

In either case, once this process is complete the RSE has:

- The enrollment certificate
- The ECA certificate (so it can verify its own enrollment certificate)
- The RA certificate (so it can encrypt the certificate batch requests to the RA)
- Any network address information necessary to allow the device to locate the RA on the network. URL is used to connect to RA. The URL remains same, however DNS server may use different IP addresses.
- The certificate policy information that indicates to the RA how many pseudonym certificates the device can store, and the required refresh rates and sizes

Information Flow:

- Step 1: The RSE generates a key pair and puts the public key from the key pair in an unencrypted enrollment certificate request. The device sends the certificate request to the DCM.
    - Step 1.1: The DCM relays the message to the ECA over a trusted link and the ECA answers with an acknowledgment message
    - Step 1.2: The DCM stores the acknowledgment message to show that the request has been received by the ECA
- Step 2: The ECA generates one enrollment certificate derived from the public key, and creates a response message for the RSE containing the enrollment certificate. DCM securely delete enrollment certification information.
- Step 3: The ECA sends the response message to the DCM. As long as the Root CA certificate is available at the end-entity device and the request was put to the ECA in a secure environment, the reply can be conducted in a standard environment. Using the Root CA's certificate, the end-entity device can check the validity of the received information using the chain of trust.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

- Step 3.1: The DCM relays the response message to the RSE
- Step 3.2: The DCM stores the fact that the request has been fulfilled.

2.4.11.6.3 Assumptions

1. RSE has successfully gone through initialization process.

2.4.11.6.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-569	In Implementation	Correct Certificate	The enrollment process shall ensure that a correctly issued enrollment certificate corresponds to the requester's private key	To make sure that incorrect certificates are not issued to the requester. Correct certificate will allow requester to authenticate its certificate batch request for pseudonym certificates.		On-board Equipment (OBE), Road-side Equipment (RSE)
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-571	SCMS PoC out of Scope	Re-Enrollment	DCM shall provide new enrollment certificates	In case, if the EE is revoked (system	Does not apply to POC.	DCM

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			to EEs already deployed, in the event that use cases for re-enrollment are identified.	malfunction), EE needs to be re-bootstrapped.	Needs to be resolved for production.	
SCMS-573	SCMS PoC out of Scope	Secure Key Injection	The private key for the enrollment certificate shall be generated on the EE or be provided to the EE by the DCM using a secure key injection mechanism.	To keep the confidentiality of the keys.	Does not apply to POC	DCM
SCMS-574	Implemented	Encrypted Enrollment Certificate	The ECA shall encrypt the enrollment certificate with EE's public key contained in the enrollment certificate request	So only the device possessing the private key for the certificate can decrypt and use the certificate for requesting pseudonym certificates.		ECA
SCMS-951	Review	Error code: raEeVerificationFailed	RA shall log this error, if an EE cannot be authenticate	EE might need re-certification	Does not apply to POC. Might be	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			d.		added to MA integration as a misbehavior.	
SCMS-1095	In Implementation	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 private key of the enrollment certificate in tamper resistant secure memory.	To avoid that the private enrollment key can be extracted.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
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		ECA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				certificates cannot have an empty PSID field.		
SCMS-1306	Review	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	A clear mapping is required for proper administration.	In cases where an enrollment cert has more than one PSID, the corresponding apps are expected to be similar in nature. Such groupings of PSIDs in an enrollment cert are likely to be related to policy decisions to be made by the SCMS Manager.	ECA
SCMS-1307	Review	Enrollment certificate lifetime	Enrollment certificates shall have a life-time of 40 years	For PoC, enrollment certificates use a life-span of 40 years to avoid any need to update enrollment	This is for PoC only	ECA

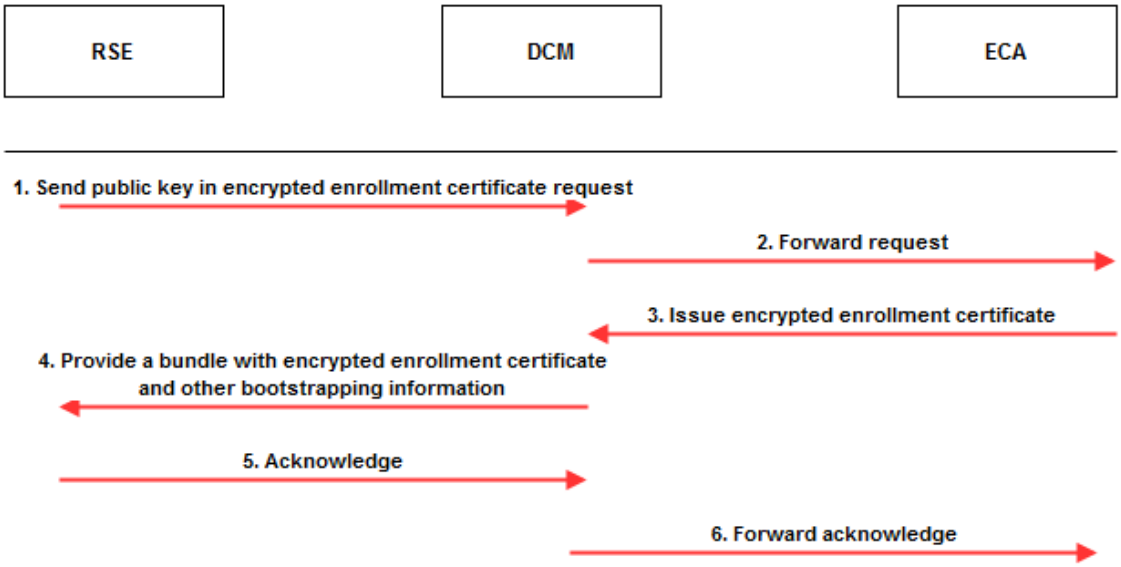
DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				certificates.		

11 issues

2.4.11.6.5 Design



2.4.11.6.6 ASN.1 Specification

- **eca-ee.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/eca-ee.asn?at=refs/heads/master
- **eca-ee-errors.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/eca-ee-errors.asn?at=refs/heads/master
- **dcm-eca.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/dcm-eca.asn?at=refs/heads/master
- **dcm-eca-errors.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/dcm-eca-errors.asn?at=refs/heads/master
- **dcm-ee.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/dcm-ee.asn?at=refs/heads/master
- **dcm-ee-errors.asn** master SCMS/scms-asnhttps://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/dcm-ee-errors.asn?at=refs/heads/master

2.4.12 Use Case 13: RSE Application Certificate Provisioning

Target release	Release 1.0
JIRA Task	SCMS-165-Finish document "RSE Initial Certificate Provisioning"In

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

	Review
Document owner	Virendra Kumar
Reviewer	
QA	

2.4.12.1 Goals

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

2.4.12.2 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 dependent on the connectivity of the RSE. If the RSE has frequent (or, always ON) connectivity, the certificate duration can be small like a day, otherwise it can be as large as 3 years. Based on the feedback from USDOT, for POC the validity duration of application certificates was decided to be 1 day and 1 hour, so that consecutive certificates will have an overlap period of 1 hour (same as pseudonym certificates).

Assumptions

- RSE is assumed to have a valid enrollment certificate.
- RSE is assumed to have Root CA, RA and PCA certificates.
- RSE is assumed to have relevant address(s) to communicate with the RA.

2.4.12.3 Design

At a high level, this use case can be divided into 3 steps as follows.

1. Request RSE Application Certificate
2. Generate RSE Application Certificate
3. 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 and sends it to the RA. The RA checks to make sure that the certificate request is correct and authorized. The RA creates and sends the request to the PCA. The PCA signs the application certificate, encrypts it for the device, 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 and returns the application certificate to the device.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

2.4.12.4 Step 13.1: Request RSE Application Certificate

Target release	Release 1.0
JIRA Task	SCMS-166-Finish document "Request RSE Certificates"In Review
Document owner	Virendra Kumar
Reviewer	
QA	

2.4.12.4.1 Goals

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

2.4.12.4.2 Background and strategic fit

The RSE decides to request application certificate from an RA, based on policy set by the SCMS Manager. The RSE may optionally contact DCM-R to determine which RA to submit the request to, or this information may be pre-configured.

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.

Two types of requests occur in the certificate provisioning process:

1. From RSE to RA
2. From RA to PCA (see Step 13.2: Generate RSE Application Certificate for details)

2.4.12.4.3 Prerequisites and Assumptions

In order to facilitate the certificate request process, the following prerequisites should be met:

- The RSE shall have successfully completed the bootstrap process (RSE bootstrapping)
- The RSE shall know the current network address of the RA

2.4.12.4.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-507	Implemented	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 issued any more certificates	Every logical RA has its own internal blacklist that is not shared with anyone	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
					else.	
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 their request was received by the RA.		RA
SCMS-522	SCMS PoC out of Scope	Retry request	If the EE doesn't receive acknowledgement (TCP ACK) within a specified amount of time, currently set to be 2 sec from the time of request, it shall retry.	to ensure that the request is received by the RA.	This is out of scope since it defines EE's 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	Certificate Provisioning Request with the RA for a minimum of 60 minute after 10 consecutive failed communication attempts resulting in no acknowledgement (TCP ACK) or no	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				Certificate Provisioning Response		
SCMS-524	SCMS PoC out of Scope	RA certificate	EE shall dynamically acquire RA's SCMS certificate in case it has changed, see EE →RA _ RA Certificate Request, EE →RA _ RA Certificate Response	so that EE can encrypt the request to the right RA	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-709	SCMS PoC out of Scope	Check for 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: Create / provide global and local policies.	• If no policy file is available on the EE, the EE is allowed to make a download attempt at	On-board Equipment (OBE), Road-side Equipment (RSE)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
					any time. • This is out of scope since it defines EE's behavior.	
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's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-767	SCMS PoC out of Scope	Check for Certificate Chain Updates	EE shall check for version changes in 'certChainFileId' field of the Global Policy file. If the version is	As CAs are added, removed, revoked, or rolled-	This is out of scope since it defines	On-board Equipment (OBE),

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			different than that of its existing file, it will take action to update it.	over, new certificate chains will have to propagated to EEs and other SCMS components. For more information: Global Certificate Chain File	EE's behavior.	Road-side Equipment (RSE)
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's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-953	SCMS PoC out of Scope	Misbehavior reporting: eeGlobalPolicyFileDownloadFailed	If EE is not able to download the global policy file (e.g. because there is none or it's corrupted), EE 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), Road-side Equipment (RSE)
SCMS-954	SCMS PoC out of Scope	Error code: eeGlobalPolicyVerificationFailed	EE shall implement OEM defined error handling and store this error code in EE's error log file, if EE is not	to enable EE side diagnostics.	This is out of scope since it defines	On-board Equipment (OBE),

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			able to verify the digital signature of the global policy file.		EE's behavior.	Road-side Equipment (RSE)
SCMS-955	SCMS PoC out of Scope	Misbehavior reporting: eeGlobalPolicyVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify the digital signature of the global 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-957	SCMS PoC out of Scope	Misbehavior reporting: eeGlobalPolicyFileParsingFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to parse the successfully downloaded global policy file (e.g. because it's 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 in its log file, 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-988	In Implementation	Error code: eeRetries	RA shall log "Error code: eeRetries", if the EE retries within the time specified in SCMS-522.	to enable server side diagnostics and to avoid		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				giving potential attackers relevant information. Retry not allowed within 2 seconds		
SCMS-990	In Implementation	Error code: moreThanAllowedTries	RA shall return status code HTTP 500, if the EE makes more than n retries within the time specified in SCMS-523, and log "Error code: moreThanAllowedTries".	More than n tries not allowed		RA
SCMS-1082	In Implementation	Error code: eeInvalidSignature	RA shall log "Error code: eeInvalidSignature", if the EE doesn't 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: eeRequestNotEncrypted	RA shall log "Error code: eeRequestNotEncrypted", if the EE doesn't encrypt the certificate request using the RA's 1609 certificate.	to enable server side diagnostics and to avoid giving potential attackers relevant informatio	A unencrypted certificate request might be an indication for misbeh	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				n	avior.	
SCMS-1084	In Implementation	Error code: eeInvalidCredentials	RA shall log "Error code: eeInvalidCredentials", 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: eeUnauthorizedRequest	RA shall log "Error code: eeUnauthorizedRequest", 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: eeMalformedRequest	RA shall log "Error code: eeMalformedRequest", 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: eeRaMismatch	RA shall log "Error code: eeRaMismatch", if this RA does not service the requesting EE.	to enable server side diagnostics and to avoid	A request from an EE that is	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				giving potential attackers relevant information.	not serviced by the requested RA might be an indication for misbehavior.	
SCMS-1088	In Implementation	Error code: eeInvalidTime	RA shall return status code HTTP 500, if the EE has an invalid system time, and log "Error code: eeInvalidTime".	to avoid EEs using the invalid certificates		RA
SCMS-1204	Implemented	Check blacklist	RA shall reject EE request, if EE is listed on its blacklist.	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)		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				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.		

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1278	Review	Certificate availability for download	RA's acknowledgement (https://jira.campllc.org/browse/SCMS-521~~SCMS-521~~) shall contain a time when the certificate will be available for download.	so that RSE can download the certificate in a timely manner.		RA
SCMS-1353	SCMS PoC out of Scope	EE gets LCCF from RA	EE shall check for and download policy an updated Local Certificate Chain File (LCCF) or Global Certificate Chain File (GCCF) 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 cert. This is out of scope since it defines EE's behavior	On-board Equipment (OBE), RA, Road-side Equipment (RSE)
SCMS-1356	SCMS PoC out of Scope	LCCF validation in EE	EE shall use the Local or Global Certificate Chain File (LCCF/GCCF) to validate received SCMS certificates and respond to P2P	EEs need to be able to validate received SCMS certificates based on	EE doesn't need to store all certificate	On-board Equipment (OBE), Road-side

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			certificate requests.	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.	chains, the LCCF provides the minimum set and EEs can learn additional chains via P2P certificate request. This is out of scope since it defines EE's behavior	Equipment (RSE)
SCMS-1397	Review	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 and not provide useful information to malicious actors.	• Standard TCP (SCMS-1090) and TLS (SCMS	ECA, RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
					- 977) errors shall be reported to EEs • All errors at the HTTP and higher levels shall 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	RA - Services View will document the actual	On-board Equipment (OBE), Road-side

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				protocol	HTTP post details This is out of scope as it defines EE behavior.	Equipment (RSE)
SCMS-1405	Review	RA accept HTTP post over TCP/IP	RA shall accept HTTP post requests 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 This is out of scope as it defines EE behavior.	RA

DRAFT

2.4.12.4.5 ASN.1 Specification

- **ee-ra.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/ee-ra.asn?at=refs/heads/master
- **ee-ra-errors.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/ee-ra-errors.asn?at=refs/heads/master

2.4.12.5 Step 13.2: Generate RSE Application Certificate

Target release	Release 1.0
JIRA Task	SCMS-167-Finish document "Generate RSE Certificates"In Review

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Document owner	Virendra Kumar
Reviewer	
QA	

2.4.12.5.1 Goals

Generate RSE certificates in a secure way.

2.4.12.5.2 Background and strategic fit

- RSE certificates have different validity periods, and the validity period for a given RSE is determined from the information contained in its enrollment certificate
- For each certificate request by RA, PCA generates a valid application certificate, encrypts the certificate for the RSE specified in the request, signs the encrypted packet, and sends it to RA
- RA makes the certificate available for download by the RSE
- PCA stores the certificate and hash of the RA-PCA certificate request for future misbehavior investigation and revocation purposes

The PCA and the RA store all information in a database. This information is only required for revocation and differs from one entity to another. Any information that is stored for revocation needs to be stored for 10 years. Any information that needs to be stored for device's lifetime will be stored for 40 years.
The PCA stores:

- A hash of the certificate request (to enable internal blacklisting at the RA)
- The certificate and its hash truncated to eight bytes, CertID8 (to allow the MA to request something from the PCA even if it gets only the digest of the certificate.)
- Validity period of the certificate (start and end times)

The RA stores:

- A hash of the certificate request. This value will be used by the MA to instruct the RA which enrollment certificate to put on the internal blacklist.
- The corresponding enrollment certificate
- Validity periods for requests for a given enrollment certificate

2.4.12.5.3 Assumptions

- RA and PCA complete all necessary sanity checks and signature verification before fulfilling with certificate provisioning request.

2.4.12.5.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS	Closed	Store RA informatio	RA shall store	so that EE can be revoked	PoC will only store	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
-530		n	information specified above (RA-stores) for a duration currently set to be 10 years	properly. 10 chosen as number of years of certificates (3) plus 7 years for historical purposes (law enforcement, legal, etc.).	3 years	
SCMS-532	Closed	Store PCA information	PCA shall store information specified at PCA-stores for a duration currently set to be 10 years	10 chosen as number of years of certificates (3) plus 7 years for historical purposes (law enforcement, legal, etc.).	PoC will only store 3 years	PCA
SCMS-755	Implemented	Store enrollment certificate	RA shall store enrollment certificate for each RSE for its lifetime, that is currently assumed to be 40 years	so that RSE can be revoked properly		RA
SCMS-757	Implemented	pca-info-storage	PCA shall store information specified above (PCA-stores) for a duration currently set to be 10	so that RSE can be revoked properly		PCA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			years			
SCMS-1155	In Implementation	check request parameters	RA shall check the certificate request parameters (including validity period) and validate with local and global policies	so that only valid requests are processed		RA
SCMS-1212	Review	RSE Application Certificate Validity Overlap	RA shall generate RSE application certificates with validity overlap for any 2 consecutive certificates by a time $t_{overlap}$, which is currently set to be 1 hour.	This is in line with pseudonym certificates.		RA
SCMS-1213	Review	RSE Application Certificate Validity	RA shall generate RSE application certificates with validity period t_validity, which is currently set to 1 day for	As per communications with USDOT, RSEs will have frequent connectivity. So, a short validity period is justified for RSE application		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			POC.	certificates.		
SCMS-1312	Review	Issue RSE application certificates with optional encryption key	PCA shall issue RSE application certificates with optional encryption key.	The encryption key is optional.	RSE application certificates always have a signature key and optionally an encryption key.	PCA
SCMS-1313	Review	Issue only one RSE application certificate valid at a time	PCA shall only issue one RSE application cert 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-1372	Review	PSID/SSP assignment to certificates	PCA/RA shall read the set of PSID/SSP values of the enrollment certificate that was used for the certificate request and use the exact same set to OBE	PSID/SSPs shall be assigned in groups such that corresponding applications are similar in nature.		PCA, RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			and RSE certificates during provisioning.			

