Certificate Types

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

On-Board Equipment (OBE)

OBE Enrollment

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

Pseudonym

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

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

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

Identification

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

Road-Side Equipment (RSE)

RSE Enrollment

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

Application

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

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

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

SCMS Component

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

Electors

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

Root CA

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

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

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

ICA

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

ECA

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

PCA

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

CRL Generator

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

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. They are described are as follows:

LA Certificates

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

RA Certificates

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

MA Certificates

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

EE Certificate Type Features

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

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

	OBE Enrollment Certificate	OBE Pseudonym Certificate	OBE Identification Certificate	RSE Enrollment Certificate	RSE Application Certificate	
					RSE with Connectivity	RSE without Connectivity
Provisioning	1 per EE per PSID category	20 per week, up to 3 years, top-up refresh using butterfly keys	1 per time period, only issue very small number of certificates at a time, top-up refresh using butterfly keys	1 per EE per PSID category	1 per time period, only issue for short time periods, require frequent renewal. RSE generates public/private key pair and provides public-key to RA	1 per time period, issue longer time periods. RSE generates public/private key pair and provides public-key to RA
Revocation	RA blacklist	leverage linkage values	add certificate digests of all issued certificates (can be more than one)	RA blacklist	Cannot renew certificates, due to RA blacklist of enrollment certificate	Add certificate digest of all issued certificates (can be more than one)
Response is Encrypted by PCA		X	X		X	X
Shuffle in RA		X				
CRL for End-entity Devices (Certificates of this type can be listed on CRL)		X	X			X
Simultaneous Validity for given PSID		X	only allow minimal overlap to account for critical events			
Linkage Values		X				
Butterfly Keys		X	X			
Continued Generation		X	X			
Issuing Certificates for Multiple Time Periods		X	X			
Pseudonymity	X	X				
Misbehavior Reporting		X	X		X	X
Non-Traceability		X				
Encryption Key			(X) (determined using butterfly key mechanism)		X	

Certificate Type Features

Requirements

Key	Status	Summary	Description	Justification	Notes	Component/s

SCMS-1311	CLOSED	Issue only one OBE identification certificate valid at a time	PCA shall only issue one OBE identification certificate to an OBE that is valid at a time for a given application.	There is no need for privacy (by definition).		PCA
SCMS-1312	CLOSED	Issue RSE application certificates with optional encryption key	PCA shall issue RSE application certificates with optional encryption key.	The encryption key is optional.	RSE application certificates always have a signature key and optionally an encryption key.	PCA
SCMS-1313	CLOSED	Issue only one RSE application certificate valid at a time	PCA shall only issue one RSE application certificate to an RSE valid at a time for a given application, except for the allowed overlap period.	There is no need for privacy.		PCA
SCMS-1314	MANUAL PROCESS	SCMS component certificate types (implicit vs. explicit)	The SCMS component shall have a certificate of explicit type.	Implicit: OBE Enrollment, RSE Enrollment, Pseudonym, Application, Identification Explicit (Self Signed): RootCA, Elector Explicit: Everything else PCA, ICA, Root CA, and elector certificates need to be of explicit type in order to support P2P distribution. All the EE certificates are of implicit type to save storage space and over-the-air bytes, and all the SCMS Component certificates are of explicit type.	Details discussed in certificate types	CRL Store, CRLG, DCM, IBLM, ICA, LA, PCA, PG, RA, RCA
SCMS-1315	MANUAL PROCESS	Only 1 certificate valid at a time	Each SCMS component shall have only 1 valid and in-use certificate at a time.	There are no privacy concerns for SCMS components that would justify more than one certificate valid at a given time. At the same time, it is desirable to keep complexity low and have maximum control over components, hence allowing exactly one certificate at a given time.		CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, PCA, PG, RA
SCMS-1316	SCMS POC OUT OF SCOPE	Additional SCMS component certificate for the next time period	Each SCMS component shall be allowed to request and receive a certificate that is valid for the next time period at a time defined by the certificate policy given by the SCMS Manager.	To allow continuity of secure communication between SCMS components.	The additional certificate is likely requested by the SCMS component towards the end of the current time period.	CRL Store, CRLG, DCM, ECA, IBLM, ICA, LA, PCA, PG, RA

6 issues

CAMP LLC Proprietary. The information contained in this document is considered an interim work product and is subject to revision without notice. The content is provided as is, only for informational purposes with no express or implied warranties that the information is accurate, up-to-date or complete. Any reliance on the content is solely at the user’s own risk. Contact the VSC5 Consortium if you have questions regarding the content.