SCMS MANAGER™

SECURITY CREDENTIAL MANAGEMENT SYSTEM

IEEE 1609.2.1 PROFILE

(VERSION 1.0.3)

March 15, 2023

Author(s)

SCMS Manager

1 TABLE OF CONTENTS

1 OVERVIEW

This document is a profile of the IEEE 1609.2.1 standard [7] noting which options are chosen. This document was created to help unify initial deployments of the IEEE 1609.2.1 standard to allow wide-spread use. Below, we will include a guide to using this document. Any time the "Standard" is referenced in this document, the reference refers to the IEEE 1609.2.1 standard. Each option profiled will provide a reference to the section itself in the standard. The version of the standard referenced in this profile is IEEE Std 1609.2.1™-2022.

1.1 TERMS AND DEFINITIONS

Authorization certificate authority (ACA) – The certificate authority who issues authorization certificates (pseudonym, identification, application).

Activation Codes for Pseudonym Certificates (ACPC) – An approach to issuing certificates that uses codes to lock certificates until the end-entity reaches out with an unlock code

Application certificate – An authorization certificate that does not hide the identity of an end entity and which does not use the butterfly key method as well. Commonly used in RSUs.

Authorization certificate – A certificate used to certify a device to perform application related activities.

Butterfly keys – A cryptographic process that uses a base elliptic curve cryptography key and an expansion process and creates many unrelated public/private key pairs that only the holder of the base key can derive

Certificate revocation list (CRL) – A list published in the system noting which certificates have had their access revoked

Certificate trust list (CTL) – A list signed by electors of which electors and root certificates are valid as anchors of trust within a Security Credential Management System (SCMS). This will be signed by the electors

Distribution center (DC) – An SCMS component that distributes public information about the SCMS system

Enrollment certificate authority (ECA) – The certificate authority which issues enrollment certificates

End-entity (EE) – The device or actor that uses the certificates provided by the SCMS for applications

Enrollment certificate – A certificate which provides authorization to request authorization certificates within the SCMS system

iPeriod – A length of time that indicates the lifetime for a certificate which is parametrized in the system to issue certificates of different lengths.

Identification certificate – A certificate for applications that does not hide identity. Application certificates are a subset of this. These certificates can either use the butterfly key method or not.

Linkage authority (LA) – An SCMS component which creates linkage values which allow revocation of pseudonym certificates while maintaining privacy

Misbehavior authority (MA) – An SCMS component which is responsible for aggregating reports of malicious behavior in the system and performing the analysis and revocation of the offending EEs.

Misbehavior Report – Reports of malicious behavior that are sent to the misbehavior authority to be aggregated and analyzed

OAuth 2.0 – A standard for authorization for obtaining web resources

On-board unit (OBU) – A type of end-entity device for passenger automobiles. Contrast with RSU.

Pseudonym certificate – An authorization certificate that hides the identity of the holder using butterfly keys and linkage values

Provider Service Identifier (PSID) – An identifier of an application activity that is put in an authorization certificate to authorize a given application.

Registration authority (RA) – The SCMS component that serves as the entry point for an EE to contact the SCMS for enrollment and authorization certificates

Road-side unit (RSU) – A type of end-entity device for infrastructure, such as road signs. Contrast with OBU

Root certificate authority (RCA) – The certificate authority that issues certificates for the root certificate which is a trust-anchor and is self-signed

Supplementary authorization server (SAS) – An optional SCMS component for issuing access tokens for operations not authorized by certificates. Uses OAuth 2.0 bearer authorization in the current version of the IEEE 16092.1 standard.

Security Credential Management System (SCMS) – A system comprising of certificate authorities and other entitles that allow the creation of a system of trusted actors based on IEEE 1609.2 certificates.

X.509 – A different certificate format than IEEE certificates that also associates some identity with a key pair.

1.2 ACRONYMS

ACA – Authorization certificate authority
ACPC – Activation codes for pseudonym certificates
API – Application programming interface
CCF – Certificate chain file
CRACA – Certificate revocation authorizing certificate authority
CRL – Certificate revocation list
CTL – Certificate trust list
DC – Distribution center
ECA – Enrollment certificate authority
EE – End entity
HTTP – Hypertext Transfer Protocol
LA – Linkage authority
MA – Misbehavior Authority
OBU – On-board unity

PKI – public key infrastructure
PSID – Provider Service Identifier
RA – Registration authority
RSU – Road-side unit
RCA – Root certificate authority
SAS – Supplementary authorization server (SAS)
SCMS – Security credential management service
TLS – Transport Layer Security
URL – uniform resource locator
USDOT – United States Department of Transportation

1.3 AUDIENCE AND SCOPE OF PROFILE

This profile is intended for both SCMS and EE operators and developers. This profile intends to limit the options in the IEEE 1609.2.1 standard [7] to a certain set of options that will allow deployments in the connected vehicle ecosystem to be unified. The information is intended to be targeted to the different sections of the IEEE 1609.2.1 standard such that a reader of this will be able to obtain clarity about how to apply a specific section of the Standard in a real-world deployment. If a section does not contain any information that needs to be profiled, this profile will not include any profiling information on that section.