10 issues

2.4.12.5.5 ASN.1 Specification

- **pca-ra.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/pca-ra.asn?at=refs/heads/master
- **`pca-ra-errors.asn`** `https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/pca-ra-errors.asn?at=refs/heads/master`

2.4.12.6 Step 13.3: Download RSE Application Certificate

Target release	Release 1.0
JIRA Task	SCMS-168-Finish document "Download RSE Certificates"In Review
Document owner	Virendra Kumar
Reviewer	
QA	

2.4.12.6.1 Goals

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

2.4.12.6.2 Background and strategic fit

The download will include application certificate and a pca_certificate_chain file containing the PCA certificate chain required to validate the application certificate.

2.4.12.6.3 Assumptions

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

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

2.4.12.6.4 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-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-	Closed	RA download via HTTPS	RA shall provide downloa	to utilize standard internet	Downloads could be e.g. policy file, Global Certificate Chain File,	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
514			ds over HTTPS (TLS).	protocols for the download process.	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 certs currently. Instead the OBE will use TLS to authenticate the other endpoint (as a server) and will use its SCMS cert to identify itself. EE authenticates via its IEEE 1609.2 enrollment certificate. The details of the authentication process are defined Step 3.4: Download of Pseudonym Certificates	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	For pseudonym certificates, this counters a somewhat exotic attack: if an attacker eavesdrops all individually encrypted pseudonym certificates (encrypted by PCA to	On-board Equipment (OBE), RA, Road-side

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				certificate (protect location privacy) or, in case of pseudonym certificates, that an adversary is able to read PCA-encrypted pseudonym certificates (adversary might extract Butterfly encryption keys from junked vehicle at a later stage and is then able to identify all EE certificates).	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.	Equipment (RSE)
SCMS	SCMS PoC out	RA authentication to EE	The EE shall	EE checks	This is out of scope since it defines EE's	On-board

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
-539	of Scope		require RA Authentication before any communication starts.	whether it talks to proper RA before communication starts and to avoid sending its enrollment certificate to a malicious RA. RA authenticates via its TLS X.509 certificate. The details of the authentication process are defined in Step 3.4: Download of Pseudonym Certificates.	behavior.	Equipment (OBE), Road-side Equipment (RSE)
SCMS	In Impleme	OCSP stapling - RA	The RA shall	This is as a	OCSP stapling provides improved	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
-540	ntation		support OSCP stapled certificate response to OBE.	means to react to RA's revocation. In case the RA is compromised, and the DNS server is compromised or spoofed, then a revocation mechanism will prevent further damage.	performance compared to CRLs. OCSP stapling is specified in RFC 6066, Section 8. 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). The RA will be able to respond to the OBE's request for an OSCP stapled certificate. The RA itself will be able to request OCSP certificate currency from an OCSP server in order that it (the RA) is assured of the other components TLS cert currency, so it will require the OCSP request URL and credentials.	
SCMS-541	SCMS PoC out of Scope	OCSP stapling - EE	The EE may use the TLS Certificate Status Request extension (OCSP stapling) to verify RA	Revocation is optional and it's up to the OEMs support it.	This is out of scope since it specifies EE's behavior If EE does not support this feature, the following might happen: An adversary that extracted the RA's private key and that successfully spoofed DNS is able to learn	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			revocation status.		EE's enrollment certificate (but not EE's private key). OCSP stapling is specified in RFC 6066, Section 8.	
SCMS-544	Closed	Download resume	RA shall support byte-wise resume of certificate batch, certificate file, or policy file, downloads, even if EE switches the IP address.	to improve reliability of the download protocol.		RA
SCMS-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	This feature helps RSEs recover from a		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			application certificate that has previously been downloaded, so long as the RSE's credentials are still valid and the certificate is not expired.	loss of certificates at the RSE level (e.g., disk corruption).		
SCMS-768	In Implementation	RA - Global Certificate Chain File	RA shall provide a Global Certificate Chain File and a Local Certificate Chain File for download by EEs.	to enable EEs to verify certificates without further CA certificate downloads. If the Global Policy File indicates a new version of the Global Certificate Chain	For more information: Global Certificate Chain File	RA

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				File than that existing on the EE, the EE will need to download it and apply it.		
SCMS-958	SCMS PoC out of Scope	Error code: eeConnectionFailed	EE shall log this error in its log file, 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 reporting: 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's corrupte	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)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			d).			
SCMS-967	SCMS PoC out of Scope	Error code: eeCertFileVerificationFailed	EE shall implement OEM defined error handling and store the error code in EE's error log file, 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 reporting: 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	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)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			certificate.			
SCMS-969	SCMS PoC out of Scope	Error code: eeCertificateFileDecryptionFailed	EE shall implement OEM defined error handling and store the error code in EE's error log file, if EE is not able to decrypt an encrypted certificate.	to enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-971	SCMS PoC out of Scope	Error code: eeCertificateVerificationFailed	EE shall implement OEM defined error handling and store the error code in EE's error log file, 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)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-972	SCMS PoC out of Scope	Misbehavior reporting: 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 implement OEM defined error handling and store the error code in EE's error log file, 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-	SCMS PoC out of Scope	Misbehavior reporting: eeCertContentFalse	EE shall initiate a misbehavior	to enable server side misbeha	This is out of scope since it defines EE's behavior.	On-board Equipment

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
974			report to MA with the observed error, if EE is not able to parse a certificate, or if the certificate has wrong content.	vior detection.		(OBE), Road-side Equipment (RSE)
SCMS-976	In Implementation	Error code: raInvalidURL	RA shall log this error code, 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	Error code: raNoTLS	RA shall return standard TLS error codes if TLS errors occur.	in order to enable client side error handling.		RA
SCMS-	In Implementation	Error code: raAuthenticationFailed	RA shall log this error, if EE-to-	to enable server side diagnost		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
978			RA authentication fails.	ics and to avoid giving potential attackers relevant information.		
SCMS-979	SCMS PoC out of Scope	Error code: eeAuthenticationFailed	EE shall store this error code in EE's error log file, 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 reporting: 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 this error, if Global Certificate Chain	to enable client side error handling.		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			File is not available.			
SCMS-1089	In Implementation	Error code: rseCertificateUnavailable	RA shall return this error, 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
SCMS-1090	In Implementation	Error code: rseRaTcpErrors	RA shall return standard TCP error codes if TCP errors occur.	in order to enable client side error handling.		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 since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS	Implemented	Check time stamp	RA shall check	If the differenc		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
-1203			the signed (by EE) time-stamp and allow a tolerance of 5 seconds.	e between the signed time-stamp and the current time is 5 seconds or less, RA will proceed with the authentication process. Otherwise RA will reject the connection.		
SCMS-1204	Implemented	Check blacklist	RA shall reject EE request, if EE is listed on its blacklist.	If EE is listed, RA will reject the connection. Otherwise RA will proceed with the authentication process. The Internal Blacklist		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				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		

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

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-1303	SCMS PoC out of Scope	Verification of certificate validity	EE shall verify the validity of a received certificate against	to verify if the certificate is issued by a trustworthy	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 Equipm

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			IEEE 1609.2-v3-D12, clause 5.1 and 5.3.	source and therefore messages signed by this certificate can be trusted.		ent (RSE)

34 issues

2.4.12.6.5 Design

- Step 1: RSE and RA authenticate to each other, see below.
- Step 2: RSE downloads the global certificate chain file (see file definition in Global Certificate Chain File).
- Step 3: RSE downloads the application certificate.

2.4.12.6.5.1 RSE-RA Authentication and RA-RSE Authentication

See Step 3.4: Download of Pseudonym Certificates - EE-RA Authentication and RA-EE Authentication

2.4.12.6.5.2 RA Revocation

See Step 3.4: Download of Pseudonym Certificates - RA Revocation

2.4.13 Use Case 14: RSE Misbehavior Reporting

Target release	Release 1.1
JIRA Task	SCMS-169-Finish document "RSE Misbehavior Reporting"Open
Document owner	Biswajit Panja
Reviewer	
QA	

2.4.13.1 Goals

- Misbehavior reports provided by RSE about misbehaving RSE
- Maintain the trust in the system
- Identify and remove bad actors

2.4.13.2 Background and strategic fit

RSEs send misbehavior reports to the MA. The format of a misbehavior report is not defined yet but a report potentially includes reported BSMs as well as the reporter's certificate and the reporter's signature. Reports may include random BSMs (casual report), suspicious BSMs, and

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

alert-related BSMs. The report is encrypted by the RSE for the MA. Note: The RSEs' misbehavior detection algorithms (also called local misbehavior detection) are not defined yet.

The following steps are executed:

- Step 1: RSE creates a misbehavior report, encrypts it to the MA, and submits it to the RA.
    - Step 1': The RA encrypt misbehavior report and forwards the encrypted report to the MA. RA shuffles misbehavior report.
    - Note: Misbehavior report older than one week not required to be stored in RSE(not requirement, for informational purposes)
    - No separate ACK, RA to RSE

2.4.13.3 Requirements

Key	Status	Summary	Description	justification	notes	Components
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 their request was received by the RA.		RA
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-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	Amount of shuffle and/or maximum delay decided by SCMS manager.	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				time are from same OBE.		
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-1009	SCMS PoC out of Scope	Error code: eeEncryptionFailed	RSE shall store this error in it's error log file, if RSE encounters an error when encrypting a misbehavior report with MA's public key.	Unable to create cipher text at RSE	This is out of scope since it defines EE's behavior.	Road-side Equipment (RSE)
SCMS-1010	In Implementation	Error code: maDecryptionFailed	MA shall store this error in MA's error log file, if MA	Unable to create plain text at MA, the cipher text sent		MA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			encounters an error when decrypting a misbehavior report.	from EE		
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-1309	SCMS PoC out of Scope	RSE sign misbehavior report	RSE shall sign misbehavior reports with RSE application certificate	To avoid forged misbehavior reports and introduce liability.	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	Road-side Equipment (RSE)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Components/s
					behavior.	
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	Review	RA accept HTTP post over TCP/IP	RA shall accept HTTP post requests 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 This is out of scope as it defines EE behavior.	RA

2.4.13.4 ASN.1 Specification

- **ee-ma.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/ee-ma.asn?at=refs/heads/master

2.4.14 Use Case 15: RSE CRL Check

Target release	Release 1.0
JIRA Task	SCMS-170-Finish document "RSE CRL Check"In Review

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Document owner	Virendra Kumar
Reviewer	Benedikt Brecht
QA	

2.4.14.1 Goals

- RSE is enabled to check whether EE certificate was revoked (e.g. by online request)

2.4.14.2 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-786	In Implementation	CRL download	MA shall provide CRL to RSE via CRL store and CRL broadcast	so that RSE can check revocation status of EE certificates	CRL entries may be dependent on the type of certificate	MA

1 issue

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

Target release	Release 1.0
JIRA Task	SCMS-171-Finish document "RSE Revocation"In Review
Document owner	Andre Weimerskirch
Reviewer	
QA	

2.4.15.1 Assumptions

- Non-pseudonymous certificate types - OBE identification certificates and RSE application certificates - integrate a 4-byte revocation identifier field (RIF) that is calculated as follows:
    - [LSB0] least significant byte of RIF: the least significant byte of the PCA identifier
    - [LSB1-3] of RIF: the three least significant bytes [LSB0-2] of the SHA-256 hash of the EE's enrollment certificate, i.e., RIF_[LSB1] = enrollment_cert[LSB0], RIF_[LSB2] = enrollment_cert[LSB1], and RIF_[LSB3] = enrollment_cert[LSB2].

2.4.15.2 Background and strategic fit

2.4.15.2.1 Misbehavior Investigation

Misbehavior investigation works as follows for RSE application certificates and OBE identification certificates (non-pseudonymous certificates without linkage values). Misbehavior

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

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.

2.4.15.2.2 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. As a consequence, the CRL does not have to specify PSIDs. Further, it has been decided that 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.

2.4.15.3 Step 16.1: RSE Application and OBE Identification Certificate Misbehavior Analysis

Target release	Release 1.0
JIRA Task	SCMS-181-Finish document "RSE Misbehavior Analysis"In Review
Document owner	Andre Weimerskirch
Reviewer	
QA	

OBE Misbehavior Analysis will be defined by CAMP's VSC6 Communications Research (CR) project and integrated with the to be awarded "Misbehavior Authority Integration" sub project.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

RSE Misbehavior Analysis is out of scope of POC. For POC, this is a "black box" that determines whether an EE misbehaved or not. The MA misbehavior analysis algorithm (aka Global Misbehavior Detection) will leverage the Investigation methods described in 16.2. RSE Application and OBE Identification Certificate Misbehavior Investigation.

A potential model for RSE Misbehavior Analysis is a black box that upon input of all misbehavior reports outputs certificates together with the label 'misbehavior detected'. The RSE Misbehavior Analysis leverages the RSE Misbehavior Investigation functions for this task. After the RSE Misbehavior Analysis outputs the labeled certificates, it passes those certificates to the RSE Revocation (16.3. RSE Application and OBE Identification Certificate Revocation (CRL, blacklist)).

The steps are as follows:

1. Misbehavior reports are provided by EE to SCMS
2. SCMS invokes Misbehavior Analysis and passes all misbehavior reports
3. Misbehavior Analysis runs the Global Misbehavior Detection and utilizes RSE Misbehavior Investigation.
4. Misbehavior Analysis continuously outputs certificates that were identified as 'misbehaving'.
5. The SCMS invokes RSE Revocation with certificates identified as 'misbehaving'

2.4.15.3.1 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-611	In Implementation	Revoke all reported certs	The MA shall revoke each reported certificate directly.	For testing purposes the PoC needs to have a simple mechanism to create CRLs.	Requirement for PoC only.	MA

1 issue

2.4.15.3.2 Not Doing

- Implementation of Misbehavior Analysis.

2.4.15.4 Step 16.2: RSE Application and OBE Identification Certificate Misbehavior Investigation

Target release	Release 1.0
JIRA Task	SCMS-182-Finish document "RSE Misbehavior Investigation"In Review
Document owner	Andre Weimerskirch
Reviewer	

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

QA	

2.4.15.4.1 Goals

- The Misbehavior Investigation is a set of functions that support Misbehavior Analysis (see Step 16.1: RSE Application and OBE Identification Certificate Misbehavior Analysis).

2.4.15.4.2 Background and strategic fit

- To support Misbehavior Analysis.

2.4.15.4.3 Assumptions

- Non-pseudonymous certificate types - OBE identification certificates and RSE application certificates - integrate a 4-byte revocation identifier field (RIF) that is calculated as follows:
    - [LSB0] least significant byte of RIF: the least significant byte of the PCA identifier
    - [LSB1-3] of RIF: the three least significant bytes [LSB0-2] of the SHA-256 hash of the EE's enrollment certificate, i.e., RIF_[LSB1] = enrollment_cert[LSB0], RIF_[LSB2] = enrollment_cert[LSB1], and RIF_[LSB3] = enrollment_cert[LSB2].

2.4.15.4.4 Design

Misbehavior investigation works as follows for RSE application certificates and OBE identification certificates (non-pseudonymous certificates without linkage values). MA can link certificates based on the revocation identifier field (RIF) and no additional steps are necessary.

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.

Note that there is no mechanism for a group revocation for these types of certificates.

2.4.15.5 Step 16.3: RSE Application and OBE Identification Certificate Revocation (CRL, blacklist)

Target release	Release 1.0
JIRA Task	SCMS-183-Finish document "RSE Revocation (CRL and blacklist)"In Review
Document owner	Andre Weimerskirch
Reviewer	
QA	

2.4.15.5.1 Goals

- The OBE Revocation is a set of functions to revoke an EE after Misbehavior Analysis determined that EE shall be revoked. The main output is
    - Blacklist EE in RA
    - Determine all certificate digests (CertIDs) so that they can be added to the CRL

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

2.4.15.5.2 Background and strategic fit

Revoke misbehaving RSEs and OBE identification certificates

2.4.15.5.3 Assumptions

- Non-pseudonymous certificate types - OBE identification certificates and RSE application certificates - integrate a 4-byte revocation identifier field (RIF) that is calculated as follows:
    - [LSB0] least significant byte of RIF: the least significant byte of the PCA identifier
    - [LSB1-3] of RIF: the three least significant bytes [LSB0-2] of the SHA-256 hash of the EE's enrollment certificate, i.e., RIF_[LSB1] = enrollment_cert[LSB0], RIF_[LSB2] = enrollment_cert[LSB1], and RIF_[LSB3] = enrollment_cert[LSB2].

2.4.15.5.4 Design

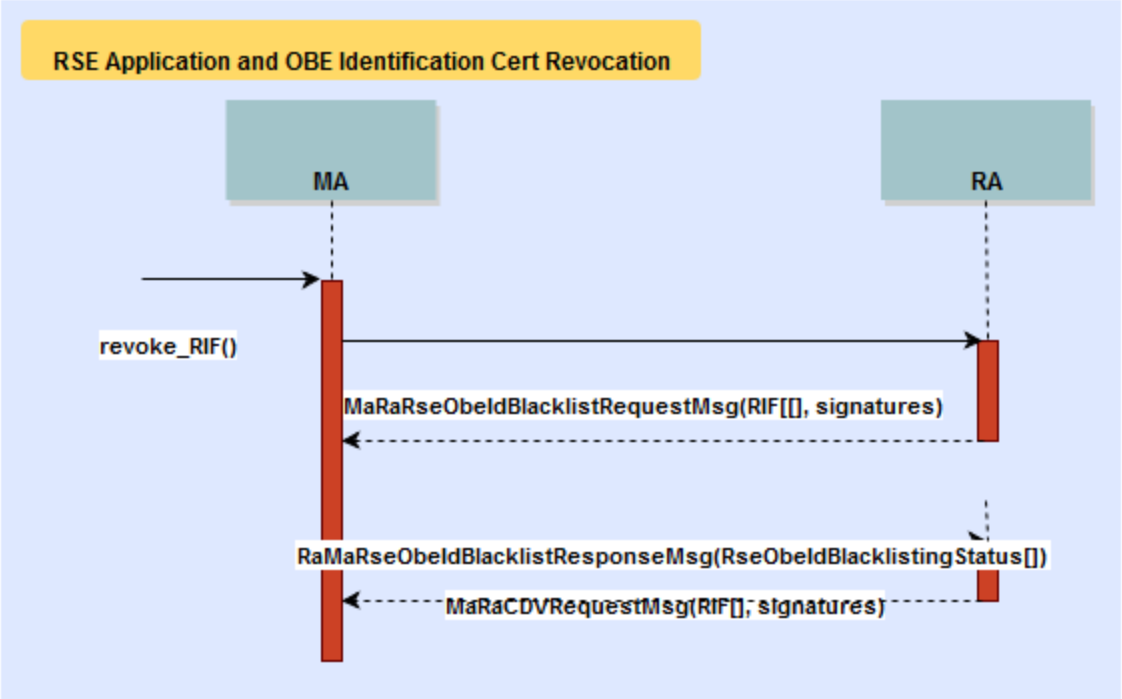
Revocation works as follows for RSE application certificates and OBE identification certificates (non-pseudonymous certificates without linkage values).

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. As a consequence, the CRL does not have to specify PSIDs. Further, it has been decided that certificates will carry all PSIDs showing up in the enrollment certificate that was used to request those certificates. This implies that blacklists are not PSID-specific either.

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary



2.4.15.5.5 Step 16.3.1: MA-RA: Revocation Identifier Field (RIF) -> blacklist entry

Target release	Release 1.0
JIRA Task	SCMS-616-Finish document "MA-RA: hash of RA-PCA request -> blacklist entry"In Review
Document owner	Andre Weimerskirch
Reviewer	
QA	

2.4.15.5.5.1 Requirements

Key	Status	Summary	Description	justification	notes
SCMS-407	In Implementation	TLS Mutual Authentication	Communication transactions between SCMS components shall be client-server mutually	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 a OCSP service at the technical component of the SCMS manager shall be deployed for revocation. See SCMS-406 for

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes
			authenticated and encrypted with TLS (except EE-RA).		information about the cipher suite, SCMS-1016 for information about OCSP, and https://jira.campllc.org/browse/SCMS-938~~SCMS-938~~ for TLS certificate management.
SCMS-789	In Implementation	Error code: internalTimeout	LA, PCA, RA shall return and log this error code, if there is an internal timeout within the component such that it cannot correctly process the request in time but can still respond to the MA.	to enable server side error handling.	
SCMS-792	In Implementation	Error code: noMaAuthorizationSignature	LA, PCA and RA shall return this error code and add an error entry to its log file, if a request from the MA does not have a signature.	to enable server side error handling.	LA, PCA and RA only accept requests that use a valid format and that are authorized. The authorization process is done by signature.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes
SCMS-793	In Implementation	Error code: invalidMaAuthorizationSignature	PCA shall return this error code and add an error entry to its log file, if the MA authorization signature is invalid.	to enable server side error handling.	PCA only accepts requests that use a valid format and that are authorized. The authorization process is done by signature
SCMS-816	Implemented	Remove Blacklist Entry: POC	There shall be a feature to remove a blacklist entry manually.	If an EE is revoked, there needs to be a mechanism to remove the blacklist entry, e.g. for testing purposes. Blacklist entries are on the level of enrollment certificates. This needs to be considered on the level of certificate types	This is only for POC. It needs to be reconsidered later whether this feature can stay or should be removed.

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes
				though, i.e., for pseudonym certificates, OBE identification certificates, and RSE application certificates.	
SCMS-910	In Implementation	Error code: raInvalidInputValueFormat	RA shall return this error code and add an error entry to its log file, if the input values are improperly formatted.	to enable server side error handling.	
SCMS-911	In Implementation	Error code: raInvalidRIFValue	If an invalid revocation identifier field (RIF) value is input, RA shall provide this error code	For diagnosis purposes this error code should be used.	
SCMS-	In Implement	RA add to blacklist	RA shall provide an interface	To support MA	

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes
916	ation		to add corresponding enrollment certificates to its internal blacklist for a given array of request identifier field (RIF) values.	processes of revoking RSE certificates by avoiding an RSE to get new RSE application certificate with its current enrollment certificate. RA simply looks up the RIF value in its internal database to determine the enrollment certificate, and adds it to the blacklist.	
SCMS-917	In Implementation	Error code: raCertificateAlreadyBlacklisted	If the input enrollment certificate is already blacklisted, the RA	For diagnosis purposes this error code should be used.	

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes
			shall return this error code		
SCMS-918	In Implementation	RA RIF value request limit	RA shall be able to process a request input of up to a configurable amount of revocation identifier field (RIF) values	Set a maximum value to allow proper sizing of IT.	
SCMS-919	In Implementation	Request limit: POC	For POC, RA shall be able to process a request of up to 10,000 request identifier field (RIF) values.	For performance reasons. This upper performance limit is used in POC.	
SCMS-921	In Implementation	Performance	The SCMS component shall respond with the correct response or an error message in time to support system throughput	There must be a defined time-out.	

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes
			requirements		
SCMS-923	In Implementation	Error code: maRequestTimeout	MA shall log this timeout error, if the RA, PCA or LA does not respond within the defined threshold time	to enable server side error handling and for diagnosis purposes MA should log this error.	
SCMS-927	In Implementation	Validation	RA shall validate the input. If the validation fails, RA shall return an error to MA. Otherwise RA shall starts its computation.	RA only accepts properly formatted requests with a valid value.	
SCMS-930	In Implementation	Log	APDU requests and responses shall be stored for a configurable amount of time in an	To allow proper auditing.	

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes
			encrypted database.		
SCMS-931	In Implementation	Log: POC	For POC, at least 10,000 APDU requests and 10,000 responses shall be stored in an encrypted database .	To allow proper auditing.	
SCMS-936	In Implementation	Error code: raNumberOfRequestsExceeded	RA shall return this error code, if more than the threshold number of request identifier field (RIF) values are input,	to enable server side error handling.	

17 issues

2.4.15.5.6 Step 16.3.2: MA-RA: Revocation Identifier Field (RIF) -> list of certificate digest values

Target release	Release 1.0
JIRA Task	SCMS-615-Finish document "MA-RA: hash of RA-PCA request -> list of certificate digest values"In Review
Document owner	Andre Weimerskirch
Reviewer	
QA	

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

2.4.15.5.6.1 Requirements

Key	Status	Summary	Description	justification	notes
SCMS-407	In Implementation	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 a OCSP service at the technical component of the SCMS manager shall be deployed for revocation. See SCMS-406 for information about the cipher suite, SCMS-1016 for information about OCSP, and https://jira.campllc.org/browse/SCMS-938~~SCMS-938~~ for TLS certificate management.
SCMS-789	In Implementation	Error code: internalTimeout	LA, PCA, RA shall return and log this error code, if there is an internal timeout within the component such that it cannot correctly process the request in time but can still respond to the MA.	to enable server side error handling.	
SCMS-791	In Implementation	Verify MA request authorization	LA, PCA and RA shall	LA, PCA, RA only accepts	There is a set (sequence) of countersignatures per request. These

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes
			verify the MA requests in terms of authorization. If the verification fails, it shall return an error to MA and add an entry to its error log. Otherwise it shall start its computation.	requests from MA that use a valid format and that are authorized. The authorization process is done by signature.	countersignatures are provided by some trusted authority, and only if the signatures verify successfully, the the command will be executed. It's a policy decision which authorities need to sign the requests. For instance, it could be as simple as MA, or as difficult as some real-world legal entity (e.g. NHTSA).
SCMS-792	In Implementation	Error code: noMaAuthorizationSignature	LA, PCA and RA shall return this error code and add an error entry to its log file, if a request from the MA does not have a signature.	to enable server side error handling.	LA, PCA and RA only accept requests that use a valid format and that are authorized. The authorization process is done by signature.
SCMS-793	In Implementation	Error code: invalidMaAuthorizationSignature	PCA shall return this error code and add an error entry to its log file, if the MA	to enable server side error handling.	PCA only accepts requests that use a valid format and that are authorized. The authorization process is done by signature

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes
			authorization signature is invalid.		
SCMS-910	In Implementation	Error code: raInvalidInputValueFormat	RA shall return this error code and add an error entry to its log file, if the input values are improperly formatted.	to enable server side error handling.	
SCMS-918	In Implementation	RA RIF value request limit	RA shall be able to process a request input of up to a configurable amount of revocation identifier field (RIF) values	Set a maximum value to allow proper sizing of IT.	
SCMS-919	In Implementation	Request limit: POC	For POC, RA shall be able to process a request of up to 10,000 request identifier field (RIF) values.	For performance reasons. This upper performance limit is used in POC.	

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes
SCMS-921	In Implementation	Performance	The SCMS component shall respond with the correct response or an error message in time to support system throughput requirements	There must be a defined time-out.	
SCMS-923	In Implementation	Error code: maRequestTimeout	MA shall log this timeout error, if the RA, PCA or LA does not respond within the defined threshold time	to enable server side error handling and for diagnosis purposes MA should log this error.	
SCMS-927	In Implementation	Validation	RA shall validate the input. If the validation fails, RA shall return an error to MA. Otherwise RA shall starts its	RA only accepts properly formatted requests with a valid value.	

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes
			computation.		
SCMS-929	In Implementation	Error code: raInvalidRIFValue	RA shall return this error code and add an error entry to its log file, if an invalid revocation identifier field (RIF) value is input.	RA only accepts properly formatted requests with a valid value.	
SCMS-930	In Implementation	Log	APDU requests and responses shall be stored for a configurable amount of time in an encrypted database.	To allow proper auditing.	
SCMS-931	In Implementation	Log: POC	For POC, at least 10,000 APDU requests and 10,000 responses shall be stored in an encrypted	To allow proper auditing.	

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes
			database .		
SCMS-933	In Implementation	RA return list of certificate digests	After inputting a valid set of RIF values, RA shall output the correct set of corresponding arrays of certificate digest values (note that one array of certificate digest values is returned per RIF value).	To support MA processes of revoking RSE certificates, RA provides a list of certificate digests to be revoked. RA simply looks up the RIF value in its internal database. If the internal database stores corresponding certificates, RA hashes the certificate and provides the certificate digest. If the internal	

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes
				database stores corresponding certificate digests, RA provides that digest.	
SCMS-936	In Implementation	Error code: raNumberOfRequestsExceeded	RA shall return this error code, if more than the threshold number of request identifier field (RIF) values are input,	to enable server side error handling.	

16 issues

2.4.16 Use Case 17: Refresh RSE Application Certificates

Target release	Release 1.0
JIRA Task	SCMS-172-Finish document "Refresh RSE Certificates"In Review
Document owner	Andre Weimerskirch
Reviewer	
QA	

2.4.16.1 Goals

- Refresh RSE certificates

2.4.16.2 Background and strategic fit

RSE application certificates are refreshed after the initial provisioning (see Use Case 13: RSE Application Certificate Provisioning). This use-case is very similar to the initial certificate provisioning except that RA did not encounter the RSE before.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

2.4.16.3 Assumptions

- Initial certificate provisioning (see Use Case 13: RSE Application Certificate Provisioning) has been executed before.
- The certificate provisioning process defined and specified in Use Case 13: RSE Application Certificate Provisioning is also used to refresh certificates.

2.4.16.4 Requirements

All requirements from use-case 13 apply:

- Step 13.1: Request RSE Application Certificate
- Step 13.2: Generate RSE Application Certificate
- Step 13.3: Download RSE Application Certificate

The following requirements apply additionally to those from Use Case 13: RSE Application Certificate Provisioning.

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-512	Closed	Global Policy file	RA shall always provide a global policy file available for download by EE	There is always a global configuration available, and that configuration shall be current		RA
SCMS-709	SCMS PoC out of Scope	Check for 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	• If no policy file is available on the EE, the EE is allowed to make a down	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				are available at Use Case 18: Create / provide global and local policies.	load attempt at any time. • This is out of scope since it defines EE's behavior.	
SCMS-767	SCMS PoC out of Scope	Check for Certificate Chain Updates	EE shall check for version changes in 'certChainFileId' field of the Global Policy file. If the version is different than that of its existing file, it will take action to update it.	As CAs are added, removed, revoked, or rolled-over, new certificate chains will have to propagated to EEs and other SCMS components. For more information: Global Certificate Chain File	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-768	In Implementation	RA - Global Certificate Chain File	RA shall provide a Global Certificate Chain File and a Local Certificate Chain File for download by EEs.	to enable EEs to verify certificates without further CA certificate downloads. If the Global Policy File indicates a new version of the Global Certificate Chain File than that existing on the EE, the EE will need to download it and apply it.	For more information: Global Certificate Chain File	RA
SCMS-952	SCMS PoC out of Scope	Error code: eeGlobalPolicyFileDownloadFailed	EE shall implement OEM defined error handling and store the error code in EE's error	As the global policy file is essential for the system to work correctly and	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			log file, if EE is not able to download the global policy file (e.g. because there is none or it's corrupted).	contains security relevant information, it is important to have an error handling whenever the EE is not able to get the latest version of that file.		
SCMS-956	SCMS PoC out of Scope	Error code: eeGlobalPolicyFileParsingFailed	EE shall implement OEM defined error handling and store this error code in EE's error log file, if EE is not able to parse the successfully downloaded global policy file (e.g. because it's corrupted).	As the global 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	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				of that file.		
SCMS-1063	In Implementation	Certificate Provisioning	RA shall implement RSE Application Certificate provisioning as defined in Use Case 13: RSE Application Certificate Provisioning	Refreshing RSE applications works in the same way as the initial certificate provisioning. However, some additional requirements need to be considered. These are defined below.		RA
SCMS-1064	In Implementation	Blacklist Check	RA shall check whether requester's enrollment certificate is on blacklist. If requester's enrollment certificate is on blacklist, then RA does not respond and	RA checks whether requester's enrollment certificate is in the blacklist database.		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			makes an entry in its log file.			
SCMS-1065	In Implementation	Error code: raBlacklisted	RA shall log this error if the requesting EE has been blacklisted. RA shall not give any response to the EE in this case.	Error's produced by an EE should always be logged for diagnosis purposes and never returned to the EE to avoid giving a potential attacker sensitive information.		RA
SCMS-1066	SCMS PoC out of Scope	Request Check	SCMS 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	Stop misbehaving RSEs that request multiple certificates per time period.	Consider this for MA integration at a later stage.	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			by its enrollment certificate).			
SCMS-1067	In Implementation	Overlap period	The tolerated overlap shall be defined by the PSID owner.	Allow an overlap between certificates of at most one hour.	For POC, the tolerated overlap shall be 1 hour.	RA
SCMS-1068	In Implementation	Error code: raRequestForMultipleCerts	RA shall log this error 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-1069	In Implementation	RA shall deny duplicate request	RA shall reject conflicting RSE request.	Detect duplicate false requests.	For a given (enrollment certificate, public key, PSID, SSP, validity period) combination, RA shall	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
					reject a duplicate, overlapping request except for the allowed overlap of 1 hour. This will catch cases in which an RSE tries to receive a second certificate for an overlapping time period.	
SCMS-1070	SCMS PoC out of Scope	Error code: raDuplicateRequest	RA shall log this error, if RSE 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: eeGlobalPolicyVerificationFailed	EE shall implement OEM defined error handling, if EE is not able to verify the digital	As the global policy file contains security relevant configuration it is essential	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			signature of the global policy file.	to verify if a recently downloaded version of that file is coming from a trustworthy source.		
SCMS-1189	SCMS PoC out of Scope	Trust Chain Broken - EE	EE shall not attempt to download a policy file If any component in the trust chain of the EE is revoked.	If the EE's ECA or other CA in the chain is revoked the EE shall not attempt to establish a connection to the RA. If an attempt is made, it will be unable to authenticate to the RA.	This is out of scope since it defines EE's behavior.	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 components (server) are only	This is out of scope since it defines	On-board Equipment (OBE), Road-side Equipmen

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			SCMS.	reachable by standard TCP/IP networking methods.	EE's behavior.	t (RSE)

17 issues

2.4.17 Use Case 18: Create / provide global, local and SCMS Manager policies

Target release	Release 1.0
JIRA Task	SCMS-490-Finish document "Create / provide global and local policies"Closed
Document owner	Tom Schaffnit
Reviewer	
QA	

2.4.17.1 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

2.4.17.2 Background and strategic fit

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

The SCMS Manager will then design 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 global policies directly affecting the EEs will result in an updated EE global policy file, which should then be downloaded by the EE whenever it next communicates with the SCMS. This is described in Step 18.3: Global Policies for EEs.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Any global or local policy changes directly affecting the EEs may be provided by the OEM, or other authorized manager of EE operations, 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: Local Policies for EEs.