For EE developers/operators, this profile will describe and limit the options for the mechanisms used to connect to an SCMS, from the network layer to the application layer. This provides a minimal set of requirements to conform to the IEEE 1609.2.1 standard and communicate successfully to the SCMS.

For SCMS developers/operators, this profile will describe parameters and technical policies that an SCMS deployment must conform to.

The intention is that an SCMS deployment and an EE both conforming to this profile shall be able to communicate and perform SCMS-related services successfully.

1.4 WORD USAGE

The word “shall”/"must", “should” and “may” follow the same definition as defined in RFC 2119 [8].

- “shall” indicates a requirement that must not be deviated from to conform to the profile
- “should” indicates a strong suggestion that devices conforming to the profile adhere to the statement, but there may be certain situations where it can be disobeyed
- “may” indicates a statement that is optional for conformance to the profile

1.5 DOCUMENT GUIDE

This document goes through each section of the Standard sequentially, profiling when necessary. Each subsection of this profile will have a section reference to which section of the Standard is being profiled. If a section is omitted, this is because no options needed to be profiled for the section.

2 ARCHITECTURE (SECTION 4)

2.1 INTERFACE AND USE CASES

2.1.1 DC-EE INTERFACE

Section reference: 4.1.2.3

This profile does not cover the DC-EE interface. Support of this interface is not necessary for conformance to this profile.

2.1.2 ECA-EE INTERFACE

Section reference: 4.1.2.4

The ECA supports communication with the EE over a secure session as defined in 1609.2.1 clause 4.2. This is profiled in section 2.1.16 of this profile.

The ECA Identifying URL will be provided by the ECA operator to the EE operator separately from this profile.

2.1.3 EE-MA INTERFACE

Section reference: 4.1.2.5

This profile does not cover the EE-MA interface. Support of this interface is not necessary for conformance to this profile.

2.1.4 EE-RA INTERFACE

Section reference: 4.1.2.6

The RA Identifying URL will be provided by the RA operator to the EE operator separately from this profile.

2.1.5 EE-SAS INTERFACE

Section reference: 4.1.2.7

This profile does not cover the EE-SAS interface. Support of this interface is not necessary for conformance to this profile.

2.1.6 TYPES OF ENROLLMENT CERTIFICATE

Section reference: 4.1.3

This profile only supports enrollment certificates following the IEEE 1609.2 format.

2.1.7 INITIAL ENROLLMENT CERTIFICATE REQUEST / DOWNLOAD

Section reference: 4.1.4.2

NOTE: The sub-bullets under bullet point a in 4.1.4.2 in the Standard seem to be a typo: bullet point a says that it will list constraints on permissions which sub-bullets 1 and 2 are not examples of constraints. Therefore, this profile does not provide profile material related to bullet point a.

Enrollment certificates published under this profile have their permissions profiled in section 4 of this profile (Section 6 of the Standard).

This profile allows different RAs to be assigned for different sets of applications if this is supported by the client. **NOTE: This is a profile of bullet item b, but bullet item b does not seem directly related to initial enrollment certificate request; it is included here to correspond to the structure of 1609.2.1.**

Indirect authorization is supported. If indirect authorization is used, the ECA operator will provide details to the EE operator about supported means of indirect authorization.

Direct authorization is supported. In the case of direct authorization:

- An ECA identifying URL will be provided by the ECA operator to the EE operator.
- The canonical identity is the HashedId32 of the public key from the canonical keypair
- The EE operator will provide the canonical identity and the canonical public key to the ECA operator.
- The canonical key acceptance policy is as follows:
    - The key must be created by a device that meets the criteria of End-Entity Security Requirements SCMS Manager specification [13]
    - The key must be created in a "secure environment" by the criteria of the End-Entity Security Requirements SCMS Manager specification.
    - The key must use a key type allowed by the Standard

  NOTE: The canonical key acceptance policy properly belongs in the Certificate Policy but is included in this profile document for convenience.

2.1.8 ENROLLMENT CERTIFICATE REGISTRATION AND BLOCKING

Section reference: 4.1.4.3.1

The enrollment certificate is used as the primary identifier of an EE to the RA. This profile does not define a different identifier.

The RA will only process requests from EEs whose enrollment certificates are registered with that RA. The EE operator will provide the enrollment certificate to the RA for registration. Details of how the EE operator obtains the enrollment certificate from the EE and of how the certificate is provided to the RA are out of scope for this profile.

Access to the RA using Oauth access tokens is not supported. **NOTE: This is written this way to be consistent with 1609.2.1, but we believe that 1609.2.1 should refer to the "supplementary authorization server (SAS)" rather than specifically to Oauth.**

The RA shall support a mechanism to block registered enrollment certificates.