2.4.17.3 Assumptions

-
  - The SCMS Manager develops and documents global policies
  - Global policies may include acceptable ranges within which local policy options may be set

2.4.17.4 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 global policy files using its complete security chain
  - The global policy files are mandatory sets of policies applicable to SCMS Components and EEs
  - There is a repository that includes global policies for all the different SCMS Components and EEs.
  - There is an EE global policy file that is conveyed to the EEs.
  - The global policy files are transferred to SCMS Components in a manner that is TBD. For PoC, the 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.

2.4.17.5 Step 18.1: Policy configuration options

Target release	Release 1.0
JIRA Task	SCMS-491-Finish document "Policy configuration options"Open
Document owner	Tom Schaffnit
Reviewer	Jeff Hahn
QA	

2.4.17.5.1 Configuration Options

Configuration options are available for global and local policy parameters.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

2.4.17.5.1.1 List of global configuration options

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
cert_chain_file_id	RA, PCA, EE	The Global Certificate Chain File (GCCF) version	This identifier is used by EE to determine if its version of the GCCF is up-to-date. If it does not match, the EE will request an update from the RA.	Y	2 bytes	Additional information on the GCCF File can be found in: Global Certificate Chain File.
la_identifier_size	EE	The size in bytes of LA identifier (la-id or LaId)	The size of the identifier used by EE to calculate linkage values of revoked certificates.	Y	2 bytes	The actual value of the identifier is included in CRL.
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 aren't trustworthy and	Y	2 weeks	This is not expected to be implemented in EEs for PoC, but should be included in the global file for PoC. There must be some

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
			rejecting all of them (and turning on an appropriate driver warning indicator).			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 =	Y	20	No maximum number capabilities; Note that CRL plan means that this can be

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
			week). This number is also the j-value. Currently that is 20 per week and this might change over time.			set no higher than 255.
cert_validity_model	RA, EE	Certificate validity model	Pseudonym certificates are either "concurrently" or "non-concurrently" valid.	Y	concurrent	This setting means that the 20 certs per week are all concurrently valid during that week; also affects CRL.
max_available_cert_supply	RA, PCA, EE	Maximum time with which to provision OBEs with pseudonym certificates	How many years worth of pseudo certs should be provided during the initial provisioning, and then maintained by top-off. For PoC it is currently 3 years.	Y	3 years	Affects ability to make major changes in the overall system; also affects size of CRL.

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
bytes_linkage_value	RA, PCA, LA, EE	Byte length of linkage values	The length in bytes of the linkage value (currently 9).	Y	9 bytes	Maximum value is 32 bytes due to SHA hash function.
bytes_group_linkage_value	RA, PCA, LA, EE	Byte length of group linkage values	The length in bytes of the group linkage value.	Y	9 bytes	Maximum value is 32 bytes due to SHA hash function.
max_group_size	RA, LA, EE	Maximum group size	The maximum number of EEs per group.	Y	4 bytes	Maximum value is 2^32. In the SCMS paper, the iterator is called "j".
max_number_of_groups	RA, LA, EE	Maximum number of groups	The maximum number of groups that is supported.	Y	4 bytes	Maximum value is 2^32.
bytes_linkage_seed	RA, LA, EE	Byte length of the linkage seed	The length in bytes of the linkage seed (currently 16).	Y	16 bytes	Maximum value is 32 bytes due to SHA hash function; also affects CRL.
bytes_group_linkage_seed	RA, LA, EE	Byte length of the group linkage seed	The length in bytes of the group linkage	Y	16 bytes	Maximum value is 32 bytes due to SHA hash

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
			seed.			function; also affects CRL.
shuffle_threshold	RA	Shuffle Threshold	Specifies the minimum number of Individual Certificate Requests to accumulate before shuffling and sending to PCA.	Y	1000	This is being considered as the minimum number for full privacy mode; Global sets acceptable option value limits; Local sets option value within Global limits.
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

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
						will be an infinite number; use of this option in deployment, if allowed, will require permission from the SCMS Manager.
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.

2.4.17.5.1.2 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

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
						sets acceptable option value limits; Local sets option value within Global limits.
certs_per_i_period	RA, LA, EE	The actual number of certificates per i-value. certs_per_i_value must be equal or larger than min_certs_per_i_value.	This is the actual number of certificates an EE receives. For POC, this is an RA setting (i.e. the setting is per RA, or possibly sub-RA, not necessarily per EE).	Y	20/40	Current plan is to use 20 as the main PoC value, but to test that 40 would also work; Note that CRL plan means that this can be set no higher than 255. All affected components and/or EEs do not necessarily need to be notified separately from the

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
						results of cert update requests.
address_la1	RA	Addresses of LA_1	Used to communicate with Linkage Authority 1.	Y		Local configuration to be approved by SCMS Manager?
address_la2	RA	Addresses of LA_2	Used to communicate with Linkage Authority 2.	Y		Local configuration to be approved by SCMS Manager?
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	TLS Certificate	X.509 certificate used for transport layer security.	Y		Local configuration
shared_key_update	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	TLS Certificate	X.509 certificate used for transport layer	Y		Local configuration

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Identifier	Affected Component	Configuration Option	Description	Required for PoC	Option Value for PoC	Comment
			security.			
tls_cert	LA	TLS Certificate	X.509 certificate used for transport layer security.	Y		Local configuration

2.4.17.5.2 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.

2.4.17.5.2.1 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).

2.4.17.5.2.2 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.

2.4.17.5.2.3 PoC

For PoC, only the format and delivery of this extended policy configuration file will be tested, but each identifier entry will have a single open-ended time span. This will be implemented for version 1.1.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

2.4.17.5.3 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 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 there shall 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 configuration options from the list of configuration options listed in 18.1 - Policy Configuration Options	shuffle_threshold and certs_per_i_period must be consistent throughout the SCMS in order to maintain nationwide interoperability; remaining local policies may be unique for particular components and	For PoC, these configuration options will be implemented manually.	

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				might be considered part of component configuration options, subject to SCMS Manager approval in most cases		
SCMS-632	SCMS PoC out of Scope	Additional local policies	Local policies, if any, other than those listed in 18.1 - Policy Configuration Options, may be implemented in the deployment design. Some of these additional local policies may be proprietary.	This requirement represents a place holder for the deployment design in order to allow for proprietary and/or as of yet undefined local policies to be administered by authorized EE or other component managers	This is out of scope for PoC. For the deployment design, local policies, if necessary, may be provided by OEMs, or other authorized managers of EE operations, to EEs in a proprietary manner. Also, local policies may be provided, as necessary, to EEs by their associated RA upon the EE's establishment of communications with the SCMS.	
SCMS-711	Manual Process	Valid PCA/ICA Certificate Chain List	The Global Certificate Chain File shall contain a list of all	EEs need to know all valid certificate chains in order to validate	The version ID is expected to be sequential, allowing the EE to check	

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
		File	valid certificate chains and a version ID	messages from other EEs and communicate with the SCMS	this version ID in the global policies file and determine if it is required to download a newer version of the Global Certificate Chain File For PoC, this file may be implemented manually (and is expected to be very small for PoC).	
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	SCMS	RA Timely	RA shall	It must be		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
-1349	PoC out of Scope	Limited Configuration Options	support the use of timely limited configuration options.	possible to 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

8 issues

2.4.17.5.4 ASN.1 Specification

- **scms-policy.asn** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/scms-policy.asn?at=refs/heads/master

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

2.4.17.6 Step 18.2: Local Policies for EEs

Target release	
JIRA Task	SCMS-492-Finish document "Local Policies for EEs"Closed
Document owner	Tom Schaffnit
Reviewer	Jeff Hahn
QA	

2.4.17.6.1 Background and strategic fit

It is the responsibility of the authorized managers of EE operations to properly configure EEs. 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. It is anticipated that the RA will then be required to send its particular integrated policy file to the PG for approval and signing by the PG prior to making it available to the EEs within its jurisdiction. This arrangement will allow the EEs to only download and process a single policy file that contains all the global policy and local policy fields relevant to that EE. However, this is out-of-scope for PoC.

2.4.17.7 Step 18.3: Global Policies for EEs

Target release	Release 1.0
JIRA Task	SCMS-493-Finish document "Global Policies for EEs"Closed
Document owner	Andre Weimerskirch
Reviewer	
QA	

2.4.17.7.1 Goals

- Provide global policies that are valid for all EEs

2.4.17.7.2 Background and strategic fit

This policy is applied to all EEs and can be flexible in terms of distribution (e.g. out-of-band, PKI security management, etc). The distribution mechanism should be flexible to allow optional push mechanism. The minimum security requirements for this distribution are out-of-scope for PoC.

2.4.17.7.2.1 Assumptions

- The global policies relevant for EEs, as listed in Section 18.1, will be included in the Global Policy File (GPF).
- The GPF will be distributed to all RAs

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

- 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 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.
- Changes to the global policies that affect EEs will be conveyed to all EEs through an updated LPF.

2.4.17.7.3 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-629	SCMS PoC out of Scope	SCMS Version	The global policy shall be capable of changing the SCMS version (see global policy parameters in 18.1 - Policy Configuration Options)	Major changes in the SCMS over time may be require; this SCMS version designation would indicate such a major change in the system	Out-of-scope for PoC as it is not intended to change version during PoC deployment	PG
SCMS-633	Manual Process	Global Policy Distribution	RA shall have mechanisms to receive signed global policy files from the Policy Generator (PG).	The SCMS Manager develops and documents global policies, prepares appropriate global policy files for EEs and	Other authorized EE managers (such as OEMs) may also need to have mechanisms to receive signed global policy files from the PG in order to provide these files to EEs using for out-of-band communication. This might be a manual process for PoC.	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				signs them within its Policy Generator function; RAs need to have these files to convey them to the EEs		
SCMS-634	Implemented	Global policy ID	The global policy shall have a unique identifier	The global policy file is expected to be updated at intervals; the unique identifier supports version control	A sequential approach would likely facilitate use of this identifier for version control	PG
SCMS-635	Implemented	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-	Implemented	Activation	The global policy shall have an	The activation time	This helps to provide an orderly implementation of changes to global	PG

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
636		time	activation time	determines at what point in time any changes in the global policy file should be implemented	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.	
SCMS-637	Implemented	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	Review	Duplicate Entries	The RA shall ensure that the field entries in the local policy files that it provides to the EEs within its jurisdiction	Local policies need to be set within the allowable global policy	For OBE, won't be tested in POC; likely to be implemented as a manual process in PoC on RA side.	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			(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.	range		
SCMS-639	Implemented	Local Policy Entries	The global policy shall allow inclusion of the local policy fields, to provide a mechanism to override local policy fields for all vehicles in the SCMS system.	Allows for global policy to specify local policy fields, as require, in cases where consistency needs to be established	For OBE, won't be tested in POC; likely to be implemented as a manual process in PoC	PG
SCMS-640	SCMS PoC out of Scope	Field sizes for SCMS protocols and SCMS datatyp	The global policy shall be capable of changing the field sizes for SCMS protocols and SCMS data	Technological evolution may require longer field sizes for global	Out-of-scope for PoC	PG

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
		es	types (see global policy parameters in 18.1 - Policy Configuration Options)	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

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-642	Manual Process	Overdue CRL tolerance	The global policy shall be capable of specifying overdue_CRL_tolerance as a time period. Likely to be implemented as a manual process in PoC.	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
SCMS-643	Manual Process	Global policy Root CA certificates	The global policy shall be capable of updating the root CA certificate(s) (see global policy parameters in 18.1 - Policy Configuration Options). This will likely be accomplished over proprietary, out-of-band communications with the	It is necessary to have an established process with which to update the root CA certificate in the event of expiration or root compromise	Automated process is out-of-scope for PoC; likely to be implemented as a manual process in PoC	PG

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			authorized managers of the respective EEs' operations. Likely to be implemented as a manual process in PoC.			
SCMS-710	In Implementation	Global Certificate Chain file - Current Version ID	The global policy file shall include the version ID, certChainFileId, of the current Global Certificate Chain file.	The EE needs to have the currently valid list of certificate chains in order to validate messages received from EEs using signatures with certificate chains different than its own and for other trusted communications with the SCMS.	This ID is implemented as a versioning indication, so that the RA can update its own Local Certificate Chain File, as necessary. The EEs can use this indication in the LPF to check if the version of the Local Certificate Chain file that it already has is the most current version of the list. After receiving a LPF, the EEs need to check to see if they have the most recent list of valid certificate chains. If this ID field indicates that there is a more recent version than that which the EE has in its storage, then the EE will need to request a download of the newer local certificate chain file (see also Section 3.1 and https://jira.campllc.org/browse/SCMS-767~~SCMS-767~~; Section 9.1 and SCMS-713; (possibly additional sections). OBE portion won't be tested in POC, but will generate EE requirements for	PG

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
					deployment.	
SCMS-1403	Review	RA shall provide the policy file (LPF) to EE in OER and XML format	RA provides the policy file to EE in OER and XML format.	To offer the two most common encoding formats.		RA

2.4.17.7.4 Design

2.4.17.7.4.1 EE Global Policy Updates

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.

2.4.17.7.4.2 EE Global Policy Naming Convention

The global policy file(s) found in the EE device specific repository shall be named according the following format:

- gp_X_Y.Z
    - where
    - X is the policy ID, up to 32 octets in case insensitive hexadecimal (this could be a truncated SHA-256 hash of policy file content)
    - Y is the i-value in case insensitive 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
        - xml

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Note: It is recommended for the RA to provide all the above formats available to the EEs, or at least the OER format.

2.4.17.8 Step 18.5: Generate Global and Local Certificate Chain File

Target release	Release 1.1
JIRA Task	
Document owner	Biswajit Panja
Reviewer	
QA	

2.4.17.8.1 Goals

The Global Certificate Chain File (GCCF) shall contain chain of PCA certificates (it will include root CAs, ICAs, PCAs). For a given EE, RA creates Local Certificate Chain File (LCCF) that contains at least all the PCA cert chains that are used to issue pseudonym certs for that EE (this is to support P2P cert distribution). Optionally, RA could choose to provide other PCA cert chains in the LCCF. Note, if the RA chooses to provide additional information beyond the additional PCA certificate chains from the GCCF to the EE, this can be done in a proprietary method. Any EE connecting to its associated RA shall get LCCF along with certificates (issued by a PCA) from that RA. For POC all content in GCCF will be contained in the required section of LCCF. For POC these files will be created manually. GCCF and LCCF are not signed.

Example: Let's say for a particular EE, RA uses PCA1 and PCA2 for generating its pseudonym certificates. RA must provide cert chains for PCA1 and PCA2 to EE, but RA can choose to provide cert 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 cert distribution protocol

2.4.17.8.2 Access & Download

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

The files will be downloaded via a HTTP get request, synonymous with the mechanism used to download the PCA certificate batch files.

2.4.17.8.3 Format

The GCCF shall be named according to the following format:

- global_certificate_chains_<globalversion>.abc, where abc is the encoding format.

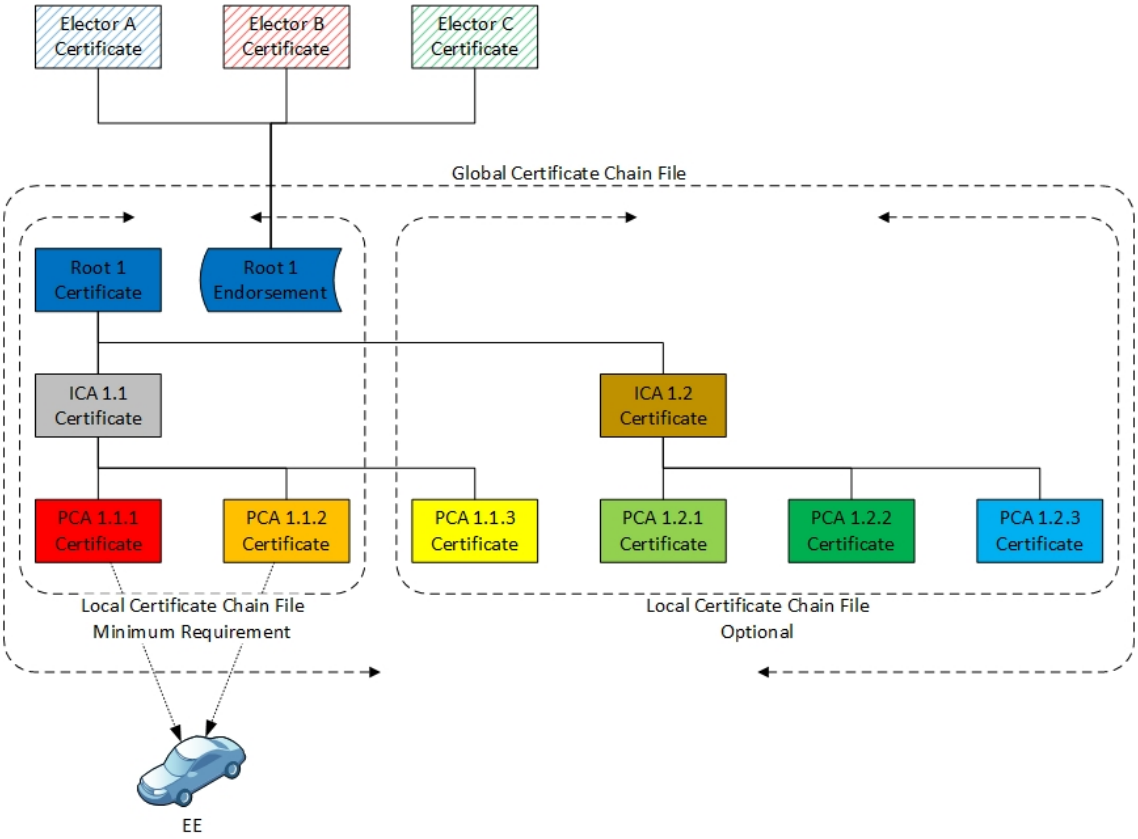
The LCCF shall be named according to the following format:

- local_certificate_chains_<globalversion>_<localversion>.abc, where abc is the encoding format

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

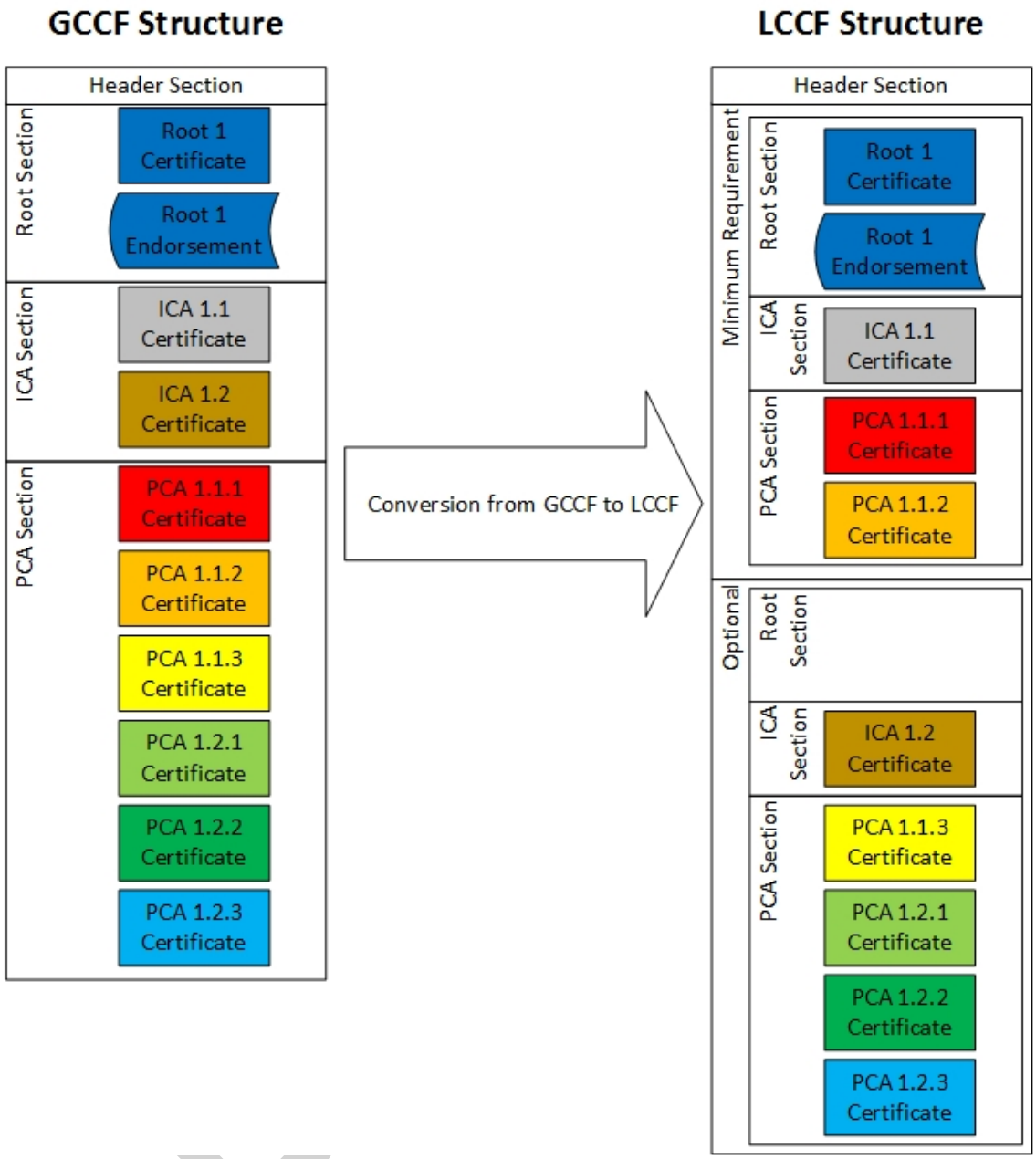
Note, it is assumed all URLs and file names are case-insensitive. The <globalversion> should match the parameter cert_chain_file_id found in the Global Policy File.

The following diagram shows the relationship between GCCF and LCCF. Note that GCCF and LCCF do not contain Elector certificates but they do contain ballots endorsing each root.



The following diagram shows the structure of GCCF and LCCF.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary



Global Certificate Chain File (GCCF) Generation:

GCCF is created by the policy generator and given 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 information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

2.4.17.8.3.1 Creation of Local Certificate Chain File(LCCF)

LCCF is created by the RA and given to all EEs whenever there is an update. For the POC the creation of LCCF is a manual process. It is upto OEMs to decide whether they want to use GCCF or create LCCF from it.

2.4.17.8.3.2 Use cases affected

1. Component setup
2. Bootstrap
    a. During bootstrap the device gets all the necessary certs, ECA, RA, MA and LCCF
3. Pseudonym certificate download
    a. RA provides the updated LCCF
4. Back end management
5. RSE bootstrap
6. RSE certificate download

2.4.17.8.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-768	In Implementation	RA - Global Certificate Chain File	RA shall provide a Global Certificate Chain File and a Local Certificate Chain File for download by EEs.	to enable EEs to verify certificates without further CA certificate downloads. If the Global Policy File indicates a new version of the Global Certificate Chain File than that existing	For more information: Global Certificate Chain File	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				on the EE, the EE will need to download it and apply it.		
SCMS-1062	Review	PG Update Global Certificate Chain File	The Policy Generator shall update the GCCF and remove all chains containing the revoked certificate as soon as it receives the "Revoke Root CA" message.	Having an updated GCCF makes verification processes at EEs more efficient.		PG
SCMS-1351	Review	Certificates of Global Certificate Chain File (GCCF)	PG shall generate a Global Certificate Chain File that contains chains of all PCA certificates including Root CAs,	The GCCF contain PCA cert chains for all SCMS instances. GCCF is created by policy generator and given to all RAs		PG

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			ICAs and PCAs.	whenever there is an update.		
SCMS-1352	Review	Local Certificate Chain File (LCCF) generation	PG shall create for a given EE a Local Certificate Chain File that contains at least all the PCA cert chains that are used to issue pseudonym certs for that EE (this is to support P2P cert distribution).	this is to support P2P cert distribution.	Each RA creates its own LCCF that only contains PCA cert chains for that particular SCMS instance. Optionally, RA could choose to provide other PCA cert chains in the LCCF.	PG
SCMS-1354	Review	Version number in GCCF and LCCF	The Policy Generator shall include a version number in the GCCF that is also included in all the	Version number is required to maintain re-freshness of GCCF and LCCF	Example: filename.globalversion.localversion	PG

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			LCCF, and each LCCF will additionally have its own version number.			
SCMS-1355	Review	GCCF and LCCF generation in POC	PG shall put all content in 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.	PG

6 issues

2.4.17.8.5 ASN.1 Definition

The content of the file shall be specified in ASN.1 and encoded with COER and shall have the following structure:

- **scms-policy.asn [102:]** https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/scms-policy.asn?at=refs/heads/master

2.4.18 Use Case 19: OBE Identification Certificate Provisioning

Target release	Release 1.1
JIRA Task	SCMS-1232Open
Document owner	Andre Weimerskirch
Reviewer	
QA	

This is TBD for Release 1.1

2.4.18.1 Goals

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

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

2.4.18.2 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, and revocation is enabled by adding individual identification certificates to the CRL. 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.

2.4.18.3 Assumptions

- The OBE is assumed to have a valid enrollment certificate that empowers it to request OBE identification certificates.
- RSE is assumed to have Root CA, RA and PCA certificates.
- RSE is assumed to have relevant address(s) to communicate with the RA.

2.4.18.4 Design

The mechanism is a mixture of the pseudonym certificate use-case and the RSE application use-case. The use-case works as follows:

- Initial request
    - EE creates a signature butterfly key (B_i)
    - Optional: EE creates an encryption key EK (but not Butterfly encryption key)
    - EE provides the signature butterfly key to RA. EE optionally provides the encryption key to RA.
    - RA creates butterfly keys based on the policy (either policy linked to EE and/or PSID; e.g. 1 cert per month for 12 months, no significant overlaps).
    - 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 signature butterfly key B_i, RIF, and optionally EK.
    - PCA issues the certificate using B_i and RIF. If EK was provided, PCA encrypts the issued certificate with EK.
    - RA collects PCA's responses, bundles them in a file, and stores it in a folder.
    - EE can now download the file.
- Top-up

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

- RA regularly checks and will initiate generation of certificates as needed and defined in the policy, using the Butterfly signature key.
- RA will look-up RIF, and send butterfly keys B_i and RIF to PCA. If EE originally provided an EK, RA will include EK.
- PCA issues certs and, if EK was provided, encrypt to EE.
- RA collects PCA's responses, bundles them in a file, and stores it in a folder.
- EE can now download the file.

This use-case is divided into the following steps

1. Step 19.1: Request for OBE Identification Certificates
2. Step 19.2: OBE Identification Certificate Generation
3. Step 19.3: Download of OBE Identification Certificates
4. Step 19.4: Schedule generation of subsequent batch of OBE identification certificates
5. Step 19.7: Download new OBE identification certificates

2.4.18.5 JIRA Items

2.4.18.6 Step 19.1: Request for OBE Identification Certificates

Target release	
JIRA Task	SCMS-1230Open
Document owner	Rekha Singoria
Reviewer	
QA	

This is TBD for Release 1.1

2.4.18.6.1 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.

2.4.18.6.2 Background and Strategic Fit

The OBE decides to request identification certificate from an RA, based on policy set by the SCMS Manager. The OBE may optionally contact DCM-R to determine which RA to submit the request to, or this information may be pre-configured.

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.

Two types of requests occur in the certificate provisioning process:

1. From OBE to RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

2. From RA to PCA (see Step 19.2: OBE Identification Certificate Generation for details)

2.4.18.6.3 Prerequisites and Assumptions

In order to facilitate the certificate request process, the following prerequisites should be met:

- The OBE shall have successfully completed the bootstrap process (OBE bootstrapping)
- The OBE shall know the current network address of the RA

2.4.18.6.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-507	Implemented	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 issued any more certificates	Every logical RA has its own internal blacklist that is not shared with anyone else.	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 since it defines EE's behavior.	On-board Equipment (OBE)
SCMS-521	Closed	Acknowledge request	RA shall acknowledge the receipt of EE's request with a TCP ACK within a specified amount of time, currently set to be 1 sec.	so that EEs know that their request was received by the RA.		RA
SCMS-522	SCMS PoC out of Scope	Retry request	If the EE doesn't receive acknowledgement (TCP ACK) within a specified amount of time, currently set to be	to ensure that the request is received by the RA.	This is out of scope since it defines EE's	On-board Equipment (OBE), Road-

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			2 sec from the time of request, it shall retry.		behavior.	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	Certificate Provisioning Request with the RA for a minimum of 60 minute after 10 consecutive failed communication attempts resulting in no acknowledgement (TCP ACK) or no Certificate Provisioning Response	This is out of scope since it defines EE's 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 in case it has changed, see EE →RA _ RA Certificate Request, EE →RA _ RA Certificate Response	so that EE can encrypt the request to the right RA	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SC	SCMS	Sign certificate	The EE shall sign	so that RA	This is	On-

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
MS-754	PoC out of Scope	request	certificate requests with its enrollment certificate.	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	out of scope since it defines EE's behavior.	board Equipment (OBE), Road-side Equipment (RSE)
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's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-986	Review	Error code: raNoInitialRequest	RA shall log "Error code: raNoInitialRequest", if this is not the OBE's initial request for pseudonym certificates and it is not a request with changed parameters.	Proper parameters are required to start the certificate provisioning process, otherwise there is already an existing request and pseudony	If this is the first request by the OBE then RA shall start certificate provisioning. RA shall	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				m certificates get pre-generated.	follow initial provisioning If a device makes a request with different parameters then RA shall begin preparing the processing of certificate. RA shall follow update pseudonym certificate provisioning	
SCMS-987	In Implementation	Error code: eeWrongParameters	RA shall log "Error code: eeWrongParameters", if a device sends request with wrong parameters.	to enable server side diagnostics and to avoid giving potential attackers relevant informatio		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				n		
SCMS-988	In Implementation	Error code: eeRetries	RA shall log "Error code: eeRetries", 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: moreThanAllowedTries	RA shall return status code HTTP 500, if the EE makes more than n retries within the time specified in SCMS-523, and log "Error code: moreThanAllowedTries".	More than n tries not allowed		RA
SCMS-1012	In Implementation	Error code: eeWrongGlobalPolicyParameter	RA shall log "Error code: eeWrongGlobalPolicyParameter", 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	A request with wrong parameters might be an indication for misbehavior.	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				ranges for the overall system that all participants in the system need to follow.		
SCMS-1082	In Implementation	Error code: eeInvalidSignature	RA shall log "Error code: eeInvalidSignature", if the EE doesn't 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: eeRequestNotEncrypted	RA shall log "Error code: eeRequestNotEncrypted", if the EE doesn't encrypt the certificate request using the RA's 1609 certificate.	to enable server side diagnostics and to avoid giving potential attackers relevant information	A unencrypted certificate request might be an indication for misbehavior.	RA
SCMS-1084	In Implementation	Error code: eeInvalidCredentials	RA shall log "Error code: eeInvalidCredentials", if the EE has invalid credentials (blacklisted, expired, unauthorized)	to enable server side diagnostics and to avoid giving potential attackers relevant	A request with invalid credentials might be an indicati	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				information	on for misbehavior.	
SCMS-1085	In Implementation	Error code: eeUnauthorizedRequest	RA shall log "Error code: eeUnauthorizedRequest", 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: eeMalformedRequest	RA shall log "Error code: eeMalformedRequest", 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: eeRaMismatch	RA shall log "Error code: eeRaMismatch", 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

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-1088	In Implementation	Error code: eeInvalidTime	RA shall return status code HTTP 500, if the EE has an invalid system time, and log "Error code: eeInvalidTime".	to avoid EEs using the invalid certificates		RA
SCMS-1204	Implemented	Check blacklist	RA shall reject EE request, if EE is listed on its blacklist.	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 informatio		RA

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				n (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-1278	Review	Certificate availability for download	RA's acknowledgement (https://jira.campllc.org/browse/SCMS-521~~SCMS-521~~) shall contain a time when the certificate will be available for download.	so that RSE can download the certificate in a timely manner.		RA
SCMS-1397	Review	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 and not provide	• Standard TCP (SCMS	ECA, RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				useful information to malicious actors.	-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	

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

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	Review	RA accept HTTP post over TCP/IP	RA shall accept HTTP post requests 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 This is out of scope as it defines EE behavior.	RA

2.4.18.7 Step 19.2: OBE Identification Certificate Generation

Target release	
JIRA Task	SCMS-1231Open

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Document owner	Rekha Singoria
Reviewer	
QA	

This is TBD for Release 1.1

2.4.18.7.1 Goals

Generate OBE identification certificates in a secure way.

2.4.18.7.2 Background and Strategic Fit

- For each certificate request by RA, PCA generates a valid identification certificate, encrypts the certificate for the OBE specified in the request, signs the encrypted packet, and sends it to RA
- RA makes the certificate available for download by the OBE
- PCA stores the certificate and hash of the RA-PCA certificate request for future misbehavior investigation and revocation purposes

The PCA and the RA store all information in a database. This information is only required for revocation and differs from one entity to another. Any information that is stored for revocation needs to be stored for 10 years. Any information that needs to be stored for device's lifetime will be stored for 40 years.
The PCA stores:

- A hash of the certificate request (to enable internal blacklisting at the RA)
- The certificate and its hash truncated to eight bytes, CertID8 (to allow the MA to request something from the PCA even if it gets only the digest of the certificate.)
- Validity period of the certificate (start and end times)

The RA stores:

- A hash of the certificate request. This value will be used by the MA to instruct the RA which enrollment certificate to put on the internal blacklist.
- The corresponding enrollment certificate
- Validity periods for requests for a given enrollment certificate

2.4.18.7.3 Assumptions

- RA and PCA complete all necessary sanity checks and signature verification before fulfilling with certificate provisioning request.