2.1.9 AUTHORIZATION CERTIFICATE REQUEST / DOWNLOAD

Section reference: 4.1.4.3.2, 4.1.4.3.3

This profile allows request of both identification and pseudonym certificates.

This profile does not support ACPC.

There will be a policy that states how an EE is determined to be entitled to certificates with particular permissions, e.g. particular PSIDs and SSPs. That policy will be published separately from this profile and may be in multiple documents, for example, there may be documents specific to a particular PSID. The policy may be global, or deployment specific, or segmented in some other way.

This profile supports authorizing a download request with the enrollment certificate used for the certificate request or one of its successors.

This profile does not support authenticating a download request with the SAS.

2.1.10 SUCCESSOR ENROLLMENT CERTIFICATE REQUEST + DOWNLOAD

Section reference: 4.1.4.3.4

There will be a policy that states how an EE is determined to be entitled to successor enrollment certificates with particular permissions. That policy will be published separately from this profile and may be in multiple documents, for example, there may be documents specific to a particular PSID. The policy may be global, or deployment specific, or segmented in some other way.

2.1.11 USE CASES NOT AUTHORIZED BY ENROLLMENT CERTIFICATE

Section reference: 4.1.4.5

All the use cases listed in 4.1.4.5 are supported in unauthorized form.

An EE conformant to this profile shall support all the use cases in 4.1.4.5 across the EE-RA interface. Support across the DC-EE interface is not required by this profile.

2.1.12 MISBEHAVIOR REPORT

Section reference: 4.1.5

Misbehavior report submission is not addressed in this document. See the SCMS Manager Misbehavior specification. [14]

2.1.13 COMPOSITE CRL

Section reference: 4.1.6

This profile supports download of both composite and individual CRLs. **NOTE: Download of composite CRLs is preferred.**

The following is the list of CRLs which this profile supports. Each series number constitutes a different `SecuredCrl` object in a `CompositeCRL`.

Signed By	Certificates in this Series	Series Number	Entries on CRL Identified By	Notes
Root certificate	CRL Signer, Policy Generator, MA	256	Certificate hash	These are all certificates which are directly signed by the root which perform system functions, so their CRL must be signed by the root.
CRL Signer	ICA, ACA, ECA, RA, LA	2	Certificate hash	These are component certificates which are the ICA or signed by the ICA.
CRL Signer	OBU Pseudonym Certificates	1	Linkage seeds	-
CRL Signer	RSU Application Certificates, OBU Identification Certificates	3	Certificate hash	Since these are distributed on a longer timeline or requested weekly only the certificate hash is used.
CRL Signer	Enrollment certificates	4	Certificate hash	Since an RA manages blocked enrollment certificates, this CRL may not need to be used.

Table 1 – List of CRL Series numbers

2.1.14 CERTIFICATE CHAIN FILES

Section reference: 4.1.7:

This profile supports download of both certificate chain files and individual CA certificates. **NOTE**: **Download of certificate chain files is preferred**.

2.1.15 ELECTOR AND RCA MANAGEMENT

Section reference: 4.1.8

See the SCMS Manager standards “Elector Policy” and “Elector Technical Specification” for profile material. [11][12]

EE devices shall be initialized with the SCMS Manager elector certificates found here: https://www.scmsmanager.org/publications/.

2.1.16 INTERFACE APPROACH

Section reference: 4.2

The ECA/RA operator must communicate the ECA / RA <SERVER> URL to the EE operator separately from this profile.

2.1.17 TIME PERIOD PARAMETERS

Section reference: 4.3.2, Table 1

The following table profiles the time-period parameters to be used by conforming EEs. These time-period parameters match up with the time-period parameters chosen for the US Connected Vehicle Pilot Deployments

Parameter Name	Value	Notes
iPeriod	Based on iPeriodEpoch and iPeriodLength defined below	
iPeriodEpoch	4 am Eastern Time, Tuesday, January 6, 2015	
iPeriodInit	0	
iPeriodLength	1 week (168 hours)	
overlap	1 hour	
baseCertNumber	PSID-specific range of (1, …)	Note that identification certificates use a "local" i-value corresponding to how many individual certificates have been created and will not use these parameters. No upper range is defined on number of "base certs" in this profile.
overlapCertNumber	Equal to baseCertNumber	
extraBands	0	

Table 2 – Time period parameters

2.1.18 SESSION PARAMETERS

Section reference: 4.3.3, Table 2

For the use cases in this profile the value of *session-scmsAuth* shall be tls1.2 or tls1.3. Usage of the value *session-iso21177* may be added later to this profile but is not supported at this time. API endpoint specific profiles of which session parameters are acceptable are defined in section 4 of this profile (Section 6 of the Standard).