2.4.18.7.4 Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCM	Revie	PCA issues implicit	PCA shall	To save		PCA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
S-1304	w	certificates	issue implicit OBE enrollment, pseudonym, and OBE identification certificates, rather than explicit certificates.	storage space and over-the-air bytes		
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 cert to an OBE valid at a time for a given application.	There is no need for privacy (by definition).		PCA, RA
SCMS-1370	Review	Certificate Validity	RA shall request PCA to generate identification certificates with validity TBD by a time t overlap , which is	t overlap to 1 hour (60 minutes) reduces the risk of a vehicle operating without a valid		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			currently set to be 1 hour.	certificate.		
SCMS-1372	Review	PSID/SSP assignment to certificates	RA shall read the set of PSID/SSP values of the enrollment certificate that was used for the certificate request and use the exact same set request OBE and RSE certificates during provisioning.	PSID/SSPs shall be assigned in groups such that corresponding applications are similar in nature.		RA

5 issues

2.4.18.8 Step 19.3: Download of OBE Identification Certificates

Target release	
JIRA Task	SCMS-1233Open
Document owner	Andre Weimerskirch
Reviewer	
QA	

This is TBD for Release 1.1

2.4.18.8.1 Goals

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

2.4.18.8.2 Background and strategic fit

The purpose of this exchange is to provide a defined method that a certified EE can use to download OBE identification certificates. These credentials will be used for V2I applications. The download will include (1) file(s) that include one certificate each, (2) a .info file that includes the time when new certificates will be available and (3) a global certificate chain file containing all PCA certificate chains required to validate the identification certificates, but not the policy file.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

2.4.18.8.3 Assumptions

1. The EE will abandon further interactions with the RA after a certain number of failed communication attempts resulted in critical errors.
2. The EE will not attempt to execute the certificate provisioning process if it finds itself on the latest CRL (assumes that the device has not been compromised by a willful violator). The device will need to execute the certification/bootstrap process again to exit a revoked state.
3. The EE may terminate the download process if sufficient storage is not available for subsequent batches.
4. RA issued certificates and stored them in a folder on RA for EE to download.
5. The Global Certificate Chain File has been downloaded and processed into the trust-store of the EE (necessary for PCA Certificate Validations).
6. The Global Certificate Chain File is being actively monitored by the EE for updates as described in Step 3.1: Check for policy updates.

2.4.18.8.4 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)
SC	In	OCSP: Stapled for	The RA shall	Most	OCSP stapling	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
MS-459	Implementation	RA to OBE	respond to an OBE request for an OSCP stapled certificate.	OBEs do not have access to CRL updates, so the RA must provide an OCSP stapled response so that the OBE can validate the RA's TLS certificate.	provides improved performance compared to CRLs. OCSP stapling is specified in RFC 6066, Section 8. 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). The RA will be able to respond to the OBE's request for an OSCP stapled certificate. The RA itself will be able to request OCSP certificate currency from an OCSP server in order that it (the RA) is assured of the other components TLS cert currency, so it will require the OCSP request URL and credentials.	
SCMS-513	Closed	RA downloads via TCP/IP	RA shall provide downloads over TCP/IP.	to utilize standard internet protocols for the	Downloads could be e.g. policy file, Global Certificate Chain File, certificates, .info file etc.	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				download process.		
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 certs currently. Instead the OBE will use TLS to authenticate the other endpoint (as a server) and will use its SCMS cert to identify itself. EE authenticates via its IEEE 1609.2 enrollment certificate. The details of the authentication process are defined	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
					Step 3.4: Download of Pseudonym Certificates	
SCMS-517	In Implementation	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-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-	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	On-board Equipment (OBE), RA, Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				encrypted pseudonym certificates (adversary might extract Butterfly encryption keys from junked vehicle at a later stage and is then able to identify all EE certificates).	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	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				enrollment certificate to a malicious RA. RA authenticates via its TLS X.509 certificate. The details of the authentication process are defined in Step 3.4: Download of Pseudonym Certificates.		
SCMS-541	SCMS PoC out of Scope	OCSP stapling - EE	The EE may use the TLS Certificate Status Request extension (OCSP stapling) to verify RA revocation status.	Revocation is optional and it's up to the OEMs support it.	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	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
					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	to improve reliability of the download protocol.		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			switches the IP address.			
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 life-time of the SCMS. It might even vary for different EEs.		RA
SCMS-548	Closed	X.info file	RA shall provide an .info file for download by EE.	The .info file provides information when new pseudonym certificates, or identification certificates, can be downloaded.	see Certificate Batch Download for more information.	RA
SCMS	Closed	Keep Certs	The RA shall allow the EE	to recover		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
- 549			to download certificates that have previously been downloaded, so long as the devices credentials are still valid and the certificates are not expired.	from a loss of certificates at the device level (e.g., disk corruption).		
SCMS - 958	SCMS PoC out of Scope	Error code: eeConnectionFailed	EE shall log this error in its log file, 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 provide this error code to EE, if certificate batch is not available.	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's corrupted), OBE shall	to enable EE side diagnostics.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			implement OEM defined error handling and store the error code in OBE's error log file.			
SCMS-966	SCMS PoC out of Scope	Misbehavior reporting: 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's 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-969	SCMS PoC out of Scope	Error code: eeCertificateFileDecryptionFailed	EE shall implement OEM defined error handling and store the error code in EE's error log file, 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 reporting: eeCertFileDecryptionFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to decrypt an encrypted	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			certificate.			
SCMS-971	SCMS PoC out of Scope	Error code: eeCertificateVerificationFailed	EE shall implement OEM defined error handling and store the error code in EE's error log file, 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 reporting: 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 implement OEM defined error handling and store the error code in EE's error log file, 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-	SCMS PoC out of	Misbehavior reporting: eeCertContentFalse	EE shall initiate a misbehavior	to enable server	This is out of scope since it defines EE's behavior.	On-board Equip

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
974	Scope		report to MA with the observed error, if EE is not able to parse a certificate, or if the certificate has wrong content.	side misbehavior detection.		ment (OBE), Road-side Equipment (RSE)
SCMS-976	In Implementation	Error code: raInvalidURL	RA shall log this error code, 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	Error code: raNoTLS	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 this error, if EE-to-RA authentication fails.	to enable server side diagnostics and to avoid		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				giving potential attackers relevant information.		
SCMS-979	SCMS PoC out of Scope	Error code: eeAuthenticationFailed	EE shall store this error code in EE's error log file, 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 reporting: 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 this error, if Global Certificate Chain File is not available.	to enable client side error handling.		RA
SCMS-982	Implemented	X.info file update period	RA shall update the .info file at least on a weekly basis.	The .info file is updated regularl		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				y to provide timely updates to EE		
SCMS-983	In Implementation	Error code: raNoInfoFileAvailable	RA shall return this error code, if it is not able to provide a current .info file.	to enable EE side error handling.	This information is probably provided by an entry in the .info file	RA
SCMS-984	SCMS PoC out of Scope	Error code: eeInfoFileDownloadFailed	OBE shall implement OEM defined error handling and store the error code in its error log file, if OBE is not able to download the .info file (e.g. because there is none or it's 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 reporting: eeInfoFileDownloadFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to download the .info file (e.g. because there is none or it's corrupted).	to enable server side misbehavior detection.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)
SC	In	Error code:	RA shall	in order		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
MS-1090	Implementation	rseRaTcpErrors	return standard TCP error codes if TCP errors occur.	to enable client side error handling.		
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 since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCMS-1203	Implemented	Check time stamp	RA shall check the signed (by EE) time-stamp and allow a tolerance of 5 seconds.	If the difference between the signed time-stamp and the current time is 5 seconds or less, RA will proceed with the authentication process. Otherwise RA will reject the		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				connection.		
SCMS-1204	Implemented	Check blacklist	RA shall reject EE request, if EE is listed on its blacklist.	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		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				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.		
SC	SCMS	OBE downloads	OBE shall	The	This is out of scope	On-

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
MS-1214	PoC out of Scope	.info file	download the .info file each time OBE tries to download pseudonym certificates.	.info file lists the time when pseudonym certificates will be available next time. EE downloads that file each time it tries to download pseudonym certificates.	since it defines EE's behavior.	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.	Whenever EE tries to download certificates, it also downloads the .info file. EE will contact RA again to downlo	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				ad certificates after the time listed in the .info file.		
SCMS-1228	Review	OBE identification certificate files	RA shall store each identification certificate to be downloaded by EE in a file X_i.tar in a specific folder known to EE. 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.	There is one OBE identification certificate per file. The files are stored in a folder known to EE, and EE then uses standard file transfer mechanisms to download the file(s).	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.tar, the second certificate is stored in X_2.tar, the 4 billion-th certificate is stored in X_EE6B2800.tar, and so on.	RA
SCMS-1263	SCMS PoC out of Scope	EE download resume	EE shall try byte-wise resume of CRL downloads from the CRL store,	This will improve reliability of the download		On-board Equipment (OBE), Road-side

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			certificate batches, certificate files, or policy files from RA in case a previous download failed.	process and reduce communication cost.		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-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 certifica	Whitelist defined in SCMS-1371	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				tes or files.		

44 issues

2.4.18.8.5 Design

- Step 1: EE and RA authenticate to each other, see Step 3.4: Download of Pseudonym Certificates.
- Step 2: EE downloads the global certificate chain file (see file definition in Global Certificate Chain File).
- Step 3: EE downloads certificate files X_i.tar, 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.tar, or as many as possible. Each X_i.tar includes a single identification certificate.
- 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 1609 format 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).

2.4.18.9 Step 19.5: Refresh OBE Identification Certificates

Target release	
JIRA Task	SCMS-1287Open
Document owner	Andre Weimerskirch
Reviewer	
QA	

2.4.18.9.1 Goals

- The goal of refreshing the OBE identification certificates to ensure that the OBE has a constant supply of certificates and related policy information. This is accomplished by periodically connecting to the RA to download policy updates and pseudonym certificates.

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

2.4.18.9.2 Background and strategic fit

OBEs are not assumed to have constant or frequent connection to the SCMS system. Therefore, certificates will be pre-generated and available to download for a significant amount of time into the future.

2.4.18.9.3 Assumptions

- The OBE has successfully completed the enrollment process.
- The OBE has the .info file from a previous download from the RA.

2.4.18.9.4 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-513	Closed	RA downloads via TCP/IP	RA shall provide downloads over TCP/IP.	to utilize standard internet protocols for the download	Downloads could be e.g. policy file, Global Certificate Chain File, certificates, .info file etc.	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				process.		
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 certs currently. Instead the OBE will use TLS to authenticate the other endpoint (as a server) and will use its SCMS cert to identify itself. EE authenticates via its IEEE 1609.2 enrollment certificate. The details of the authentication process are defined Step 3.4: Download of Pseudonym Certificates	RA
SCMS-517	In Implementation	Tunneling through LOP	RA shall provide downloads only via a LOP hardware interface,	to anonymize the location of EEs.		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			which removes all location information from the incoming request.			
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 in Step 3.4:	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				Download of Pseudonym Certificates.		
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-958	SCMS PoC out of Scope	Error code: eeConnectionFailed	EE shall log this error in its log file, 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 this error code, if EE requests invalid	to enable server side diagnostics and to avoid giving	This is not in ASN.1 but http 404	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			URL.	potential attackers relevant information		
SCMS-977	In Implementation	Error code: raNoTLS	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 this error, 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 store this error code in EE's error log file, 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 reporting: eeAuthenticationFailed	EE shall initiate a misbehavior report to MA	to enable server side misbehavior	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE),

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			with the observed error, if RA-to-EE authentication fails.	detection.		Road-side Equipment (RSE)
SCMS-1196	SCMS PoC out of Scope	Stored .info file	OBE shall have a .info file stored from the previous connection to the RA.	The .info file is used to determine the next allowed connection attempt.	This is out of scope since it defines OBE's behavior.	On-board Equipment (OBE)
SCMS-1203	Implemented	Check time stamp	RA shall check the signed (by EE) time-stamp and allow a tolerance of 5 seconds.	If the difference between the signed time-stamp and the current time is 5 seconds or less, RA will proceed with the authentication process. Otherwise RA will reject the connection.		RA
SCMS-	Implemen	Check	RA shall reject EE	If EE is listed, RA		RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
1204	ted	blacklist	request, if EE is listed on its blacklist.	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,		

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				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-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

17 issues

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

2.4.18.10 Step 19.6: Request updated policies

Target release	
JIRA Task	
Document owner	Andre Weimerskirch
Reviewer	
QA	

2.4.18.10.1Goals

- The policy download mechanism is required to ensure that the OBE is always using the latest policy for new downloaded certificate batches. The ongoing download of the policy files is identical to the initial policy download process as described in Step 3.1: Check for policy updates from the SCMS point of view.

2.4.18.10.2Background and strategic fit

From an EE point of view the download time is controlled by the .info file that was downloaded from the RA the previous time.

2.4.18.10.3Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-512	Closed	Global Policy file	RA shall always provide a global policy file available for download by EE	There is always a global configuration available, and that configuration shall be current		RA
SCMS-709	SCMS PoC out of Scope	Check for 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	• If no policy file is available on the EE, the EE is allowed to make	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
				certificates. Policy definition details are available at Use Case 18: Create / provide global and local policies.	a download attempt at any time. • This is out of scope since it defines EE's behavior.	
SCMS-767	SCMS PoC out of Scope	Check for Certificate Chain Updates	EE shall check for version changes in 'certChainFileId' field of the Global Policy file. If the version is different than that of its existing file, it will take action to update it.	As CAs are added, removed, revoked, or rolled-over, new certificate chains will have to propagated to EEs and other SCMS components. For more information: Global Certificate Chain File	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)
SCM	SCMS	Error code: eeGlobalPolicyFileDownloa	EE shall implement	As the global	This is out of	On-board Equipment

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
S-952	PoC out of Scope	dFailed	OEM defined error handling and store the error code in EE's error log file, if EE is not able to download the global policy file (e.g. because there is none or it's corrupted).	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.	scope since it defines EE's behavior.	(OBE), Road-side Equipment (RSE)
SCMS-953	SCMS PoC out of Scope	Misbehavior reporting: eeGlobalPolicyFileDownloadFailed	If EE is not able to download the global policy file (e.g. because there is none or it's corrupted), EE 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), Road-side Equipment (RSE)
SCM	SCMS	Error code: eeGlobalPolicyVerification	EE shall implement	to enable EE side	This is out of	On-board Equipment

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
S-954	PoC out of Scope	Failed	OEM defined error handling and store this error code in EE's error log file, if EE is not able to verify the digital signature of the global policy file.	diagnostics.	scope since it defines EE's behavior.	(OBE), Road-side Equipment (RSE)
SCMS-955	SCMS PoC out of Scope	Misbehavior reporting: eeGlobalPolicyVerification Failed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify the digital signature of the global 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: eeGlobalPolicyFileParsingFailed	EE shall implement OEM defined error handling and store this error code in EE's error log file, if EE is not able to parse the successfully downloaded global policy	As the global 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)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			file (e.g. because it's corrupted).	important to have an error handling whenever the EE is not able to read the latest version of that file.		
SCMS-957	SCMS PoC out of Scope	Misbehavior reporting: eeGlobalPolicyFileParsingFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to parse the successfully downloaded global policy file (e.g. because it's 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-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 download a policy file If any component in the trust chain of the	If the EE's ECA or other CA in the chain is revoked the EE shall not	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			EE is revoked.	attempt to establish a connection to the RA. If an attempt is made, it will be unable to authenticate to the RA.		
SCMS-1353	SCMS PoC out of Scope	EE gets LCCF from RA	EE shall check for and download policy an updated Local Certificate Chain File (LCCF) or Global Certificate Chain File (GCCF) 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 cert. This is out of scope since it defines EE's behavior	On-board Equipment (OBE), RA, Road-side Equipment (RSE)
SCMS-1356	SCMS PoC out of Scope	LCCF validation in EE	EE shall use the Local or Global Certificate Chain File (LCCF/GCCF) to validate	EEs need to be able to validate received SCMS certificates based on their	EE doesn't need to store all certificate chains, the LCCF provides	On-board Equipment (OBE), Road-side Equipment (RSE)

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
			received SCMS certificates and respond to P2P certificate requests.	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.	the minimum set and EEs can learn additional chains via P2P certificate request. This is out of scope since it defines EE's behavior	

13 issues

2.4.18.10.4User interaction and design

- Step 1: EE will use .info file from the last certificate batch download to determine the time a download can be attempted.
- Step 2: EE and RA authenticate to each other.
- Step 3: EE downloads the policy file.

2.4.18.11 Step 19.7: Download new OBE identification certificates

Target release	
JIRA Task	SCMS-1235-Finish Step 19.5: Download new OBE identification certificatesOpen
Document owner	Andre Weimerskirch
Reviewer	
QA	

This is TBD for Release 1.1

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

2.4.18.11.1Goals

- See Step 19.3: 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: 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 EE point of view the process is slightly different than the process for initial provisioning.
- The RA will record the last time an EE 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 EE reestablishes a connection. The new certificates will be available for download at the time specified in the .info file.

2.4.18.11.2Assumptions

- EE/RA already scheduled generation of OBE identification certificates. See Step 19.4: Schedule generation of subsequent batch of OBE identification certificates

2.4.18.11.3Requirements

Key	Status	Summary	Description	justification	notes	Component/s
SCMS-508	SCMS PoC out of Scope	Stop pre-generating certificates for inactive device	RA shall stop pre-generating pseudonym/OBE identification certificates for a device that has not connected to RA for a given amount of time	So that computing resources are not wasted for inactive devices. If device has not connected for a certain period	Stop/resume pre-generation is out of scope for PoC. Time is currently set to be 3 years. Based on the implementation, the LA may also stop pre-generating pre-linkage values.	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
			as specified by the SCMS Manager	of time, the assumption is the device is no longer available or in service.		
SCMS-509	Closed	Stop pre-generating pseudonym 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 for revoked devices		RA
SCMS-	SCMS PoC out of	Resume pre-generating	RA shall resume pre-generati	If the OBE submits a	Stop/resume pre-generation is out of scope for PoC.	RA

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
553	Scope	certificates	on of pseudonym/OBE identification certificates if an OBE submits a new request after a silent period where RA had stopped pre-generating	valid request, it is a signal that the OBE is participating again regardless of the length of the silent period.		
SCMS-576	Implemented	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 base on system load. Should there be a maximum? • PoC scope will be to update .info file for active EEs only.	RA
SCMS-	SCMS PoC out of	OBE revoke	A revoked OBE	Once an OBE	This is out of scope since it defines EE's behavior.	On-board Equip

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

DRAFT

Key	Status	Summary	Description	justification	notes	Component/s
1163	Scope	d	shall not attempt to download pseudonym certificate batches/ OBE identification certificate files.	detects that it has been revoked, it shall stop attempting to download more certificates.		ment (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 timesta	This is out of scope since it defines EE's behavior. • If no pseudonym certificates are available on the OBE for the current i_period (week), the OBE is allowed to make a download attempt at any time. • If no pseudonym certificates are available on the OBE for the next i_period (week), the OBE is allowed to make a download attempt at any time. • If no identification certificate is available on the OBE for the current or next time period, the OBE is allowed to make a download attempt at any time.	On-board Equipment (OBE)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				mp is the earliest the OBE is allowed to connect to the RA for the next download.		
SCMS-1188	SCMS PoC out of Scope	Trust Chain Broken - OBE	OBE shall not attempt to download pseudonym certificate batches/ OBE identification certificate files if any component in the trust chain of the OBE is revoked.	If the OBE's ECA or other CA in the chain is revoked the OBE shall not attempt to establish a connection to the RA. If an attempt is made, it will	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
				be unable to authenticate to the RA.		
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)

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Status	Summary	Description	justification	notes	Component/s
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-1293	Review	Schedule pre-generation of OBE pseudonym and OBE identification certificates	RA shall schedule pre-generation of certificates to meet the availability requirements of certificate download defined by the SCMS Manager.	Certificate requests may vary. The SCMS must ensure that certificates are available before the current certificate expires.	For pseudonym certificates, the availability requirement is specified in http://wiki.campllc.org/display/SP/3.4.+Download+of+Pseudonym+Certificates. For identification certificates, a certificate for the next time period shall always be available.	RA

10 issues

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

2.4.18.11.4Design

- Step 1: EE 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: EE and RA authenticate to each other.
- Step 3: EE downloads the Step 18.5: Generate Global and Local Certificate Chain File
    - 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: EE will download all or as many as possible, certificate files that it does not already have stored locally. It is the responsibility of the EE to determine which certificate files to download (i.e. skip files that have already been successfully downloaded and processed).
- Step 5: EE downloads the .info file (generated and updated by RA). The .info file contains the time when the next certificate batches will be available.

2.5 Modifications to Crypto Primitives

Here we describe modifications to crypto primitives that are used in multiple use cases to prevent duplication of content. 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. Also, 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.

Note: Test vectors for Linkage Values and Group Linkage Values updated description below as well as for Butterfly Expansion Function can be found in Stash.

2.5.1 Use of AES as a Derivation Function

Using AES as a derivation function is not nice from security point of view as AES is a reversible function. Even though we currently don't 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.

- Linkage values:
    a. In the old usage, as explained in Linkage Values, 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
        i. plv1(i, j) = $[AES_{ls1(i)}(la_id1 \,||\, j \,||\, 0^{80})]_{72}$, where

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

1. ls1(i) = [SHA-256(la_id1 || ls1(i-1) || 0^{112})]$_{128}$, where
    a. ls1(0) is a 128-bit string chosen at random for every device.

ii. plv2(i, j) = [$AES_{ls2(i)}$(la_id2 || j || 0^{80})]$_{72}$, where
1. ls2(i) = [SHA-256(la_id2 || ls2(i-1) || 0^{112})]$_{128}$, where
    a. ls2(0) is a 128-bit string chosen at random for every device.

b. 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

i. plv1(i, j) = [($AES_{ls1(i)}$(la_id1 || j || 0^{80})) **XOR (la_id1 || j || 0^{80})**]$_{72}$, where
1. ls1(i) = [SHA-256(la_id1 || ls1(i-1) || 0^{112})]$_{128}$, where
    a. ls1(0) is a 128-bit string chosen at random for every device.

ii. plv2(i, j) = [($AES_{ls2(i)}$(la_id2 || j || 0^{80})) **XOR (la_id2 || j || 0^{80})**]$_{72}$, where
1. ls2(i) = [SHA-256(la_id2 || ls2(i-1) || 0^{112})]$_{128}$, where
    a. 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

- Group linkage values:

a. In the old usage, as explained in Group Linkage Values, group linkage values are bit strings of size 9 bytes, computed as follows:
Group linkage value for time period i, for all j = 1 to 2^32, and group chain identifier k:
glv(i, j, k) = gplv1(i, j, k) XOR gplv2(i, j, k), where

i. gplv1(i, j, k) = [$AES_{gs1(i, k)}$(la_id1 || j || 0^{80})]$_{72}$, where
1. gs1(i, k) = [SHA-256(la_id1 || gs1(i-1, k) || 0^{112})]$_{128}$, where
    a. gs1(0, k) is a 128-bit string chosen at random for every group.

ii. gplv2(i, j, k) = [$AES_{gs2(i, k)}$(la_id2 || j || 0^{80})]$_{72}$, where
1. gs2(i, k) = [SHA-256(la_id2 || gs2(i-1, k) || 0^{112})]$_{128}$, where
    a. gs2(0, k) is a 128-bit string chosen at random for every group.

b. In the **new usage** with AES in Davies-Meyer mode as a derivation function, linkage values are computed as follows:
Group linkage value for time period i, for all j = 1 to 2^32, and group chain identifier k:
glv(i, j, k) = gplv1(i, j, k) XOR gplv2(i, j, k), where

i. gplv1(i, j, k) = [($AES_{gs1(i, k)}$(la_id1 || j || 0^{80})) **XOR (la_id1 || j || 0^{80})**]$_{72}$, where

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

1. gs1(i, k) = [SHA-256(la_id1 || gs1(i-1, k) || 0^{112})]$_{128}$, where
    a. gs1(0, k) is a 128-bit string chosen at random for every group.

ii. gplv2(i, j, k) = [$AES_{gs2(i, k)}$(la_id2 || j || 0^{80}) **XOR (la_id2 || j || 0^{80})**]$_{72}$, where

1. gs2(i, k) = [SHA-256(la_id2 || gs2(i-1, k) || 0^{112})]$_{128}$, where
    a. gs2(0, k) is a 128-bit string chosen at random for every group.

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

- Encrypted indices for group linkage values:
    a. In the old usage, as explained in Group Linkage Values, encrypted indices are computed as follows. Let ik be the 128-bit indices key shared between the LA-pair in question, then for all j = 1 to 2^32, and group chain identifier k, encrypted indices (denoted as ei(j, k)) = AES_{ik}(j || k || 0^{64}).
    b. In the **new usage** with AES in Davies-Meyer mode as a derivation function, encrypted indices are computed as follows. Let ik be the indices key shared between the LA-pair in question, then for all j = 1 to 2^32, and group chain identifier k, ei(j, k) = AES_{ik}(j || k || 0^{64}) **XOR (j || k || 0^{64})**.
- Butterfly expansion function: With our new usage of AES in Davies-Meyer mode as a derivation function, the butterfly expansion function is modified as in the following section Butterfly Expansion Function.

2.5.2 Butterfly Expansion Function

The butterfly expansion function described in Butterfly Keys doesn't 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 decided 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 in Butterfly Keys can be summarized as:

- Device picks 2 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:

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

- Device picks 2 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 2 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 **$f_k^{int}(x) = (AES_k(x+1) \text{ XOR } (x+1)) \,||\, (AES_k(x+2) \text{ XOR } (x+2)) \,||\, (AES_k(x+3) \text{ XOR } (x+3))$** 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

2.5.3 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 cert is the length of 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 1st, 2004.

If leap seconds happen we may choose to adjust the start validity time of the certs so it isn't 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.

2.5.4 Clock Time corresponding to i=0

For Safety Pilot, the clock time corresponding to i=0 was defined to be 00:00 UTC January 1st 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. Taking all these into account, i=0 corresponds to: **4:00 am Eastern Time on Tuesday, January 6th, 2015** (i.e., 4023 days and 8 hours or **347,616,000 seconds** since 1609.2 epoch).

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

2.5.5 Encryption of Pre-linkage Values by LA for PCA

In the old design, when LA sends pre-linkage values to RA for pseudonym certificate provisioning, it encrypts them for PCA using symmetric encryption. The secret key used for encryption is shared between LA and PCA through an out-of-band means. This has an impact on privacy (though only minor) from a malicious PCA, if RA uses more than 1 pair of LAs for a given PCA, as PCA can easily tell which pair of LAs were used in any given request sent by RA to PCA. This privacy impact can easily be mitigated if LA were to use public-key encryption for encrypting pre-linkage values for PCA, as a ciphertext generated using public-key encryption doesn't need to contain any sender-related (in this case, LA) information. However, the team realized that using public-key encryption will add a significant amount of computational overhead on both LA and PCA, and decided to stick with symmetric encryption, **with a recommendation for RA to keep the number of pairs of LAs per PCA as low as possible, ideally 1**.

2.5.6 Misbehavior Investigation: PCA returns encrypted pre-linkage values to MA

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

The original design is described in MA → PCA_ MA requests pre-linkage values from PCA (Misbehavior Detection) and PCA → MA_ PCA replies to pre-linkage values request (Misbehavior Detection).

The new design is described in Step 8.2: OBE Misbehavior Investigation, 8.2.1 MA-PCA: linkage value -> encrypted pre-linkage value, LA's host name, and 8.2.2 LA - MA: encrypted pre-linkage value -> LinkageInformation.

2.5.7 Crypto Primitives affecting End-Entity

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

- Use of AES as a Derivation Function
- Butterfly Expansion Function
- Clock Time corresponding to i=0
- Pseudonym Certificate Validity

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Appendix A. EE Requirements with “EE-Handshake” label

Key	Summary	Description	justification	notes	Component/s	Labels
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)	EE-Handshake UseCase1 UseCase13Step3 UseCase19Step3 UseCase19Step5 UseCase3Step1 UseCase3Step4 UseCase9
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	EE-Handshake UseCase1 UseCase9
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 certs currently. Instead the OBE will use TLS to authenticate the other endpoint (as a server) and will use its SCMS cert to identify itself. EE authenticates via its IEEE 1609.2 enrollment certificate. The details of the authentication process are defined Step 3.4: Download of Pseudonym Certificates	RA	EE-Handshake UseCase1 UseCase13Step3 UseCase19Step3 UseCase19Step5 UseCase3Step1 UseCase3Step4 UseCase9
SCMS-522	Retry request	If the EE doesn't receive acknowledgement (TCP ACK) within a specified amount of time, currently set to be 2 sec from the time of request, it shall retry.	to ensure that the request is received by the RA.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)	EE-Handshake UseCase13Step1 UseCase19Step1 UseCase3Step2
SCMS-523	Number of retries	EE shall limit the number of retries to a maximum of 10 in a 60 minute period	Certificate Provisioning Request with the RA for a minimum of 60 minute after 10 consecutive failed communication attempts resulting in no acknowledgement (TCP ACK) or no Certificate Provisioning Response	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)	EE-Handshake MA-Integration UseCAse19Step1 UseCase13Step1 UseCase3Step2
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 (adversary might extract Butterfly encryption keys from junked vehicle at a later stage and is then able to identify all EE 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	On-board Equipment (OBE), RA, Road-side Equipment (RSE)	EE-Handshake UseCase13Step3 UseCase19Step3 UseCase3Step4 UseCase9

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Summary	Description	justification	notes	Component/s	Labels
				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 in Step 3.4: Download of Pseudonym Certificates.	This is out of scope since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)	EE-Handshake UseCase1 UseCase13Step3 UseCase19Step3 UseCase19Step5 UseCase3Step1 UseCase3Step4 UseCase9
SCMS-541	OCSP stapling - EE	The EE may use the TLS Certificate Status Request extension (OCSP stapling) to verify RA revocation status.	Revocation is optional and it's up to the OEMs support it.	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)	EE-Handshake UseCase13Step3 UseCase19Step3 UseCase3Step4 UseCase9
SCMS-958	Error code: eeConnectionFailed	EE shall log this error in its log file, 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)	EE-Handshake UseCase13Step1 UseCase13Step3 UseCase19Step3 UseCase19Step5 UseCase3Step1 UseCase3Step4 UseCase9
SCMS-979	Error code: eeAuthenticationFailed	EE shall store this error code in EE's error log file, 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)	EE-Handshake UseCase13Step3 UseCase19Step3 UseCase19Step5 UseCase3Step1 UseCase3Step4 UseCase9
SCMS-1090	Error code: rseRaTcpErrors	RA shall return standard TCP error codes if TCP errors occur.	in order to enable client side error handling.		RA	EE-Handshake UseCase13Step3 UseCase19Step3 UseCase3Step4 UseCase9
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 since it defines EE's behavior.	On-board Equipment (OBE), Road-side Equipment (RSE)	EE-Handshake UseCase13Step3 UseCase19Step3 UseCase3Step4 UseCase9
SCMS-1208	EE securely stores X.509 root certificate	EE shall store the X.509 root certificate in tamper-resistant storage.	The EE will need to communicate securely, at the TLS level, with the RA (e.g. in order to download pseudonym certs) 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)	EE-Handshake UseCase11Step3 UseCase12Step1 UseCase2Step1
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),	EE-Handshake UseCase10 UseCase12 UseCase14

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Summary	Description	justification	notes	Component/s	Labels
					Road-side Equipment (RSE)	UseCase17 UseCase2 UseCase3 UseCase5 UseCase6 UseCase9

Appendix B. EE Requirements Table

Key	Summary	Description	Labels
SCMS-335	EE issues a CRL Request	An EE shall issues a HTTP get to the CRL Store to obtain the latest CRL.	UseCase6
SCMS-341	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.	UseCase6
SCMS-342	CRL Store Authentication	The EE shall authenticate the CRL Store through usual SSL/TLS means.	UseCase6
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.	UseCase11Step2.1-PCA
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.	EE-Handshake UseCase13Step3 UseCase19Step3 UseCase19Step5 UseCase3Step1 UseCase3Step4 UseCase9
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	MA-Integration UseCase19Step1 UseCase3Step2
SCMS-522	Retry request	If the EE doesn't receive acknowledgement (TCP ACK) within a specified amount of time, currently set to be 2 sec from the time of request, it shall retry.	EE-Handshake UseCase13Step1 UseCase19Step1 UseCase3Step2
SCMS-523	Number of retries	EE shall limit the number of retries to a maximum of 10 in a 60 minute period	EE-Handshake MA-Integration UseCase13Step1 UseCase19Step1 UseCase3Step2
SCMS-524	RA certificate	EE shall dynamically acquire RA's SCMS certificate in case it has changed, see EE →RA _ RA Certificate Request, EE →RA _ RA Certificate Response	UseCase13Step1 UseCase19Step1 UseCase3Step2
SCMS-537	RA-to-EE encryption	The RA-to-EE communication shall be encrypted.	EE-Handshake UseCase13Step3 UseCase19Step3 UseCase3Step4 UseCase9
SCMS-539	RA authentication to EE	The EE shall require RA Authentication before any communication starts.	EE-Handshake UseCase13Step3 UseCase19Step3 UseCase19Step5 UseCase3Step1 UseCase3Step4 UseCase9
SCMS-541	OCSP stapling - EE	The EE may use the TLS Certificate Status Request extension (OCSP stapling) to verify RA revocation status.	EE-Handshake UseCase13Step3 UseCase19Step3 UseCase3Step4 UseCase9
SCMS-556	Secure process	There shall be a secure operational process for devices manufactures to inject EE firmware, enrollment certificates etc.	UseCase12 UseCase2 rework