2.1.19 WEB API PARAMETERS (GENERIC)

Section reference: 4.3.4, Table 3

The value of *webApi-eeAuth* shall be none for this profile. The value *webApi-eeAuth=oAuth2.0* is not supported for this profile.

2.1.20 WEB API PARAMETERS (SCMS REST API V3)

Section reference: 4.3.5, Table 4

All values of *scmsV3-eeAuth* are used in this profile. The value of the *scmsV3-eeAuth* parameter is profiled on a per-endpoint basis in section 4 of this profile (Section 6 of the standard).

The *scmsV3-error* parameter shall have value *fine* on test systems and shall have value *coarse* on production systems. This will provide detailed information while testing and limit the amount of information shared in a production environment. Caveats about specific error codes being returned are noted later in the profile.

The o*ptions* parameter is profiled per endpoint later in this profile document.

2.1.21 USE CASE RELATED PARAMETERS

Section reference: 4.3.6, Table 5, Table 6, Table 7

The parameters in Table 5,6, and 7 shall be configured per SCMS-provider by a local policy file (LPF) that is currently being worked on in parallel to this profile. In the absence of an LPF, default values for these parameters are defined in the table below. For the PSID-specific parameters in the Standard such as *ra-maxPreloadTime*, the assumption with the table below is that it is for all PSIDs.

Parameter name	**Value**
eca-maxAge	1 week (168 hours)
eca-maxReqs	100,000
eca-maxWait	1 month
eca-minWait	1 hour
ra-acpcSupport	No
ra-butterflyType	Original
ra-maxAge	1 week (168 hours)
ra-maxGenDelay	1 week (168 hours)
ra-maxReqs	1
ra-maxPreloadTime	Range of (2 weeks, 3 years)
ra-minWait	1 hour
download-maxAge	1 hour
download-maxReqs	100
download-minWait	5 minutes

Table 3 – Use case parameters

3 SESSION PARAMETERS (SECTION 5)

3.1 PHYSICAL SECURITY

Section reference: 5.2

The usage of a physical session is not profiled in this profile. Support for physical sessions is not required as part of this profile.

3.2 TRANSPORT LAYER SECURITY (TLS)

Section reference: 5.3

The *ITU-T X.509 certificate acceptance policy* for an SCMS component server (RA, ECA) shall be that the *subjectAltName* in the certificate matches the identifying URL for the SCMS component.

The usage of TLS session resumption shall not be supported as part of this initial profile. The max lifetime of a session shall be 5 minutes.

Client authentication is supported. The ITU-T X.509 certificate acceptance policy for client authentication will be negotiated between the EE operator and SCMS operator.

3.3 ISO/TS 21177

Section reference: 5.4

If ISO/TS 21177 is supported in a future version of this profile, the *IEEE 1609.2 certificate acceptance policy* shall be that the *CertificateId* matches the identifying URL for the SCMS component.

4 SCMS WEB API USE CASE PROFILES (SECTION 6)

4.1 GENERAL WEB API

4.1.1 PROTOCOL PARAMETERS

Section reference: 6.1.2

This profile does not cover the OAuth 2.0 authentication. Support of *webApi-eeAuth=oAuth2.0*, is not necessary for conformance to this profile.

4.2 OAUTH 2.0 SUPPORT

Section reference: 6.2

This profile does not cover the OAuth 2.0 authentication. Support of clause 6.2 is not necessary for conformance to this profile.

4.3 USE CASE SUPPORTING INFORMATION

4.3.1 PROTOCOL PARAMETERS

Section reference: 6.3.1.3

scmsV3-error=fine is supported only for test implementations.

scmsV3-error=coarse is augmented in this profile by the following HTTP error codes, i.e., conformant implementations provide these error codes in addition to HTTP 500.

- 404 Not Found: Used when the certificates are not generated yet. The requester is suggested to retry at a later time.
- 408 Request Timeout: Used to indicate to the EE that it should retry after *eca-minWait* / *ra-minWait* / *download-minWait* and up to *eca-maxReqs* / *ra-maxReqs* / *download-maxReqs* times (with the parameters coming from Table's 5 / 6 / 7 of the Standard respectively).
- 412 Precondition Failed: Used if the If-Modified-Since header precondition fails (i.e., the requester has the most updated version of the requested resource).

4.3.2 HEADERS

Section reference: 6.3.1.6

The following HTTP headers are supported in this profile.

- If-Modified-Since: The use of the If-Modified-Since header is specified in IETF RFC 7232 [9]. This is used with download of system information for a device to check if they have the most up-to-date version of the CCF, CTL, CRL, etc. The HTTP error code will be 412 if the resource has not been modified since the last revision and the device can safely trust that they have the most up-to-date version of the system.
- Range: The use of the Range header is specified in IETF RFC 7233 [10] using the bytes range unit. This is used in this Standard for download of certificate files by a device to support recovery from a failed download.

4.4 WEB API USE CASES

Section reference: 6.3, Annex C

The following section profiles all the use cases in section 6.3 of the Standard. For each use case, this profile will use the template from Annex C.2 to profile what options are supported. The use-case specific information from Annex C.4 of the standard will also be profiled too. This profile will also note if any information about this use is or is anticipated to be included as part of the local policy file (LPF) which is being developed in parallel to this profile.

The additional information needed for each parameter in Annex C.3 of the Standard is profiled here. If any additional information needs to be profiled on a per-use case basis from Annex C.3, that will be included in the use case profile below. The below list includes information on additional information for each parameter in Annex C.3 that is used in this profile.

- *scmsAuth=tls1.2 / scmsAuth=tls1.3:* The certificate acceptance policy for X.509 can be found in section 3.2 of this profile.
- *eeAuth=canonical*: The canonical key acceptance policy can be found in section 2.1.7 of this profile.
- *webApi-options*: The use of different HTTP headers (options) is noted in section 4.3.2 of this profile.

4.4.1 ENROLLMENT CERTIFICATE REQUEST

Section reference: 6.3.4.2

The following table fills in the profile for authentication from Annex C.2 of the standard.

Category	Parameter code	Values supported	Permissible combinations
session	scmsAuth	*tls1.2, tls1.3*	n/a
	eeAuth	*none*	
webApi	Name	*scmsV3*	
	eeAuth	*none*	
scmsV3	eeAuth	*canonical*	
	Error	*coarse (production), fine (test)*	
	Options	n/a	

Table 4 – Enrollment certificate request profile

The following information from Annex C.4 of the standard is also profiled:

1) Supported permissions:
    - Enrollment certificates published under this profile will always have "wildcard" permissions, i.e. will have certRequestPermissions be a sequence of PsidGroupPermissions of length 1 with subjectPermissions indicating the choice all
2) eeAuth options:
    - The eeAuth options are noted in the table above
3) Table 5 Parameters:
    - The parameters from Table 5 are profiled in section 2.1.21 of this profile.

The following additional constraints on the response to the enrollment certificate request endpoint are as follows:

- The returned `Certificate` shall not have a `CertificateId` field of type `LinkageData`
- The returned `Certificate` shall not have an `OperatingOrganizationId`

4.4.2 AUTHORIZATION CERTIFICATE REQUEST

Section reference: 6.3.5.2

The following table fills in the profile for authentication from Annex C.2 of the Standard.

Category	Parameter code	Values supported	Permissible combinations
session	scmsAuth	*tls1.2, tls1.3*	n/a
	eeAuth	*none*	
webApi	name	*scmsV3*	
	eeAuth	*none*	
scmsV3	eeAuth	*enrollment*	
	error	*coarse (production), fine (test)*	
	options	n/a	

Table 5 – Authorization certificate request profile

The following information from Annex C.4 of the Standard is also profiled:

1) Permissions:
    a. This profile applies to all permissions included in the IEEE PSID list [1]. As noted in section 2.1.9, there will be a policy published that determine how an EE is determined to be entitled to authorization certificates with particular permissions.
2) eeAuth options:
    a. The eeAuth options are noted in the table above
3) Table 6 Parameters:
    a. The parameters from Table 6 are profiled in section 2.1.21 of this profile which mentions that these parameters may be further profiled in the LPF.
4) Pseudonym certificate time parameters:
    a. The time period parameters are profiled in section 2.1.17 of this profile.

4.4.3 AUTHORIZATION CERTIFICATE DOWNLOAD

Section reference: 6.3.5.3

The following table fills in the profile for authentication from Annex C.2 of the standard.

Category	Parameter code	Values supported	Permissible combinations
session	scmsAuth	*tls1.2, tls1.3*	
	eeAuth	*none*	
webApi	name	*scmsV3*	
	eeAuth	*none*	
scmsV3	eeAuth	*enrollment*	
	error	*coarse (production), fine (test)*	
	options	*Range*	

Table 6 – Authorization certificate download profile

The following information from Annex C.4 of the standard is also profiled:

1) eeAuth options: The eeAuth options are noted in the table above
2) Filename in URL or not: This profile shall use the variation without the filename in the URL
3) acpcSupport and butterflyType: Section 2.1.21 of this profile notes that there is no ACPC support in this profile and that butterflyType shall use *original* for this profile.
4) Table 7 parameters: The parameters from Table 7 are profiled in section 2.1.21 of this profile which mentions that these parameters may be further profiled in the LPF.

4.4.4 SUCCESSOR ENROLLMENT CERTIFICATE REQUEST

Section reference: 6.3.5.4

The following table fills in the profile for authentication from Annex C.2 of the standard.

Table 7 – Successor enrollment certificate request profile

Category	Parameter code	Values supported	Permissible combinations
session	scmsAuth	*tls1.2, tls1.3*	n/a
	eeAuth	*none*	
webApi	name	*scmsV3*	
	eeAuth	*none*	
scmsV3	eeAuth	*enrollment*	
	error	*coarse (production), fine (test)*	
	options	n/a	

The following information from Annex C.4 of the standard is also profiled:

1) Supported permissions: Section 2.1.10 of this profile notes that there will be a profile published that notes how an EE is determined to be entitled to successor enrollment certificates with particular permissions.
2) eeAuth options: The eeAuth options are noted in the table above
3) Table 6 parameters: The parameters from Table 6 are profiled in section 2.1.21 of this profile which mentions that these parameters may be further profiled in the LPF.

4.4.5 SUCCESSOR ENROLLMENT CERTIFICATE DOWNLOAD

Section reference: 6.3.5.5

The following table fills in the profile for authentication from Annex C.2 of the standard.

Category	Parameter code	Values supported	Permissible combinations
session	scmsAuth	*tls1.2, tls1.3*	n/a
	eeAuth	*none*	
webApi	name	*scmsV3*	
	eeAuth	*none*	
scmsV3	eeAuth	*enrollment*	
	error	*coarse (production), fine (test)*	
	options	*Range*	

Table 8 – Successor enrollment certificate download profile

The following information from Annex C.4 of the standard is also profiled:

1) eeAuth options: The eeAuth options are noted in the table above
2) Table 7 parameters: The parameters from Table 7 are profiled in section 2.1.21 of this profile which mentions that these parameters may be further profiled in the LPF.

4.4.6 MISBEHAVIOR REPORT SUBMISSION

Section reference: 6.3.5.6

The following table fills in the profile for authentication from Annex C.2 of the standard.

Category	Parameter code	Values supported	Permissible combinations
session	scmsAuth	*tls1.2, tls1.3*	n/a
	eeAuth	*none*	
webApi	name	*scmsV3*	
	eeAuth	*none*	
scmsV3	eeAuth	*enrollment*	
	error	*coarse (production), fine (test)*	
	options	n/a	

Table 9 – Misbehavior report submission profile

The following information from Annex C.4 of the standard is also profiled:

1) eeAuth options: The eeAuth options are noted in the table above

4.4.7 CERTIFICATE CHAIN FILE INCLUDING CTL DOWNLOAD

Section reference: 6.3.5.7

The following table fills in the profile for authentication from Annex C.2 of the standard.

Category	Parameter code	Values supported	Permissible combinations
session	scmsAuth	*tls1.2, tls1.3*	n/a
	eeAuth	*none*	
webApi	name	*scmsV3*	
	eeAuth	*none*	
scmsV3	eeAuth	*none*	
	error	*coarse (production), fine (test)*	
	options	*If-Modified-Since*	

Table 10 – Certificate chain file including CTL download profile

The following information from Annex C.4 of the standard is also profiled:

1) eeAuth options: The eeAuth options are noted in the table above.
2) Table 7 parameters: The parameters from Table 7 are profiled in section 2.1.21 of this profile which mentions that these parameters may be further profiled in the LPF.

The CtlSeriesId used for the API endpoint shall be the SCMS Manager CtlSeriesId from Annex M.

4.4.8 COMPOSITE CRL INCLUDING CTL DOWNLOAD

Section reference: 6.3.5.8

The following table fills in the profile for authentication from Annex C.2 of the standard.

Category	Parameter code	Values supported	Permissible combinations
session	scmsAuth	*tls1.2, tls1.3*	n/a
	eeAuth	*none*	
webApi	name	*scmsV3*	
	eeAuth	*none*	
scmsV3	eeAuth	*none*	
	error	*coarse (production), fine (test)*	
	options	*If-Modified-Since*	

Table 11 – Composite CRL including CTL download profile

The following information from Annex C.4 of the standard is also profiled:

1) eeAuth options: The eeAuth options are noted in the table above.
2) Table 7 parameters: The parameters from Table 7 are profiled in section 2.1.21 of this profile which mentions that these parameters may be further profiled in the LPF.

The CtlSeriesId used for the API endpoint is the SCMS Manager CtlSeriesId from Annex M.

4.4.9 INDIVIDUAL CA CERTIFICATE DOWNLOAD

Section reference: 6.3.5.9

The following table fills in the profile for authentication from Annex C.2 of the standard.

Category	Parameter code	Values supported	Permissible combinations
session	scmsAuth	*tls1.2, tls1.3*	n/a
	eeAuth	*none*	
webApi	name	*scmsV3*	
	eeAuth	*none*	
scmsV3	eeAuth	*none*	
	error	*coarse (production), fine (test)*	
	options	*If-Modified-Since*	

Table 12 – Individual CA certificate download profile

The following information from Annex C.4 of the standard is also profiled:

1) eeAuth options: The eeAuth options are noted in the table above.
2) Table 7 parameters: The parameters from Table 7 are profiled in section 2.1.21 of this profile which mentions that these parameters may be further profiled in the LPF.

4.4.10 INDIVIDUAL CRL DOWNLOAD

Section reference: 6.3.5.10

The following table fills in the profile for authentication from Annex C.2 of the standard.

Category	Parameter code	Values supported	Permissible combinations
session	scmsAuth	*tls1.2, tls1.3*	n/a
	eeAuth	*none*	
webApi	name	*scmsV3*	
	eeAuth	*none*	
scmsV3	eeAuth	*none*	
	error	*coarse (production), fine (test)*	
	options	*If-Modified-Since*	

Table 13 – Individual CRL download profile

The following information from Annex C.4 of the standard is also profiled:

1) eeAuth options: The eeAuth options are noted in the table above.
2) Table 7 parameters: The parameters from Table 7 are profiled in section 2.1.21 of this profile which mentions that these parameters may be further profiled in the LPF.

4.4.11 CTL DOWNLOAD

Section reference: 6.3.5.11

The following table fills in the profile for authentication from Annex C.2 of the standard.

Category	Parameter code	Values supported	Permissible combinations
session	scmsAuth	*tls1.2, tls1.3*	n/a
	eeAuth	*none*	
webApi	name	*scmsV3*	
	eeAuth	*none*	
scmsV3	eeAuth	*none*	
	error	*coarse (production), fine (test)*	
	options	*If-Modified-Since*	

Table 14 – CTL download profile

The following information from Annex C.4 of the standard is also profiled:

1) eeAuth options: The eeAuth options are noted in the table above.
2) Table 7 parameters: The parameters from Table 7 are profiled in section 2.1.21 of this profile which mentions that these parameters may be further profiled in the LPF.

The CtlSeriesId used for the API endpoint is the SCMS Manager CtlSeriesId from Annex M. Note that the CCF including CTL download is preferred over this API endpoint in this profile.

4.4.12 RA CERTIFICATE DOWNLOAD

Section reference: 6.3.5.12

The following table fills in the profile for authentication from Annex C.2 of the standard.

Category	Parameter code	Values supported	Permissible combinations
session	scmsAuth	*tls1.2, tls1.3*	n/a
	eeAuth	*none*	
webApi	name	*scmsV3*	
	eeAuth	*none*	
scmsV3	eeAuth	*none*	
	error	*coarse (production), fine (test)*	
	options	*If-Modified-Since*	

Table 15 – RA certificate download profile

The following information from Annex C.4 of the standard is also profiled:

1) eeAuth options: The eeAuth options are noted in the table above.
2) Table 7 parameters: The parameters from Table 7 are profiled in section 2.1.21 of this profile which mentions that these parameters may be further profiled in the LPF.

4.4.13 MA CERTIFICATE DOWNLOAD

Section reference: 6.3.5.13

The following table fills in the profile for authentication from Annex C.2 of the standard.

Category	Parameter code	Values supported	Permissible combinations
session	scmsAuth	*tls1.2, tls1.3*	n/a
	eeAuth	*none*	
webApi	name	*scmsV3*	
	eeAuth	*none*	
scmsV3	eeAuth	*none*	
	error	*coarse (production), fine (test)*	
	options	*If-Modified-Since*	

Table 16 – MA certificate download profile

4.4.14 CERTIFICATE MANAGEMENT INFORMATION STATUS DOWNLOAD

Section reference: 6.3.5.14

The following table fills in the profile for authentication from Annex C.2 of the standard.

Table 17 – Certificate management status information status download profile

Category	Parameter code	Values supported	Permissible combinations
session	scmsAuth	*tls1.2, tls1.3*	n/a
	eeAuth	*none*	
webApi	name	*scmsV3*	
	eeAuth	*none*	
scmsV3	eeAuth	*none*	
	error	*coarse (production), fine (test)*	
	options	*If-Modified-Since*	

5 CERTIFICATE PROFILES (SECTION 7)

The following sections profile additional restrictions in on certificate profiles

5.1 X.509 ENROLLMENT CERTIFICATES

Section reference: 7.6.3.8

X.509 enrollment certificates are not supported as part of this profile.

6 MISCELLANEOUS (SECTIONS 8-11)

6.1 CTL FILES

Section reference: 8.6

The CtlSeriesId used for the purposes of this profile is the US SCMS Manager `CtlSeriesId` with value “03 48 00 00 00 00 00 00”.

6.2 CRYPTOGRAPHY

The following section will profile cryptographic options present in section 9 of the Standard.

6.2.1 COCOON KEY EXPANDER AND BUTTERFLY KEY EXPANDER

Section reference: 9.2.2

The design in Figure 12, using a cocoon key expander at the RA and a butterfly key expander at the ACA, is the only design supported in this profile.

6.2.2 BUTTERFLY KEY MECHANISM

Section reference: 9.2.5

The original butterfly key mechanism is the only butterfly mechanism supported as part of this profile.

6.2.3 ACPC SUPPORT

Section reference: 9.4

The use of the ACPC mechanism is not supported as part of this profile.

6.3 CERTIFICATE VALIDITY CONDITIONS

6.3.1 ENROLLMENT CERTIFICATE REQUEST VALIDITY CONDITIONS

Section reference: 10.1.3:

Further validity conditions for the `ToBeSignedCertificate` in the enrollment certificate request are as follows:

- The `ToBeSignedCertificate.region` field shall have the `identifiedRegion` field for the USA, Canada and Mexico only
- The `ToBeSignedCertificate.verificationKey` shall not be a key that was used in a previous enrollment certificate request under the same SCMS operator
- The `ToBeSignedCertificate.validityPeriod` shall be contained within the validity period for an issuing ECA in the SCMS system.
- The `ToBeSignedCertificate.crlSeries` shall contain the value 4.
- The `ToBeSignedCertificate.id.name` shall exist and uniquely identify the device in some way
- The `ToBeSignedCertificate.type` shall be of type implicit

6.3.2 SUCCESSOR ENROLLMENT CERTIFICATE REQUEST

Section reference: 10.1.4:

The further validity conditions on this request are the same as defined in section 6.3.1 of this profile.

6.3.3 AUTHORIZATION CERTIFICATE REQUEST VALIDITY CONDITIONS

Section reference 10.1.5

Further validity conditions for the `ToBeSignedCertificate` in the authorization certificate request are as follows:

- If `EeRaCertRequest.additionalParams` does not include butterfly keys, `ToBeSignedCertificate.id` shall not be of type `LinkageData`

- The `ToBeSignedCertificate.validityPeriod` shall be contained within the validity period for an issuing ACA in the SCMS system.
- The `ToBeSignedCertificate.type` shall be of type implicit
- The `ToBeSignedCertificate.crlSeries` shall correspond to the parameters in an `EeRaCertRequest` in the following way:
    - If `EeRaCertRequest.additionalParams` includes butterfly keys and `ToBeSignedCertificate.id` is of type `LinkageData`, `ToBeSignedCertificate.crlSeries` shall be 1
    - If `EeRaCertRequest.additionalParams` includes butterfly keys and `ToBeSignedCertificate.id` is not of type `LinkageData`, `ToBeSignedCertificate.crlSeries` shall be 3
    - If `EeRaCertRequest.additionalParams` does not include butterfly keys and `ToBeSignedCertificate.id` is not of type `LinkageData`, `ToBeSignedCertificate.crlSeries` shall be 3

6.3.4 AUTHORIZATION CERTIFICATE REQUEST AUTHORIZED BY X.509 CERTIFICATE

Section reference 10.1.8:

The further validity conditions on this request are the same as defined in section 6.3.3 of this profile.

7 REFERENCES

[1] IEEE Standards Association, PSID Public Listing[1]
[2] IEEE Std 1609.2, Guidance Notes[2]

[3] IEEE Std 1609.2™-2016, IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages.[3,4]

[4] IEEE Std 1609.2a™-2017, IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages—Amendment 1.

[1] Public PSID listing can be found here: https://standards.ieee.org/products-services/regauth/psid/public.html
[2] Guidance notes for the standard can be found here: https://grouper.ieee.org/groups/vt-its/1609/public/guidance-notes/

[3] The IEEE standards or products referred to in Clause 2 are trademarks owned by The Institute of Electrical and Electronics Engineers, Incorporated.
[4] IEEE publications are available from The Institute of Electrical and Electronics Engineers (http://standards.ieee.org/).

[5] IEEE Std 1609.2b™-2019, IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages—Amendment 2.

[6] IEEE Std 1609.2.1™-2020, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Certificate Management Interfaces for End Entities

[7] IEEE Std 1609.2.1™-2022, IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Certificate Management Interfaces for End Entities

[8] IETF RFC 2119, Key words for use in RFCs to Indicate Requirement Levels.[5]

[9] IETF RFC 7232, Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests.

[10] IETF RFC 7233, Hypertext Transfer Protocol (HTTP/1.1): Range Requests.

[11] SCMS Manager, Elector Policy.[6]
[12] SCMS Manager. Elector Technical Specification.
[13] SCMS Manager, End-Entity Security Requirements, Design Guidance, And Validation Approach
[14] SCMS Manager, Misbehavior Report and Application Specification.

8 VERSION HISTORY

Version	Date	Comments
1.0.0	January 23, 2023	Initial release
1.0.2	February 16, 2023	Updated TOC and Footer
1.0.3	March 15, 2023	Updated to scmsV3

[5] IETF publications are available from the Internet Engineering Task Force (https://www.ietf.org/).

[6] SCMS Manager publications and elector certificates can be found here: https://www.scmsmanager.org/publications/.