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Summary	Description	Labels
SCMS-557	Secure chain of custody	EE shall get firmware, enrollment certificates etc. injected with a secure chain of custody for device manufacturers.	UseCase12 UseCase2
SCMS-560	Certified Software	EEs shall ensure that during bootstrapping process only certified software is provisioned.	UseCase12 UseCase2
SCMS-583	Butterfly keys	The EE shall generate new butterfly keys/expansion functions for the new RA.	UseCase11Step3
SCMS-684	Encryption	EE shall encrypt misbehavior reports with the Misbehavior Authority's public key before sending.	UseCase14 UseCase5
SCMS-709	Check for Policy Updates	EE shall check for and download policy updates upon establishing communications with the RA	UseCase13Step1 UseCase17 UseCase19Step6 UseCase3Step1 UseCase9Step1
SCMS-754	Sign certificate request	The EE shall sign certificate requests with its enrollment certificate.	UseCase13Step1 UseCase19Step1 UseCase3Step2
SCMS-767	Check for Certificate Chain Updates	EE shall check for version changes in 'certChainFileId' field of the Global Policy file. If the version is different than that of its existing file, it will take action to update it.	UseCase13Step1 UseCase17 UseCase19Step6 UseCase3Step1 UseCase9Step1
SCMS-776	Encrypt certificate request	The EE shall encrypt the request using the RA certificate.	UseCase13Step1 UseCase19Step1 UseCase3Step2
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.	UseCase11Step2.2
SCMS-865	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 Certs.	UseCase11Step2.2
SCMS-866	OBEs obtaining new Pseudonym 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 Certificates that chain up to the new Root CA.	UseCase11Step2.2
SCMS-949	Error code: eeInitCertProvFailed	EE generates this code when the Initialization process fails at completing a certificate provisioning of any of the certificates	ErrorCode UseCase12Step1 UseCase2Step1
SCMS-950	Error code: eeInitCRLProvError	EE generates this code when the Initialization process fails at completing the CRL provisioning.	ErrorCode UseCase12Step1 UseCase2Step1
SCMS-952	Error code: eeGlobalPolicyFileDownloadFailed	EE shall implement OEM defined error handling and store the error code in EE's error log file, if EE is not able to download the global policy file (e.g. because there is none or it's corrupted).	ErrorCode UseCase17 UseCase19Step6 UseCase3Step1 UseCase9Step1
SCMS-953	Misbehavior reporting: eeGlobalPolicyFileDownloadFailed	If EE is not able to download the global policy file (e.g. because there is none or it's corrupted), EE shall initiate a misbehavior report to MA with the observed error.	MA-Integration UseCase13Step1 UseCase19Step6 UseCase3Step1 UseCase9Step1
SCMS-954	Error code: eeGlobalPolicyVerificationFailed	EE shall implement OEM defined error handling and store this error code in EE's error log file, if EE is not able to verify the digital signature of the global policy file.	ErrorCode UseCase13Step1 UseCase19Step6 UseCase3Step1 UseCase9Step1

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Summary	Description	Labels
SCMS-955	Misbehavior reporting: eeGlobalPolicyVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify the digital signature of the global policy file.	MA-Integration UseCase13Step1 UseCase19Step6 UseCase3Step1 UseCase9Step1
SCMS-956	Error code: eeGlobalPolicyFileParsingFailed	EE shall implement OEM defined error handling and store this error code in EE's error log file, if EE is not able to parse the successfully downloaded global policy file (e.g. because it's corrupted).	ErrorCode UseCase17 UseCase19Step6 UseCase3Step1 UseCase9Step1
SCMS-957	Misbehavior reporting: eeGlobalPolicyFileParsingFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to parse the successfully downloaded global policy file (e.g. because it's corrupted).	MA-Integration UseCase13Step1 UseCase19Step6 UseCase3Step1 UseCase9Step1
SCMS-958	Error code: eeConnectionFailed	EE shall log this error in its log file, if it cannot connect to RA because there is a connection timeout.	EE-Handshake ErrorCode UseCase13Step1 UseCase13Step3 UseCase19Step3 UseCase19Step5 UseCase3Step1 UseCase3Step4 UseCase9
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's corrupted), OBE shall implement OEM defined error handling and store the error code in OBE's error log file.	ErrorCode UseCase19Step3 UseCase3Step4 UseCase9Step2
SCMS-966	Misbehavior reporting: 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's corrupted).	MA-Integration UseCase13Step3 UseCase19Step3 UseCase3Step4 UseCase9Step2
SCMS-967	Error code: eeCertFileVerificationFailed	EE shall implement OEM defined error handling and store the error code in EE's error log file, if EE is not able to verify the digital signature of an encrypted certificate.	ErrorCode UseCase13Step3 UseCase3Step4 UseCase9Step2
SCMS-968	Misbehavior reporting: 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.	MA-Integration UseCase13Step3 UseCase3Step4 UseCase9Step2
SCMS-969	Error code: eeCertificateFileDecryptionFailed	EE shall implement OEM defined error handling and store the error code in EE's error log file, if EE is not able to decrypt an encrypted certificate.	ErrorCode UseCase13Step3 UseCase19Step3 UseCase3Step4 UseCase9Step2
SCMS-970	Misbehavior reporting: eeCertFileDecryptionFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to decrypt an encrypted certificate.	MA-Integration UseCase19Step3 UseCase3Step4 UseCase9Step2
SCMS-971	Error code: eeCertificateVerificationFailed	EE shall implement OEM defined error handling and store the error code in EE's error log file, if EE is not able to verify a certificate.	ErrorCode UseCase11Step3 UseCase13Step3 UseCase19Step3 UseCase3Step4 UseCase9Step2
SCMS-972	Misbehavior reporting: eeCertVerificationFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to verify a certificate.	MA-Integration UseCase13Step3 UseCase19Step3 UseCase3Step4 UseCase9Step2
SCMS-973	Error code: eeCertContentFalse	EE shall implement OEM defined error handling and store the error code in EE's error log file, if EE is not able to parse a certificate, or if the certificate has wrong content.	ErrorCode UseCase13Step3 UseCase19Step3 UseCase3Step4 UseCase9Step2
SCMS-974	Misbehavior reporting: 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.	MA-Integration UseCase13Step3 UseCase19Step3 UseCase3Step4 UseCase9Step2
SCMS-979	Error code: eeAuthenticationFailed	EE shall store this error code in EE's error log file, if RA-to-EE authentication fails.	EE-Handshake ErrorCode UseCase13Step3 UseCase19Step3 UseCase19Step5 UseCase3Step1 UseCase3Step4 UseCase9
SCMS-	Misbehavior reporting: eeAuthenticationFailed	EE shall initiate a misbehavior report to MA with the observed error, if RA-to-EE authentication fails.	MA-Integration UseCase13Step3 UseCase19Step3

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Summary	Description	Labels
980			UseCase19Step5 UseCase3Step1 UseCase3Step4 UseCase9
SCMS-984	Error code: eeInfoFileDownloadFailed	OBE shall implement OEM defined error handling and store the error code in its error log file, if OBE is not able to download the .info file (e.g. because there is none or it's corrupted).	ErrorCode UseCase19Step3 UseCase3Step4 UseCase9Step2
SCMS-985	Misbehavior reporting: eeInfoFileDownloadFailed	EE shall initiate a misbehavior report to MA with the observed error, if EE is not able to download the .info file (e.g. because there is none or it's corrupted).	MA-Integration UseCase19Step3 UseCase3Step4 UseCase9Step2
SCMS-991	Error code: eeCRLStoreAuthenticationFailed	EE shall store this error in its log file, if it cannot authenticate the CRL Store.	ErrorCode UseCase6
SCMS-994	Error code: eeCRLDownloadFailed	EE shall store this error and the reason in its log file, if EE is not able to download the CRL file.	ErrorCode UseCase6
SCMS-995	Error code: eeCRLVerificationFailed	EE shall store this error in its log file, if EE's verification of the CRL signature fails.	ErrorCode MA-Integration UseCase6
SCMS-1009	Error code: eeEncryptionFailed	RSE shall store this error in it's error log file, if RSE encounters an error when encrypting a misbehavior report with MA's public key.	ErrorCode UseCase14
SCMS-1013	Error code: eeEncryptionFailed	EE shall store this error in its error log file, if EE encounters an error when encrypting a misbehavior report with MA's public key.	ErrorCode UseCase5
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.	UseCase11Step1.2
SCMS-1076	Error code: eeGlobalPolicyVerificationFailed	EE shall implement OEM defined error handling, if EE is not able to verify the digital signature of the global policy file.	ErrorCode UseCase17
SCMS-1095	RSE Enrollment	RSE enrollment shall be the same as OBE enrollment as specified in Step 2.2: Enrollment (Bootstrapping)	UseCase12Step2
SCMS-1159	EE securely stores Elector certificates	EE shall store the Elector certificates in secure tamper-resistant storage.	UseCase12Step1 UseCase2Step1
SCMS-1160	EE securely stores Root CA certificate	EE shall store the Root CA certificate in secure tamper-resistant storage.	UseCase12Step1 UseCase2Step1
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.	UseCase10 UseCase11Step3
SCMS-1163	OBE revoked	A revoked OBE shall not attempt to download pseudonym certificate batches/OBE identification certificate files.	UseCase19Step7 UseCase9Step2
SCMS-1164	OBE next download timing	OBE shall use the stored .info file to schedule the next download attempt.	UseCase19Step7 UseCase9Step2
SCMS-	Expired Certificate Batches	The OBE shall only download pseudonym certificate batches for the current and future i_period.	UseCase9Step2

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Summary	Description	Labels
1167			
SCMS-1168	OBE pseudonym certificate duplicate downloads	OBE shall not download pseudonym certificate batches that are already verified and stored on the device.	UseCase9Step2
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.	UseCase11Step2.2
SCMS-1171	EE revoked	EE shall not attempt to download a policy file, if it is revoked.	UseCase19Step6 UseCase9Step1
SCMS-1174	EE stores the Policy Generator certificate	EE shall store the Policy Generator certificate.	UseCase12Step1 UseCase2Step1
SCMS-1176	EE stores the CRLG certificate	EE shall store the Certificate Revocation List Generator certificate.	UseCase12Step1 UseCase2Step1
SCMS-1188	Trust Chain Broken - OBE	OBE shall not attempt to download pseudonym certificate batches/OBE identification certificate files if any component in the trust chain of the OBE is revoked.	UseCase19Step7 UseCase9Step2
SCMS-1189	Trust Chain Broken - EE	EE shall not attempt to download a policy file If any component in the trust chain of the EE is revoked.	UseCase17 UseCase19Step6 UseCase9Step1
SCMS-1190	RA URL Update	EE shall be able to update RA's URL.	UseCase11Step3
SCMS-1191	TLS Root Update	EE shall be able to receive and store an updated TLS (x.509) Root Certificate.	UseCase11Step3
SCMS-1192	Secure Update	All update methods used shall conform to established SCMS security policies.	Policy UseCase11Step3
SCMS-1196	Stored .info file	OBE shall have a .info file stored from the previous connection to the RA.	UseCase19Step5 UseCase9
SCMS-1201	EE certificate download via HTTPS over TCP/IP	EE shall use HTTPS (TLS) over TCP/IP to download files from the SCMS.	EE-Handshake UseCase13Step3 UseCase19Step3 UseCase3Step4 UseCase9
SCMS-1207	EE stores Certificate Revocation List	EE shall store the Certificate Revocation List in tamper-resistent storage.	UseCase12Step1 UseCase2Step1
SCMS-1208	EE securely stores X.509 root certificate	EE shall store the X.509 root certificate in tamper-resistant storage.	EE-Handshake UseCase11Step3 UseCase12Step1 UseCase2Step1
SCMS-1209	EE securely stores Local Certificate Chain File	EE shall store the Local Certificate Chain File in tamper-resistant storage.	UseCase12Step1 UseCase2Step1
SCMS-	EE Secure Key Storing	EE shall store the private key of the enrollment certificate in tamper resistant secure memory.	UseCase12Step2 UseCase2Step2

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Summary	Description	Labels
1210			
SCMS-1214	OBE downloads .info file	OBE shall download the .info file each time OBE tries to download pseudonym certificates.	UseCase19Step3 UseCase3Step4 UseCase9Step2 rework
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.	UseCase19Step3 UseCase3Step4 UseCase9Step2
SCMS-1216	OBE calculates linkage values	OBE shall calculate the currently valid linkage values for each CRL entry that describes a set of pseudonym certificates and store temporarily for further use.	Delete UseCase8Step4 rework
SCMS-1217	OBE compares linkage values	OBE shall compare the linkage value in each received sender certificate against the list of revoked linkage values.	UseCase8Step4
SCMS-1219	OBE updates linkage value list	OBE shall update the list of revoked linkage values for each time period (week). OBE shall either update the linkage value or remove the linkage value.	UseCase8Step4
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 time period (week).	UseCase8Step4
SCMS-1221	OBE processes CRL	OBE shall process the updated CRL/CRL chunk and update its CRL within 1 minute after receiving the update CRL or CRL chunk.	UseCase8Step4
SCMS-1222	Removed CRL entry	OBE shall apply a missing CRL entry (from a previous CRL) for at least one more time period (week) if an updated CRL misses this CRL entry.	MA-Integration UseCase8Step4
SCMS-1223	OBE checks against CRL for other certificate types	EEs shall check all received sender certificates against the most recent CRL. If the sender certificate is listed, OBE shall discard the received message.	UseCase8Step4
SCMS-1224	OBE stops sending	OBE shall stop sending over-the-air DSRC messages, if it detects that it has been listed on the CRL.	UseCase8Step4
SCMS-1226	EE Timely Limited Configuration Options	EE shall support the use of timely limited configuration options.	UseCase18Step1
SCMS-1227	EE Timely Limited Configuration Options: POC	For POC, EE shall support the parsing of a timely limited configuration option policy file.	UseCase18Step1
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.	UseCase13Step3 UseCase19Step3 UseCase3Step1 UseCase3Step4 UseCase6 UseCase9
SCMS-1270	Network connection	EEs shall use TCP/IP to communicate with the SCMS.	EE-Handshake UseCase10 UseCase12 UseCase14 UseCase17 UseCase2 UseCase3 UseCase5 UseCase6 UseCase9
SCMS-1279	Error code: certificateDecryptionFailed	EE shall log this error If certificate decryption failed at EE.	ErrorCode UseCase13Step3 UseCase3Step4
SCMS-	Error code: eeCertificateNotReadable	EE shall log this error if any certificate is not readable.	ErrorCode MA-Integration UseCase13Step3 UseCase3Step4

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Summary	Description	Labels
1280			
SCMS-1285	OBE stops sending: revoked ECA for OBE's enrollment certificate	OBE shall stop sending over-the-air messages, if it detects (via CRL) that it's ECA, or any ICA between it's ECA and the Root CA, has been revoked.	UseCase8Step4
SCMS-1286	OBE stops sending: revoked PCA for OBE's pseudonym certificates	OBE shall stop using all pseudonym certificates issued by a certain PCA, if OBE detects (via CRL) that this PCA, or any ICA between PCA and Root CA, has been revoked.	UseCase8Step4
SCMS-1289	OBE identification certificate duplicate downloads	The OBE shall not download OBE identification certificates that are already verified and stored in OBE.	UseCase19Step7
SCMS-1291	Expired Certificate Files	The OBE shall only download OBE identification certificate files for the current and future time periods.	UseCase19Step7
SCMS-1302	OBE check received BSMs against CRL	OBE shall check all received BSMs against the CRL using the mechanism described in IEEE 1609.2-v3-D12: • Clause 5.1.3.4 • Clause 6.4.10 and 6.4.11 • Clause 7	UseCase8Step4
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.	UseCase13Step3 UseCase19Step3 UseCase3Step4
SCMS-1308	OBE sign misbehavior reports	OBE shall sign a misbehavior report with a currently valid (at time of event observation) pseudonym certificate.	UseCase5
SCMS-1309	RSE sign misbehavior report	RSE shall sign misbehavior reports with RSE application certificate	UseCase14
SCMS-1338	Split GCCF/LCCF from scms-policy + refinements	1. Separate out GCCF from the Global Policy File (GPF) and make it a separate specification. The link between the GPF and GCCF is the GCCF version number which will be referenced inside the GPF. 2. The GPF gets signed by the Policy Generator. The GCCF does not have a signature on the file. 3. Create a specification for an LCCF. This will share the same structure as the GCCF, but the structure will be repeated in two sections - one required and one optional. A local RA can decide what elements of the GCCF to include in each section of the LCCF. 4. The version number on an LCCF will have two components - one will be a copy of the GCCF version, the other will be a local version number assigned by the RA 5. The LCCF does not have a signature of the file.	
SCMS-1353	EE gets LCCF from RA	EE shall check for and download policy an updated Local Certificate Chain File (LCCF) or Global Certificate Chain File (GCCF) upon establishing communications with the RA	UseCase13Step1 UseCase19Step6 UseCase3Step1 UseCase9Step1
SCMS-1356	LCCF validation in EE	EE shall use the Local or Global Certificate Chain File (LCCF/GCCF) to validate received SCMS certificates and respond to P2P certificate requests.	UseCase13Step1 UseCase19Step6 UseCase3Step1 UseCase9Step1

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Key	Summary	Description	Labels
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.	UseCase11Step1.3
SCMS-1404	EE send data via HTTP post over TCP/IP	EE shall use HTTP post to send data towards the RA	UseCase10 UseCase13Step1 UseCase14 UseCase19Step1 UseCase3Step2 UseCase5

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Appendix C. 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
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
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

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Acronym	Full form / description
	does not succumb to a single failure.
ETSI	European Telecommunications Standards Institute
FCC	Federal Communication Commision
FCW	Forward Collision Warning
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standards
FM	Frequency Modulation
FMVSS	Federal Motor Vehicle Safety Standards
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
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
LCCF	Local Certificate Chain File
LA	Linkage Authority
LOP	Location Obscurer Proxy
LCI	Linkage Chain Identifier
LCM	Local Certificate Management
LCW	Lane Change Warning
LOP	Location Obscurer Proxy
LS	Linkage Seed
LTA	Left Turn Assist

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Acronym	Full form / description
LV	Linkage Value
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.
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
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

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Acronym	Full form / description
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).
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 is created by establishing a virtual point-to-point connection through the use of dedicated connections, virtual tunneling protocols, or traffic encryption.
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).

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

Acronym	Full form / description
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

DRAFT

The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary