5GAA Automotive Association

Credential Management Supporting V2X Commercial Deployments

5GAA Automotive Association
Technical Report

CONTACT INFORMATION:
Executive Manager – Thomas Linget
Email: liaison@5gaa.org

MAILING ADDRESS:
5GAA c/o MCI Munich
Neumarkter Str. 21
81673 München, Germany
www.5gaa.org

This document has been prepared by the 5G Automotive Association (5GAA) and is based on the information and technology available at the time of its publication. It reflects the most current and accurate version to the best of 5GAA's knowledge. As technologies and industry standards continue to evolve, 5GAA is committed to regularly reviewing and updating this document as necessary to ensure its continued relevance and accuracy.

VERSION:	1.0
DATE OF PUBLICATION:	14 July 2025
DOCUMENT TYPE:	Technical Report
EXTERNAL PUBLICATION:	Yes
DATE OF APPROVAL BY 5GAA BOARD:	5 May 2025

Contents

Overview

Currently, for V2X[1] direct communication there is no available common policy (certificate policy for Public Key Infrastructure, or PKI, operators) for Security Credential Management System (SCMS) in the U.S. or Canada. A few SCMS providers created their own policies, which are not only incomplete but there are no published common policy documents feasible for SCMS PKI operation, hindering the widespread adoption of the technology. The Government of Canada sponsored an effort which resulted in a model for consideration.

A common Certificate Policy (CP) would help facilitate an ecosystem supporting interoperability and shared trust for V2X direct communication. The European Union addresses this issue by taking a central regulatory role, creating the CP, Security Policy (SP) and C-ITS Point of Contact (CPOC) documents that govern a V2X PKI for direct communication. North America need not duplicate what has been done elsewhere, though an accepted policy will build a greater ecosystem and support V2X direct deployment among a diverse set of automakers and other transport agencies.

The Certificate Policy Proposal contributing to this Work Item (WI) will subsequently evolve into a Technical Report (TR) that develops a clear CP leveraging global best practices for security PKI and practical experience securing V2X direct communication, as well as common processes to facilitate an approach to SCMS.

[1] 5GAA definition: Cellular-V2X (C-V2X) is an umbrella term which encapsulates all 3GPP V2X technologies, including both direct (PC5) and mobile network communications (Uu), unless otherwise stated. If only direct or only mobile network communications are addressed, then the terms 'direct' and 'mobile network' are used, respectively

For V2X mobile network communication, certificates are needed to authenticate interconnected backend systems and to protect communication between the systems, this TR will also elaborate on how to handle those certificates.

Problem statement

A policy establishing criteria for SCMS infrastructure setup in North America (US and Canada) does not exist, which precludes interoperability and shared trust throughout the ecosystem for V2X direct communication. A similar situation has been avoided in Europe where the European Telecommunications Standards Institute (ETSI) and the European Commission have developed and published such a process that can be audited by third parties to verify compliance with the defined security requirements. This presents a challenge to all stakeholders as SCMS providers are left guessing what may be deemed acceptable in terms of cloud/on-premise/remote hosting and hybrid setups and operation along a number of metrics, in addition to ensuring interoperability.

This also means stakeholders including automakers, road operators and suppliers are left without audited/validated verification of security compliance, presenting vulnerabilities for bad actors to take advantage of, jeopardizing the very safety we are trying to protect. There is no accepted criteria and methodology that can guarantee that the SCMS service is operated in a secure way, ultimately verified by third parties. Commercial incentives alone have been insufficient to achieve alignment, creating a barrier to commercial deployment and interoperability along with shared trust. There is risk that deployments without a common policy may not fulfil the goals expected of a US and Canadian C-V2X ecosystem for direct communication.

For C-V2X mobile network communication, standard IT technology is used for connections between backend systems,[2] however a harmonized approach would greatly simplify and thus accelerate deployments.

[2] https://5gaa.org/road-traffic-operation-in-a-digital-age-a-holistic-cross-stakeholder-approach/

Contents

Scope

The present document aims to produce a Technical Report that properly lays out the context of the issue, including the situation within North America, and lays out a CP blueprint, providing a global best practice for security PKI and practical experience securing V2X direct and mobile network communication. After this, the TR will then provide a common set of documented processes to facilitate a common approach to SCMS. The TR will be broken down into different chapters, each covering the context, CP and the advised common set of processes, respectively.

Upon finalization of this Work Item, the TR should be published and shared externally.

Current situation

V2X direct communication requires the use of certificates to verify the authenticity and integrity of the messages being shared such that the data sets can be utilized for driver safety, traffic efficiency, and for automated vehicle applications. For V2X mobile network mode, certificates are used to secure communication between trusted backend systems in the ecosystem,[3, 4] and potentially for the signing of messages. V2X direct mode for many applications has the added objective of maintaining a reasonable level of anonymity/privacy for end entities. For V2X mobile network mode where information sharing is done via interconnected backend systems, i.e. an end user has given consent to its service provider to handle personal data as part of the service agreement, a commonly accepted certificate policy is necessary to ensure interoperability and shared trust throughout the V2X ecosystem. Interoperability and shared trust are both critical to supporting mass deployments and ensuring a competitive and dynamic ecosystem involving a diverse set of automakers, transport agencies, and other stakeholders including security providers.

The various regions around the world that are embracing V2X communication are adopting a credential management system and corresponding policies to govern all aspects of certificate-handling including enrolment, issuance and revocation of digital certificates. The European Union has a central regulatory role and established the Certificate Policy[5], Security Policy[6], and C-ITS Point of Contact[7] documents that govern European V2X PKI, also known as the C-ITS Credential Management System. The Government of Canada also recognized the importance of having these policies and sponsored an effort which stopped short of becoming legislation and resulted in a model[8] for consideration by industry. The SCMS Manager LLC operating in the US has also prepared and shared online an initial version of a CP[9] for the U.S. Other entities in the US and Canada have also prepared and published their own certificate policies, including Blackberry[10] Certicom.

[3] https://5gaa.org/road-traffic-operation-in-a-digital-age-a-holistic-cross-stakeholder-approach/

[4] https://5gaa.org/vehicle-to-network-to-everything-v2n2x-communications-architecture-solution-blueprint-use-cases/

[5] C-ITS Certificate Policy - Release 3.0 - 2024 May 24
https://cpoc.jrc.ec.europa.eu/data/documents/E01941_C-ITS_Certificate_Policy_Release_3_0_FINAL.pdf

[6] C-ITS Security Policy - Release 3.0 - 2023 Sep 16
https://cpoc.jrc.ec.europa.eu/data/documents/e01941_C-ITS_Security_Policy_v3.0._20230916.pdf

[7] CPOC Protocol - Release 3.0
https://cpoc.jrc.ec.europa.eu/data/documents/e01941_CPOC_Protocol_v3.0_20240206.pdf

[8] Model Canadian Certificate Policy
https://tc.canada.ca/en/innovation-centre/priority-reports/security-credential-management-system-scms-model-canadian-certificate-policy
(Request the document)

[9] SCMS Manager Provider Requirements– Draft version 1.0
https://www.scmsmanager.org/wp-content/uploads/2023/10/SCMS-Manager-Provider-Requirements_v1_000.pdf
(partial CP can be found in Annex I)

[10] Blackberry V2X CA Certificate Policy V1.3
https://blackberry.certicom.com/content/dam/certicom/pdf/BlackBerry_V2X_CA_Certificate_Policy_v1.3.pdf

An initial draft of a North American SCMS Certificate Policy has been shared within 5GAA and draws the best from each of the published documents referenced above in addition to incorporating best practices from other well-established PKIs stemming from other industries including internet browsers. There is a supplementary comparison document[11] which references the various policies that exist and outlines what has been leveraged in the initial 5GAA draft. These policies all aim to inform and guide industry through the setup and operation of the credential management system, outlining compliance requirements for the SCMS Manager, SCMS Providers and the Infrastructure Owner Operators (who are managing the End Entity, or EE, devices), and describing the various roles and responsibilities of the stakeholders involved.

As of today, there is no commonly accepted Certificate Policy in North America, but through the 5GAA SCMS task we are working to harmonize and advance an industry-acceptable CP for SCMS. Nor has any previous work addressed how to harmonize the security and certificate-handling for a V2X solution using backend information sharing, i.e. V2X mobile network mode. For example, the European security policy[12] focused on the direct mode and omitted the mobile network mode which plays an important role in a complete V2X solution.

The Certificate Policy proposal contributed to this Work Item is only a draft to help accelerate the group's progress and will subsequently evolve into a Technical Report that produces the Certificate Policy leveraging global best practices, practical experience, and a common process to facilitate an approach to SCMS. By working with various stakeholders including SCMS Manager LLC we aim to have a thorough, rigorous and industry-acceptable policy.

The current absence of an accepted CP hinders interoperability and shared trust within the ecosystem, particularly amongst providers, and the secure interconnection between backend systems. For example, if two devices, D1 and D2, receive their certificates from two different SCMS providers, S1 and S2, such that the root CA of S1 is not trusted by the root CA of S2 (and vice versa), then D1 and D2 will not be able to trust each other's messages. With an industry-wide acceptable CP comes the opportunity to establish a Certificate Trust List (CTL) that robustly establishes trust by hosting the various compliant root CAs on this list that can be referenced to verify integrity.

A similar situation has been avoided in Europe where ETSI and the European Commission have developed and published such a policy that can be audited by third parties to verify compliance with the defined security requirements. This absence in North America presents a challenge to all stakeholders as SCMS Providers are left guessing what may be deemed acceptable in terms of cloud, on-premises, and hybrid setups and operations along several metrics, in addition to ensuring interoperability. It is imperative that SCMS Providers know the criteria/policy necessary to ensure addition and removal from the CTL, and ambiguity in criteria should be avoided to ensure acceptable compliance and inclusion/exclusion.

Not having a commonly accepted policy also means stakeholders – including automakers, road operators and suppliers – are left without the means to help third-

[11] Comparative analysis of the PKI Ecosystems_231128_v1.2.docx
5GAA_WI-SCMS-Policy-242007_Comparative analysis of the PKI Ecosystems_231128_v1.2.docx

[12] See footnote 5

party auditors independently and objectively verify security compliance aimed at mitigating vulnerabilities that bad actors may exploit. This could jeopardize the very safety we are trying to protect.

Below is a list of PKI policies and their implementation from different organizations and regions that have been reviewed. There may be additional unpublished documents that could be leveraged, too. The following outlines how each reviewed policy contributes to work on the 5GAA SCMS CP Technical Report.

eIDAS Regulation (EU)

Contributions to SCMS CP:

- Democratic involvement in policymaking.
- Adoption of RFC 3647 format for CPs and CPSs.
- Inclusion of certification bodies under EA-MRA as eligibility criteria for certification.
- A model avoiding multiple trust lists adopted to reduce complexity and potential failure points.

Mozilla Root Policy (MRP)

Contributions to SCMS CP:

- Emphasis on community-edited CP to ensure transparency and inclusivity.
- Adoption of the RFC 3647 structure to standardize documentation.
- Incorporation of the root inclusion process that involves public consultation and has no direct costs.

CA/Browser Forum

Contributions to SCMS CP:

- Integration of a governance structure that balances the interests of different member groups.
- Highlighting the need for transparent and democratic CP modifications.

BlackBerry Certificate Policy

Contributions to SCMS CP:

- Adoption of some well-defined requirements from BlackBerry's policy, focusing on technical and legal governance of V2X certificates.
- Utilization of BlackBerry's approach to CP structure according to RFC 3647, ensuring comparability with other CPs.

SCMS Manager LLC

Contributions to SCMS CP:

- Incorporated EE device hardware security module (HSM) certification schemes to enhance security measures.

EU CCMS Policy

Contributions to SCMS CP:

- Used the EU's simplified PKI structure as a model, particularly its levels of certification that allow for phased compliance and interoperability testing.
- Emphasized the need for a central CP and CTL management to ensure uniformity across the ecosystem.

Model Canadian Certificate Policy

Contributions to SCMS CP:

- Leveraged extensive research and community involvement in developing the CP, ensuring it met the specific needs and conditions of the North American market.
- Adopted audit frequency and governance models that align with both EU standards and North American regulatory requirements.
- Each of these policies contributed specific elements related to structure, governance, transparency, and technical requirements that were integrated into the draft SCMS CP to create a comprehensive, secure and interoperable framework suitable for the North American V2X environment. This integration aims to standardize security PKI practices while accommodating the unique aspects of the regional ecosystem.

Way forward

Certificate-handling for V2X direct

Annex A contains a draft Certificate Policy for Secure Credential Management Systems. The draft CP addresses the unique needs and conditions of the North American market while ensuring a competitive ecosystem. By thoroughly analyzing and integrating the best practices from across the global PKI community, including the automotive and transportation sectors' V2X communications and well-established domains such as internet browsers, we have laid a solid foundation for a robust SCMS framework, though this is a draft and stakeholder input is highly desirable and expected to gain industry adoption.

The harmonization efforts reflected in the draft CP are designed to mitigate risks related to incompatibility and trust issues, thereby stimulating adoption. By adopting a composite approach that includes contributions from the EU CP, SCMS Manager LLC, Canadian Model CP, Mozilla Root Policy, CA/Browser Forum, and other significant entities, we ensure that the policy is not only comprehensive but also reflects the democratic and transparent governance necessary for widespread acceptance.

As we move forward, it is essential to continue this collaborative approach, refining the CP to align with international standards and regional requirements, thus supporting a secure, interoperable and efficient V2X ecosystem. The ultimate goal is to establish a commonly accepted, auditable and validated framework that not only promotes technological innovation but also safeguards the integrity and security of vehicular and transportation communications throughout North America.

Certificate-handling for V2X mobile network

V2X using mobile network and backend communication is an important part of V2X, and the usage, deployments and interest of interconnected backend systems increases for such V2X solutions, e.g. [13, 14, 15, 16, 17, 18, 19]

[13] ITSA-B5.9-2024-Deployment-Plan_FINAL-PDF.pdf

[14] IP-based interface profile, which is part of release 2.0.x of the C-Roads harmonised C-ITS specifications: https://www.croads.eu/fileadmin/user_upload/media/Dokumente/Harmonised_text_v2.pdf

[15] https://www.stellantis.com/en/news/press-releases/2023/may/safely-aware-industry-leading-v2x-activation-equips-1-8-million-stellantis-vehicles-with-emergency-vehicle-alert-system

[16] https://www.mobilidata.be/en

[17] https://dmi-ecosysteem.nl/en/theme-page-urban-traffic/techniek-achter-talking-traffic/

[18] https://5gaa.org/road-traffic-operation-in-a-digital-age-a-holistic-cross-stakeholder-approach/

[19] https://5gaa.org/vehicle-to-network-to-everything-v2n2x-communications-architecture-solution-blueprint-use-cases/

For these types of standard IT methods are used for authentication and to ensure secure communication between interconnected backend actors, e.g. using TLS, X509 certificates, mutual authentication. However, as the number of interconnected actors increase, it is becoming important to harmonise security solutions and simplify the integration of new actors into the ecosystem of interconnected actors, e.g. by harmonized handling, certificate formats, etc., thus providing scalability and increased flexibility for connections between backend systems. One important component to achieve this is a common Root Certificate Authority (CA), or a few Root CAs to provide common trust anchor(s) for the backend interconnect security domain (i.e. similar as for V2X direct communication security domain).

Existing CP(s) from CA suppliers can be leveraged for the V2X backend security domain because it is reusing existing procedures and proven security methods.

It is recommended to consider the V2X backend security domain and related PKI when planning for V2X deployments, e.g. as a combined effort with CAs and PKI for direct communication, potentially leveraging providers of CAs for direct communication and 1609.2 certificates, since a base functionality is to provide X509 certificates.

1 Introduction

1.1 Overview

This document is a Certificate Policy (CP) Proposal for Vehicle-to-Everything Public Key Infrastructure (V2X PKI) services intended for use in a Security Credential Management System (SCMS).

This CP proposal is based on the EU CCMS CP; there are no restrictions on its use under the CC-BY 4.0 license to do this, so the experience made by researchers are reusable for fast time-to-market SCMS implementations. The modifications made in the original document were needed due to the differences of CCMS and SCMS.

As the CP is an implementation of the IEEE 1609.2.1 standard, some details of this standard are referenced for ease of reading and uniform understanding, though this document in that context is subservient to the specifications outlined by IEEE if any disparities arise.

1.2 Document name and identification

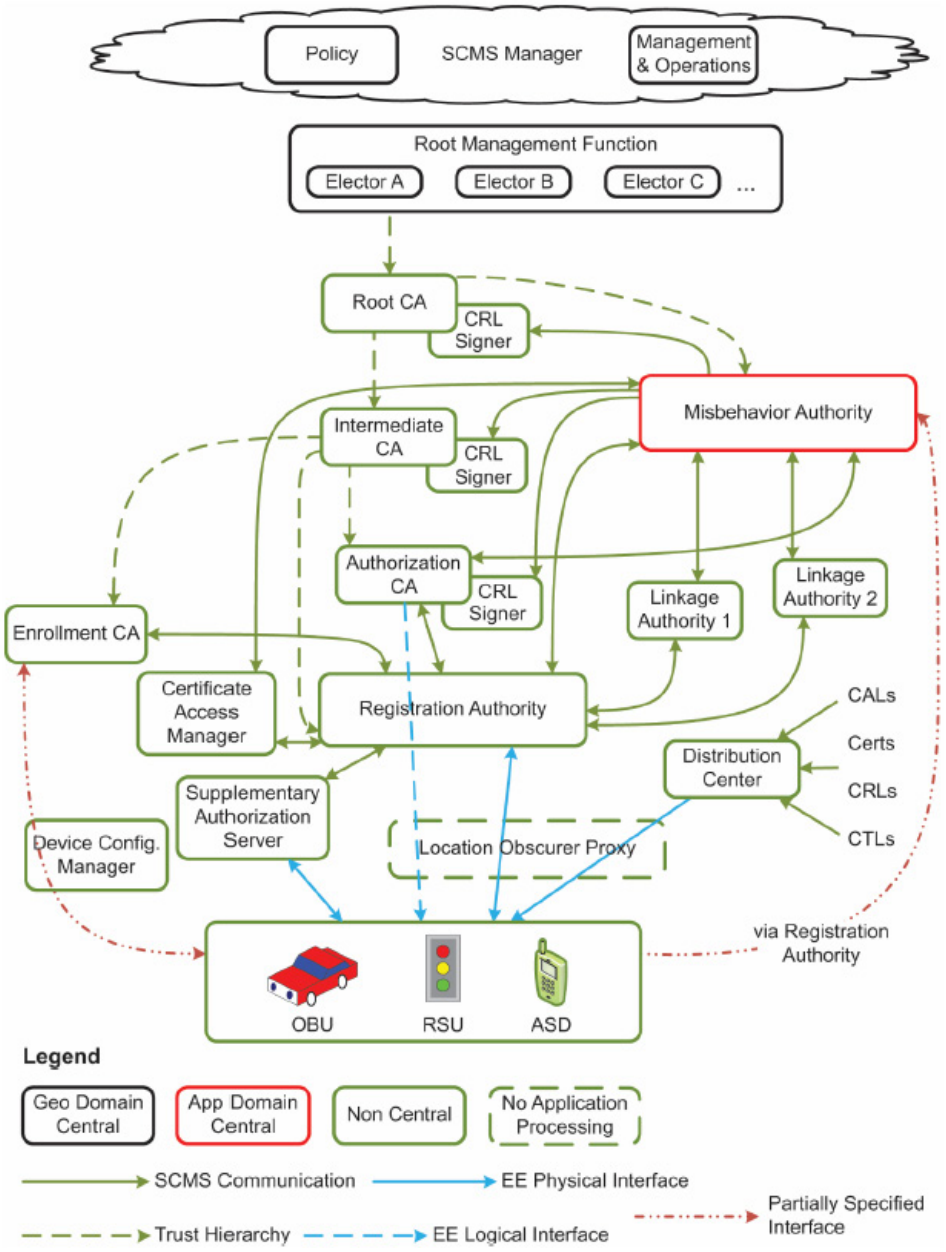
For the document name and identification, please refer to the title on the cover page and the table at page 2.

1.3 PKI participants

1.3.1 Introduction

Public Key Infrastructure participants play an obvious role in the PKI defined by the present policy. Unless explicitly prohibited, a participant can assume multiple roles at the same time. Although assuming specific roles simultaneously may be prohibited or flagged in the event of an identified conflict of interest or to ensure a segregation of duties.

The hierarchy for the SCMS model is described in IEEE 1609.2.1. and the PKI model participants are the those described in this specification.



1.3.2 SCMSMO

(1) The SCMSMO (SCMSO) is a body which manages the Certificate Trust List (CTL).

1.3.3 Electors

(2) The Electors are signing the CTL. Electors shall sign on receipt of an appropriately authenticated request of signing the CTL.

(3) The quorum is 3 of 5. This is an updateable parameter.

1.3.3.1 Publication Center (PUB)

The publication responsibilities are slightly different for the SCMSMO than an SCMS Provider, so we call this the 'Publication Center' (PUB).

(4) The SCMS Certificate Policy shall be distributed through a public internet URL (both current and all old versions) as part of the PUB. The policies shall be signed or sealed by an electronic signature certificate and thus timestamped. The preparation of policy modifications is a task for the Policy Committee, the publication to the internet URL is a task for the Publication Body.

(5) The SCMS Manager CTLs shall be distributed through a public internet URL (both current and all old version) as part of the PUB. The published CTLs shall be a quorum signed by the Electors. Changes to the published CTL shall be announced and distributed to participating SCMS Providers.

(6) The SCMS Manager additional information shall also be distributed through a public internet URL as part of the PUB. Such additional information could be all Elector certificates.

1.3.4 Accredited PKI Auditor

(7) The accredited PKI Auditor:

(a) shall be accredited for auditing SCMS Providers and Electors as stated in Section 8:

(1) shall audit the Electors and the SCMS Providers, which are operating Root CAs or a Sub-CAs,

(2) shall receive the CPS of the Elector and the SCMS Provider,

(3) shall be responsible to distribute the audit results to the CTL Committee for validation for inclusion of Elector or SCMS Providers' Root CA,

(4) shall decide if a CP modification requires a supplementary audit or not.

(b) shall be accredited to certify End Entity devices according to the Certificate Policy as stated in the Section 8.

1.3.5 SCMS Provider

(8) The SCMS Provider operates one or more elements from the following list: Root CA, ICA, ECA, ACA, LA, RA, MA, CRL Signer based on the IEEE 1609.2.1. It shall offer PKI services which are needed for revocation checking of certificates.

(9) The SCMS Provider shall have its CPS(s) compliant with the SCMS CP. The SCMS Provider shall manage its SCMS Services (including CAs) according to its CPS(s).

(10) The SCMS Provider shall be audited against this CP and its CPS(s) and has to apply for inclusion of its Root CA certificate on the CTL.

(11) The SCMS Provider shall submit regular audit results to the SCMSMO. The frequency of the audits is defined in Section 8.2.

(12) If a SCMS Provider does not own a Root CA, it must demonstrate that it has a contractual agreement with the SCMS Provider operating a Root CA included on the CTL, in order to get trusted Sub-CA certificates.

(13) An SCMS Provider shall cooperate with MAs.

1.3.5.1 Root CA

(14) As stated in IEEE 1609.2.1, a CA that issues certificates for other entities and whose certificate was issued by itself. Root CAs are rarely brought online because any Root CA compromise has a significant impact.

1.3.5.2 Intermediate CA (ICA)

(15) Based on IEEE 1609.2.1 definition: A CA whose certificate was issued by another CA and whose main responsibility is to issue certificates to other CAs, like ACA and ECA.

1.3.5.3 Enrollment CA (ECA)

(16) As stated in IEEE 1609.2.1: A CA whose main responsibility is to issue enrollment certificates.

(17) The initial enrollment certificate shall be provisioned via DCM or ECA, while the successor enrollment certificate shall be provisioned by the RA.

(18) Enrollment CA

(a) shall support:

(1) IEEE 1609.2.1 enrollment certificates for enrollment certificate request.

(b) may support (and document in its CPS if this is the case):

(1) X.509 certificates for enrolment certificate request,

(2) OAuth access token for enrollment certificate request at the ECA.

1.3.5.4 Authorization CA (ACA)

(19) As stated in IEEE 1609.2.1: A CA whose main responsibility is to issue authorization certificates.

1.3.5.5 CRL Signer

(20) A CAs CRL can be signed by the CA itself or alternatively by a CRL Signer.

1.3.5.6 Distribution Center

(21) Every SCMS Provider shall have a Distribution Center, where the following public information shall be available, if applicable:

(a) certificates included in the chain (Root CA, ICA, ECA, ACA),

(b) CCF,

(c) CRLs,

(d) composite CRL, including CTL according to IEEE 1609.2.1.,

(e) CTLs,

(f) CRLs for all CRACA according to IEEE 1609.2.1., if CRL Signer is used

1.3.5.7 Linkage Authority (LA)

(22) As stated in IEEE 1609.2.1: A component of the Security Credential Management System that provides inputs to the linkage value calculation process to enable efficient revocation (large number in one step) of pseudonym certificates while preserving the privacy of an End Entity against the Authorization Certificate Authority (ACA).

1.3.5.8 Misbehavior Authority (MA)

(23) As stated in IEEE 1609.2.1: A component of the Security Credential Management System that receives reports of malicious or potentially malicious application activities, analyzes them, and determines whether or not to take mitigating actions. An MA operates in cooperation with LA, RA and ACA.

(24) An MA should cooperate with all SCMS Providers published on the CTL.

(25) An MA should provide linking information for reported ACs.

(26) An MA should support the end entity revocation requests from other MAs.

1.3.5.9 Registration Authority (RA)

(27) Based on IEEE 1609.2.1: A component of the Security Credential Management System that is generally the main point of contact for an End Entity and is responsible for provisioning the EE with authorization and successor enrollment certificates. RA also provides system information.

(28) The tasks of an RA are the following:

(a) supporting the authorization certificate provision to valid end entities,

(b) supporting the successor enrollment certificate provision to valid end entities,

(c) providing system information for end entities (CTL, Certificate chain certificates, CRL, CCF,)

(d) forwards misbehavior reports for MA.

(29) With regard to (15) the RA

(a) shall support:

(1) IEEE 1609.2.1 enrollment certificates for authorization certificate request.

(b) may support (and document in its CPS if this is the case):

(1) X.509 certificates for authorization certificate request,

(2) OAuth access token for authorization certificate request at RA.

1.3.5.10 Device Configuration Manager (DCM)

(30) An optional component of the SCMS that is responsible for bootstrapping an EE and providing secure connection between the EE and the ECA (as defined in the IEEE 1609.2.1.)

1.3.6 End Entity

(31) The End Entities which use certificates and relate keys to sign and/or encrypt messages for different applications.

1.4 Certificate usage

1.4.1 Applicable domains of use

(32) Certificates issued under the present CP are intended to be used to validate digital signatures and encryption/decryption in the SCMS V2X communication context.

(33) The certificate profiles defined in IEEE 1609.2.1 determine the certificate usages of the SCMS ecosystem entities.

1.4.2 Limits of responsibility

(34) Certificates are not intended, nor authorized, for use in:

(a) circumstances that offend, breach or contravene any applicable law, regulation, decree or government order,

(b) circumstances that breach, contravene or infringe the rights of others,

(c) breach of this CP or the relevant subscriber agreement,

(d) any circumstances where their use could lead directly to death, personal injury or severe environmental damage (e.g. through failure in the operation of nuclear facilities, aircraft navigation or communication, or weapons control systems),

(e) circumstances that contravene the overall objectives of greater road safety and more efficient road transport in North America, Australia, Korea, Japan or another jurisdiction.

1.5 Policy administration

This Certificate Policy is managed by the SCMSMO's Policy Committee.

The contact email address for this Committee: policy@scmsmo.org

1.5.1 Updating of this certificate policy

(35) The update of this certificate policy is managed by the Policy Committee of the SCMSMO (SCMSMO). Each Contributor member can participate in the update of this CP.

1.5.2 Updating of CPSs of CAs listed in the CTL

(36) Each Root CA listed in the CTL shall publish its own CPS, which must follow this policy. A Root CA may add additional requirements but shall ensure that all requirements of this CP are met at all times.

(37) Each Root CA listed in the CTL shall implement an appropriate change process for its CPS document.

(38) The change process shall ensure that all changes to this CP are carefully analyzed and, if necessary for compliance with the CP as amended, the CPS is updated within the timeframe laid down in the implementation step of the change process for the CP. In particular, the change process shall involve emergency change procedures that ensure timely implementation of securityrelevant changes to the CP.

(39) The change process shall include appropriate measures to verify CP compliance for all changes to the CPS. Any changes to the CPS shall be clearly documented.

(40) The Root CA shall notify the SCMSMO's CTL Committee of any change made to the CPS with at least the following information:

(a) an exact description of the change,

(b) the rationale for the change,

(c) contact details of the person responsible for the CPS,

(d) planned timescale for implementation.

(41) The Root CA shall notify and send its CPS to its accredited auditor if any change was made to the CPS.

1.5.3 CPS approval procedures

(42) Before starting their services (point in time audit), or at the periodic reevaluation under this CP, the SCMS model elements (Elector, Root CA, ICA, ECA, ACA, RA, MA, LA, CRL Signer, DC) shall present their CPS to an accredited auditor as part of their compliance audit.

(43) Based on the audit results of Root CA/Elector, the SCMSMO's CTL Committee can decide about the addition of Root CA/Elector to the CTL.

(44) Based on the audit results and the CPS of Sub-CA or other SCMS elements, the issuing CA can evaluate the risks of interoperation with that SCMS element.

1.6 Definitions and acronyms

(45) The definitions and acronyms of IEEE 1609.2.1-2022 (Section 3.1 and 3.2) apply.

For easy reading, they are referenced below:

Application Activities: The activities that are carried out to achieve the business or operational goals of a distributed application.

Application Domain: The collection of application instances and management services that carry out and support a specific collection of application activities.

Application Instance: A single instance of an implementation of a component of a distributed application, running on a single device (or perceived as running on a single device from the perspective of other participants in the application domain).

Authorization Certificate: A certificate that is used to authorize application activities. Contrast: enrollment certificate.

Authorization Certificate Authority (ACA): A Certificate Authority (CA) whose main responsibility is to issue authorization certificates.

Binary Hash Tree: A data structure in which each node at level l + 1 has its value derived by applying a hash function to its parent node at level l, such that the publication of one node value at level l + 1 allows the derivation of all node values at levels l and below.

Blocked Enrollment Certificate: An enrollment certificate that has been determined to be no longer eligible to authorize certificate requests or certificate download requests.

Butterfly Key: The final cryptographic public key or private key produced by the butterfly key process.

Butterfly Key Certificate Request: A request created by an End Entity that is intended to result in the issuance of multiple certificates, with the keys in those certificates created via the butterfly key process.

Butterfly Key Expander (BKE): A component of the Security Credential Management System that adds an additional random elliptic curve point to each cocoon public key to create the butterfly public key (or the implicit certificate) for an explicit certificate.

Butterfly Key Parameters: The caterpillar public key and the expansion function used in the butterfly key process.

Butterfly Key Process: A process used in certificate generation where an initial caterpillar public key is modified using an expansion function by the Cocoon Key Expander (CKE) to create a cocoon public key, and further modified by a BKE to produce a butterfly public key (or an implicit certificate) for an explicit certificate, in such a way that only the holder of the original caterpillar private key can derive the butterfly private key

corresponding to the butterfly public key (or, the implicit certificate). It is infeasible for a party that does not know the caterpillar private key to derive the corresponding butterfly private key.

Butterfly Private Key: The final cryptographic private key produced by the butterfly key process.

Butterfly Public Key: The final cryptographic public key produced by the butterfly key process.

Canonical Identifier: A device identifier used to look up the device's canonical key.

Canonical Key: A device key with a long lifetime, used to request enrollment certificates. canonical key acceptance policy: A set of conditions applied to a canonical key and its metadata to determine whether that key is acceptable to authorize an enrollment certificate request received by a particular Enrollment Certificate Authority (ECA).

Caterpillar Key: The initial cryptographic public key or private key input to the butterfly key process.

Caterpillar Private Key: The initial cryptographic private key input to the butterfly key process.

Caterpillar Public Key: The initial cryptographic public key input to the butterfly key process.

Certificate Acceptance Policy: A policy setting constraints on the digital certificates (ITU-T Recommendation X.509 or IEEE Std 1609.2 based) that may be used to authorize certain activities.

Certificate Acceptance Policy: A statement of properties that a SCMS component certificate is required to have when it is used to authenticate that SCMS component in the context of a Transport Layer Security (TLS) session.

Certificate Trust List (CTL): A list of the Electors and the root certificate authorities (Root CAs) that are trusted by a particular SCMS Manager, signed by the eligible Electors.

Characterization Parameters: Parameters used to indicate properties of a protocol mechanism (secure session or Web API) specified in this document, with the purpose of making the properties of a composite protocol (secure session + Web API) clear.

Client (of a registration authority [RA]): Any entity within the system that uses a particular Registration Authority (RA) for certificate management activities.

Cocoon Key Expander (CKE): A component of the SCMS that uses the expansion function to create a series of statistically uncorrelated cocoon public keys.

Cocoon Key: The intermediate cryptographic public key or private key produced by applying an expansion function to a caterpillar key in the

butterfly key process.

Cocoon Private Key: The intermediate cryptographic private key produced by applying an expansion function to a caterpillar private key in the butterfly key process.

Cocoon Public Key: The intermediate cryptographic public key produced by applying an expansion function to a caterpillar public key in the butterfly key process.

Delegated Registration Authority: An organization responsible for assigning identifiers, or identifier sets, from a designated range of values of the identifier CtlSeriesId defined in this standard. The name indicates that the authority to assign from the indicated range has been assigned to the delegated registration authority by the IEEE Registration Authority.

Derivable Node: A node in a binary hash tree whose value can be derived from published node values.

Device Configuration Manager (DCM): A component of the SCMS that is responsible for bootstrapping an End Entity and providing secure connection between the EE and the Enrollment Certificate Authority (ECA).

Direct Authorization (for enrollment certificate request): A mode of authorization for enrollment certificate request where the enrollment certificate request generated by an EE device contains a proof that the device is entitled to that enrollment certificate.

Direct Communication: communication between road user and the infrastructure directly. (for example PC5).

Distribution Center (DC): A component of the SCMS that distributes public information such as certificates and certificate revocation lists. Contrast: Registration Authority.

Elector: A component of the SCMS that manages trust of Root Certificate Authority (Root CA) certificates and peer Elector certificates.

End Entity (EE): An actor that uses digital certificates to authorize application activities. Contrast: Certificate Authority (CA).

End Entity Node: A bottom-layer node in a binary hash tree used to calculate an Activation Codes for Pseudonym Certificates (ACPC) private activation value (APrV).

Enrollment Certificate: A certificate that is used to request authorization certificates and to manage other interactions between an EE and the SCMS. Contrast: authorization certificate.

Enrollment Certificate Authority (ECA): A Certificate Authority (CA) that issues enrollment certificates.

Expansion Function: A function used to produce cocoon keys from a caterpillar key in the butterfly key process.

Identification Certificate: An authorization certificate that is constructed so as not to deliberately obscure the real-world identity of the certificate

holder. Contrast: pseudonym certificate.

Identifying Uniform Resource Locator (URL): A resource locator that acts as a long-lived identifier for an SCMS component.

IEEE Registration Authority (IEEE RA): A unit of IEEE that assigns unambiguous names to objects in a way that makes the assignment available to interested parties.

Indirect Authorization (for enrollment certificate request): A mode of authorization for enrollment certificate request where the enrollment certificate request generated by an EE device does not contain a proof that the device is entitled to that enrollment certificate, and the proof is instead provided to the ECA by some other means.

Individual Certificate Request: A request for a CA to issue a single certificate. The request may come from the relevant EE or from the RA. Contrast: butterfly key certificate request.

Intermediate Certificate Authority (ICA): A CA whose certificate was issued by another CA and whose main responsibility is to issue certificates to another CA, that is, an ACA, ECA, or another ICA.

i-period: A validity period for a certificate, identified by an i-value to simplify management of temporal sequences of certificates issued to an EE.

i-period epoch: The date at which i-periods of the indicated length started.

i-period length: The length of time that an i-period lasts.

i-period series: A series of temporal intervals, each of the same length, identified by an i-value that increases by one for each successive interval.

ITU-T X.509 certificate: A digital certificate following the format specified in ITU-T Recommendation X.509.

i-value: An integer identifying an i-period.

j-value: An integer identifying the index within an i-period.

Linkage Authority (LA): A component of the SCMS that provides inputs to the linkage value calculation process to enable efficient revocation of pseudonym certificates while preserving the privacy of an EE against the ACA.

Location Obscurer Proxy (LOP): A component of the SCMS that is responsible for hiding location information of an EE from the RA.

Minimal Length Hex Encoding (of an integer): The encoding of an integer with the minimum necessary number of hexadecimal characters. For example, an i-value of 76 is encoded as 0x4C. Examples of quantities that will be subject to minimal length hex encoding include i-values, j-values, and Provider Service Identifiers (PSIDs).

Misbehavior Authority (MA): A component of the SCMS that receives reports of malicious or potentially malicious application activities, analyzes them, and determines whether or not to take mitigating actions.

Omitted Node: A node in a binary hash tree whose value is omitted from the encoding of the binary hash tree and whose value cannot be derived from published nodes. Contrast: published node.

Parent Enrollment Certificate: An enrollment certificate that maintains continuity of ownership with a subsequent enrollment certificate (a successor enrollment certificate), such that if a certificate management activity could be authorized with the parent enrollment certificate that same activity can also be authorized with the successor enrollment certificate.

Physically Secure Session: A communications session in which security is provided by the fact that both endpoints of the session are in the same physically secure environment.

Privacy Against Insiders: A property of a system such that the system protects users of the system from having personal information revealed even to privileged actors within that system.

Private Key: A cryptographic key, used for key exchange, decryption, and/or signature generation, that has a corresponding public key such that the private key cannot feasibly be derived from the public key using public information.

Pseudonym Certificate: An authorization certificate that is designed to help protect the privacy of an EE. This is achieved using mechanisms such as linkage valued-based revocation. An EE that uses pseudonym certificates will typically have multiple certificates valid at the same time to allow that EE to use different certificates at different times and locations, disrupting an eavesdropper's ability to track them.

Public Key: A cryptographic key, used for key exchange, encryption, and/or signature verification, that has a corresponding private key such that the private key cannot feasibly be derived from the public key using public information.

Public Key Infrastructure (PKI): A system of certificate authorities and supporting entities to support the management of digital certificates and public keys.

Published Node: A node in a binary hash tree whose value is published in the encoding of the binary hash tree or can be derived from the values of other published nodes. Contrast: omitted node.

Registration Authority (RA): A component of the SCMS that is the main point of contact for an EE, and is responsible for provisioning the EE with authorization and successor enrollment certificates. Contrast: Distribution Center (DC), IEEE Registration Authority (IEEE RA).

Relying party: A participant of the ecosystem, who is consuming the signed datasets provided by the ecosystem.

Root Certificate Authority (Root CA): A CA that issues certificates for other entities and whose certificate was issued by itself.

Security Credential Management System (SCMS): A system of certificate authorities and supporting entities to support distribution of trust in a system based on IEEE 1609.2 digital certificates.

Security Credential Management System Manager Organization (SCMSMO): A role aimed at governing the entire SCMS, including defining and enforcing the certificate and security policies to be applied to Electors and Root CAs.

Successor Enrollment Certificate: An enrollment certificate that maintains continuity of ownership with a previous enrollment certificate (a parent enrollment certificate), such that if a certificate management activity could be authorized with the parent enrollment certificate that same activity can also be authorized with the successor enrollment certificate.

Transport Layer Security (TLS): A security protocol developed and maintained by the Internet Engineering Task Force (IETF) providing confidentiality, integrity, and authentication services.

Validity Period (of a certificate): The time period during which a certificate is to be trusted. In the IEEE 1609.2 system, this is indicated by the validityPeriod field in the certificate, that is, the time period starting at validityPeriod.start and ending at (validityPeriod.start + validityPeriod. duration).

Acronym or abbreviation	Meaning
ACPC	Activation Codes for Pseudonym Certificates
ACA	Authorization Certificate Authority
AES	Advanced Encryption Standard
APDU	Application Protocol Data Unit
API	Application Programming Interface
APrV	Activation Codes for Pseudonym Certificates (ACPC) private activation value
APuV	Activation Codes for Pseudonym Certificates (ACPC) public activation value
ASD	Aftermarket Safety Device
AT	Access Token
CA	Certificate Authority
CAM	Certificate Access Manager
CAMP	Crash Avoidance Metrics Partners LLC
CAL	Certificate Access List
CCF	Certificate Chain File
CCG	Client Credentials Grant
C-OER	Canonical Octet Encoding Rules
CRACA	Certificate Revocation Authorizing Certificate Authority
CRL	Certificate Revocation List
CTL	Certificate Trust List
DC	Distribution Center
DCM	Device Configuration Manager

Acronym or abbreviation	Meaning
DER	Distinguished Encoding Rules
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ECA	Enrollment Certificate Authority
ECC	Elliptic Curve Cryptography
EE	End Entity
ECDSA	Elliptic Curve Digital Signature Algorithm
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
I2V	Infrastructure-to-Vehicle
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITS	Intelligent Transportation Systems
JSON	JavaScript Object Notation
JWKS	JavaScript Object Notation (JSON) Web Key Set
JWT	JavaScript Object Notation (JSON) Web Yoken
LA	Linkage Authority
LOP	Location Obscurer Proxy
LV	Linkage Value
M2M	Machine-to-Machine
NAT	Network Address Translation
OAS	OAuth Authorization Server
OBU	On-board Unit
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
OER	Octet Encoding Rules
OID	Object Identifier
P2PCD	Peer-to-Peer Certificate Distribution
PCA	Pseudonym Certificate Authority
PKI	Public Key Infrastructure
PLV	Pre-linkage Value
PSID	Provider Service Identifier
RA	Registration Authority
REST	Representational State Transfer
RFC	Request for Comments
RSU	Roadside Unit
SAS	Supplementary Authorization Server
SCMS	Security Credential Management System
SCMSMO	Security Credential Management System Manager Organization
SPDU	Secured Protocol Data Unit
SSME	Security Services Management Entity
SSP	Service Specific Permissions
TLS	Transport Layer Security
URL	Uniform Resource Locator

Acronym or abbreviation	Meaning
USDOT	United States Department of Transportation
UTC	Coordinated Universal Time
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
WAVE	Wireless Access in Vehicular Environments
WSA	Wireless Access in Vehicular Environments (WAVE) Service Advertisements

2 Publication and repository responsibilities

2.1 Methods for the publication of certificate information

(46) The publication methods are described in Section 2.5.

2.2 Time or frequency of publication

(47) The SCMSMO shall publish its CTL within 15 days after an addition. In the case of removal, a new CTL shall by published in 24 hours.

(a) The SCMSMO shall publish its CP within 15 days after accepted modification.

(b) The SCMSMO shall publish the new Elector certificates when they start their operation.

(48) SCMS Providers shall publish their newly issued CA certificates as they start operation via DC and/or RA.

(a) (45a) The SCMS Providers shall publish CPS within 15 days after the accepted modification.

(49) SCMS Providers shall publish their CRLs 24 hours after a status change via DC and/or RA.

2.3 Repositories

(50) The SCMSMO shall publish in its Publication Center the information listed in Section 1.3.3.1

(51) Every SCMS Provider shall publish either in its Distribution Center or in the RA the information listed in Section 1.3.5.6

2.4 Access controls on repositories

(52) The Publication Center of the SCMSMO shall be publicly available.

(53) The Distribution Center shall be publicly available.

(54) The modification of entries in DC, PUB or RA Repository shall have access controls and comply at least with the general standards of secure

information-handling outlined in WebTrust for CAs v2.1 (actual version) or SOC2 Trust Services or in ISO/IEC 27001 or TISAX (actual version).

(55) The SCMS Providers shall include in the CPS what type of authentication they support for access controls on their repositories.

2.5 Publication of certificate information

2.5.1 Publication of information by the SCMSMO

(56) The SCMSMO shall publish in its Publication Center the information listed in Section 1.3.3.1

2.5.2 Publication of information by an SCMS Provider

(57) Every SCMS Provider shall publish either in its Distribution Center or in the RA the information listed in Section 1.3.5.6

2.5.3 Publication of Information by a RA

(58) The RA shall publish the information listed in Section 1.3.5.6

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

3.1.1.1 Names for Electors and Root CAs

(59) The Elector and Root CA certificate shall contain a single and unique value based on the request and approved by the SCMSMO as a CertificateId attribute of the name in accordance to IEEE 1609.2.1. The SCMSMO is responsible for the uniqueness of names within its system.

3.1.1.2 Names for ICA

(60) The ICA certificate shall contain a single and unique value allocated by the SCMS Provider of its issuing CA as a CertificateId attribute of the name in accordance with IEEE 1609.2.1.

3.1.1.3 Names for ACA

(61) The ACA certificate shall contain a single and unique value allocated by the SCMS Provider of its issuing ICA as a CertificateId attribute of the name in accordance with IEEE 1609.2.1.

3.1.1.4 Names for ECA

(62) The ECA certificate shall contain a single and unique value allocated by the SCMS Provider of its issuing ICA as a CertificateId attribute of the name in accordance with IEEE 1609.2.1.

(63) The ECA shall have an identifying URL as defined in IEEE 1609.2.1. The *Id* field should be equal to the identifying URL.

3.1.1.5 Names for RA

(64) The RA certificate may contain a single and unique value allocated by the SCMS Provider of its issuing RA certificate as a CertificateId attribute of the type name in accordance with IEEE 1609.2.1.

(65) The RA shall have an identifying URL as defined in IEEE 1609.2.1. The *Id* field should be equal to the identifying URL.

3.1.1.6 Names for DC

(66) The DC certificate may contain a single and unique value allocated by the SCMS Provider of its issuing RA certificate as a CertificateId attribute of the type name in accordance with IEEE 1609.2.1.

(67) The DC shall have an identifying URL as defined in IEEE 1609.2.1. The *Id*

field should be equal to the identifying URL.

3.1.1.7 Names for MA and LA

No stipulation.

3.1.1.8 Names for End Entity certificates

(68) The enrollment certificates of end entities may contain a single CertificateId attribute in accordance with IEEE 1609.2.1. The ECA is responsible for the uniqueness of these *Id*s.

(69) The authorization shall be direct. A unique identifier, known as the canonical identifier, it shall be registered by the ECA together with the canonical public key to authenticate and authorize the initial enrollment certificate request, according to IEEE 1609.2.1.

(70) The Authorization certificates of end entities in accordance with IEEE 1609.2.1. may contain a single CertificateId attribute of type linkageData for Linkage-based certificate identifiers and binaryId, or none for Hash ID-based certificate identifiers.

3.1.1.9 Identification of certificates

(71) A certificate following the IEEE 1609.2 format shall be identified by its HashedId8 value.

3.1.2 Need for names to be meaningful

No stipulation.

3.1.3 Anonymity and pseudonymity of end-entities

(72) An authorization certificate shall not contain any name or information that links the subject to its real identity. The ACA and RA responsible for this.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

(73) The Elector, Root CA, ICA, ACA, LA, MA names shall be unique.

(74) The canonical IDs for End Entities shall be unique.

(75) The SCMSMO shall ensure that a Root CA 3-byte hash certificate identifier (HashedId3) is unique in the scope of the overall trust model.

NOTE: This is needed because a Root CA might be applied also as a CRACA ID in a Sub-CA certificate, and that needs a unique HashedId3 value.

(76) The SCMS Provider of Root CA and ICA shall ensure that the HashedId8 certificate identifier of each Sub-CA is unique.

(77) The enrollment certificate's HashedId8 shall be unique within the issuing ECA.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

(78) The participant shall prove that it holds the private key corresponding to the public key included in its certificate and this proof shall be checked by the relevant entity. The following table shows which actor is relevant for checking the key ownership of each actor.

Key owner	The actor responsible for the verification	Comments
Elector	SCMSMO	self-signed IEEE 1609.2 certificate
Root CA	SCMSMO	self-signed IEEE 1609.2 certificate
ICA	Root CA	-
ECA	ICA	-
ACA	ICA	-
RA	ICA	-
LA	ICA	-
MA	ICA	-
CRL Signer	Corresponding CA	-
DC	Corresponding CA	-

3.2.2 Authentication of organization identity

3.2.2.1 Authentication of Elector organization identity

(79) The Elector shall provide to the SCMSMO evidence of the identification and accuracy of the name and associated data. The CTL Committee is responsible for validation of the Elector.

(80) The subject's organization identity shall be verified at the time of certificate enrollment for Elector signatures by the SCMSMO using appropriate means and in accordance with the present certificate policy.

(81) The organization evidence provided shall include the same as specified in Section 3.2.2.2.

3.2.2.2 Authentication of Root CAs' organization identity

(82) In an application form to the SCMSMO, the Root CA shall provide the identity of the organization and registration information, composed of:

(a) organization name,

(b) postal address,

(c) e-mail address,

(d) the name of a physical contact person in the organization,

(e) telephone number,

(f) digital fingerprint (i.e. SHA 256 hashvalue) of the Root CA's certificate in printed form,

(g) cryptographic information (i.e. cryptographic algorithms, key lengths) in the Root CA certificate,

(h) all permissions that the Root CA is allowed to use and to pass to the subCAs.

(83) The SCMSMO shall check the identity of the organization and other registration information provided by the certificate applicant for the insertion of a Root CA certificate in the CTL.

(84) The SCMSMO shall collect either direct evidence, or an attestation from an appropriate and authorized source (e.g. company registration document), of the identity (e.g. name) and, if applicable, any specific attributes of subjects to which a certificate is issued. Submitted evidence may be in the form of paper or electronic documentation.

(85) The subject's organization identity shall be verified at the time of registration by appropriate means and in accordance with the present certificate policy.

(86) At each certificate application, evidence shall be provided of:

(a) the full name of the organizational entity (private organization, government entity or non-commercial entity),

(b) nationally recognized registration or other attributes that may be used, as far as possible, to distinguish the organizational entity from others with the same name.

3.2.2.3 Authentication of SubCAs organization identity

(87) The Root CA shall check the identity of the organization and other registration information provided by applicants for ICA certificates.

(88) The ICA shall check the identity of the organization and other registration information provided by applicants for ACA, ECA, LA, MA, RA certificates.

(89) The issuing CA shall check the identity of the organization and other registration information provided by applicants for CRL Signer and DC certificates.

(90) At a minimum, the issuing CA shall:

(a) determine that the organization exists by using at least one thirdparty identity proofing service/database or, alternatively, organizational documentation issued by or filed with the relevant government agency or recognized authority that confirms the existence of the organization,

(b) require the certificate applicant to confirm certain information about the organization, that it has authorized the certificate application and that the person submitting it on behalf of the applicant is authorized to do so. Where a certificate includes the name of an individual as an

authorized representative of the organization, it shall also confirm that it employs that individual and has authorized him/her to act on its behalf.

(91) Validation procedures for issuing CA certificates shall be documented in a CPS of the issuing CA (Root CA and ICA).

3.2.2.4 Authentication of End Entities' subscriber organization

(92) Before the subscriber (manufacturer/operator) can register with a trusted ECA to enable its End Entities for sending EC certificate requests, the ECA shall:

(a) check the identity of the subscriber organization and other registration information provided by the certificate applicant,

(b) check that the EE type (i.e. the concrete product based on brand, model and version of the EE) meets all the following compliance assessment criteria:

(1) certificate of compliance with the SCMSMO's CP,

(2) confirm standards compliance and interoperability validation via third-party certification as defined by OmniAir or equivalent scheme,

(3) declaration of full conformity with SCMS Manager 'End Entity Security Requirements, Design Guidance, and Validation Approach'; further profiles can be agreed on by the SCMSMO Policy Committee.

(93) At a minimum, the ECA shall:

(a) determine that the organization exists by using at least one thirdparty identity proofing service/database or, alternatively, organizational documentation issued by or filed with the relevant government agency or recognized authority that confirms the existence of the organization,

(b) require the certificate applicant to confirm certain information about the organization, that it has authorized the certificate application and that the person submitting the application on its behalf is authorized to do so. Where a certificate includes the name of an individual as an authorized representative of the organization, it shall also confirm that it employs that individual and has authorized him/her to act on its behalf.

(94) Validation procedures for EE subscribers shall be documented in a CPS of the ECA.

3.2.3 Authentication of individual entity

3.2.3.1 Authentication of Elector/Sub-CA/other SCMS model elements individual entity

(95) For the authentication of an individual entity (physical person) identified in association with a legal person or organizational entity (e.g. the subscriber),

evidence shall be provided of:

(a) full name of the subject (including surname and given names, in line with the applicable law and national identification practices),

(b) date and place of birth, reference to a nationally recognized identity document or other attributes of the subscriber that may be used, as far as possible, to distinguish the person from others with the same name,

(c) full name and legal status of the associated legal person or other organizational entity (e.g. the subscriber),

(d) any relevant registration information (e.g. company registration) of the associated legal person or other organizational entity,

(e) evidence that the subject is associated with the legal person or other organizational entity.

Submitted evidence may be in the form of paper or electronic documentation.

(96) To verify his/her identity, the authorized representative of SCMS model elements or a subscriber shall provide documentation proving that he/she works for the organization (certificate of authorization). He/she shall also show an official ID.

(97) For the initial enrollment certificate process, a representative of the Sub-CA or other SCMS model elements shall provide the corresponding issuing CA with all necessary information.

(98) The personnel at the Root CA/ICA shall verify the identity of the certificate applicant (representative) and all associated documents, applying the requirements of 'trusted personnel' (i.e. the process of validating application information and generating the certificate by the Root CA/ICA shall be carried out by 'trusted persons' at the Root CA/ICA, under at least dual supervision, as they are sensitive).

3.2.3.2 Authentication of End Entities' subscriber identity

(99) EE subscribers are represented by authorized end-users in the organization who are registered at the ECA. These end-users designated by organizations (manufacturers or operators) shall prove their identity and authenticity before:

(a) being registered at the corresponding ECA, including its canonical public key, canonical ID (unique identifier) and permissions in accordance with the EE.

3.2.3.3 Authentication of End Entities' identity

(100) EE subjects of enrollment certificates shall authenticate themselves when requesting enrollment certificates by using direct authentication.

(101) The ECA shall check the authentication using the canonical public key corresponding to the EE.

(102) EEs shall authenticate themselves when requesting authorization certificates by using their unique enrollment certificate or X.509 certificate.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

3.2.5.1 Validation of Elector, Root CA, ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC

(103) Every organization shall identify in its CPS at least one representative role (e.g. a security officer) responsible for requesting new certificates and renewals.

3.2.5.2 Validation of End Entity subscribers

(104) At least one representative role (e.g. security officer) responsible for registering End Entities shall be known to and approved by the Enrollment CA.

3.2.5.3 Validation of End Entities

(105) The EE subscriber shall confirm and provide the evidence to the SCMS Provider that each device has met any required device or application certifications prior to enrollment.

3.2.6 Criteria for interoperation

(106) For communication between EEs and the SCMS, model element interfaces defined by the IEEE 1609.2.1 shall be implemented.

(107) The RA and ACA shall support authorization certificate requests and responses that comply with IEEE 1609.2.1

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for standard re-key requests

3.3.1.1 Elector certificates

No stipulation.

3.3.1.2 Root CA certificates

No stipulation.

3.3.1.3 ICA, ECA, RA, ACA, LA, MA, CRL signer, DC certificate renewal or re-keying

(108) Prior to the expiry of a Sub-CA or other SCMS model elements, the Sub-CA or other SCMS model elements shall request a new certificate to maintain continuity of certificate usage. The Sub-CA or other SCMS model elements shall generate a new key pair to replace the expiring key pair and sign the re-key request containing the new public key with the current valid private key ('re-keying'). The Sub-CA or other SCMS model elements shall generate a new key pair and sign the request with the new private key (inner signature) to prove delivery/possession. The whole request shall be signed ('oversigned') with the current valid private key (outer signature) to ensure the integrity and authenticity of the request. If an encryption and decryption key pair is used, possession of private decryption keys shall be proven.

(109) The identification and authentication method covering routine re-keying for other SCMS model elements/entities shall be the same as that for the issuance of an initial CA certificate validation.

3.3.1.4 End Entities' enrolment credentials

(110) Prior to the expiry of an existing enrollment certificate, the EE shall request a successor certificate to maintain continuity of certificate usage. The EE shall generate a new key pair to replace the expiring one and request a successor certificate containing the new public key; the request shall be signed with the current valid enrollment certificate private key.

(111) The EE shall sign the enrollment certificate request with the newly-created private key (inner signature) to prove delivery/possession. The EE shall then sign the whole request ('oversigned') with the current valid private key (outer signature) and encrypted to the receiving RA or ECA as specified in IEEE 1609.2.1, to ensure the confidentiality, integrity and authenticity of the request.

3.3.1.5 End Entities' authorization certificates

(112) The certificate re-key for authorization certificates is based on the same process as the initial authorization.

3.3.2 Identification and authentication for re-key requests after revocation

3.3.2.1 CA certificates

(113) The identification and authentication process for a Root CA and a Sub-CA certificate re-keying after revocation shall be handled in the same way as the initial issuance of that certificate.

3.3.2.2 End Entity certificates

(114) The authentication of an End Entity for enrollment or authorization certificate re-keying after revocation shall be handled in the same way as the initial issuance of that certificate.

3.4 Identification and authentication for revocation request

3.4.1.1 Elector and Root CA certificates

(115) If an Elector or a Root CA decides to request its removal from the CTL, the request shall be authenticated by the Elector/Root CA via the SCMSMO.

(116) Acceptable procedures for authenticating a subscriber's revocation requests include:

(a) a written and signed message on corporate letter paper from the subscriber requesting revocation, with reference to the certificate to be revoked,

(b) communication with the SCMS Provider providing reasonable assurances that the person or organization requesting revocation is in fact the subscriber; depending on the circumstances, such communication may include one or more of the following: e-mail, postal mail or courier service.

3.4.1.2 ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC certificates

(117) Requests to revoke ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC certificates shall be authenticated by the issuing CA.

(118) Acceptable procedures for authenticating a subscriber's revocation requests include:

(a) a written and signed message on corporate letter paper from the subscriber requesting revocation, with reference to the certificate to be revoked,

(b) communication with the SCMS Provider reasonable assurances that the person or organization requesting revocation is in fact the subscriber; depending on the circumstances, such communication may include one or more of the following: e-mail, postal mail or courier service.

3.4.1.3 End Entity enrollment certificates and authorization certificates

(119) A request to revoke an EE enrollment certificate can originate from the EE subscriber or from MA. If initiated by the subscriber, requesters shall authenticate themselves with the MA.

(120) A request to revoke an EE authorization certificate can originate from the EE subscriber or from MA. If initiated by the subscriber, the requester shall authenticate themselves with the MA.

4 Certificate lifecycle operational requirements

4.1 Certificate application

(121) The term 'certificate application' refers to the following processes:

(a) registration and setup of a trust relationship between the Electors and the SCMSMO including the insertion of the Elector certificate in the CTL,

(b) registration and setup of a trust relationship between the Root CA and the SCMSMO, including the insertion of the first Root CA certificate in the CTL,

(c) registration and setup of a trust relationship between the ICA and the Root CA, including the issuance of a new ICA certificate,

(d) registration and setup of a trust relationship between the ECA, RA, ACA, LA, MA, CRL Signer, DC and the ICA, including the issuance of a new certificate for ECA, RA, ACA, LA, MA, CRL Signer, CRACA, DC,

(e) registration of the EE at the ECA or X.509 CA by the manufacturer/operator/DCM,

(f) End Entity's request for an enrollment certificate and authorization certificate.

(122) The certificate application shall be validated and also the identity of person submitting the application shall be verified.

4.1.1 Who can submit a certificate application

4.1.1.1 Elector

(123) The Elector shall generate its own key pairs and issue a certificate by itself. The Elector shall submit a certificate application for endorsement through its designated representative to the SCMSMO.

4.1.1.2 Root CA

(124) Root CAs shall generate their own key pairs and issue their root certificate by themselves. A Root CA can submit a certificate application for endorsement through its designated representative to the SCMSMO.

4.1.1.3 ICA

(125) An authorized representative of the ICA shall submit the certificate request application to the relevant Root CA.

4.1.1.4 ECA, RA, ACA, LA, MA, DC

(126) An authorized representative of ECA, RA, ACA, LA, MA, DC shall submit the certificate request application to the relevant ICA.

4.1.1.5 CRL Signer

(127) An authorized representative of a CRL Signer shall submit the certificate request application to the authorized representative of the relevant CRACA.

4.1.1.6 End Entity

(128) Subscribers shall register their EEs at the ECA either directly or via DCM. EE subscribers may register their end entities also to a X.509 CA, if the ECA supports enrollment request based on an X.509 certificate.

(129) Each EE registered at the ECA or X.509 CA may send enrollment certificate requests according to IEEE 1609.2.1.

(130) Each EE may send authorization certificate requests without demanding any subscriber interaction. Before requesting an authorization certificate, an EE shall have a valid enrollment certificate or X.509 certificate that is trusted (registered and not blocked) by the RA.

4.1.2 Enrolment process and responsibilities

(131) Permissions for Root CAs' and Sub-CAs' to issue certificates for special (governmental) purposes (i.e. mobile and fixed EEs) where restricted by law may be granted only by the relevant authority having jurisdiction (under legislation) to authorize the requested credentials.

4.1.2.1 Electors

(132) After being audited and selected, the Elector is responsible for signing the CTL prepared by the SCMSMO's CTL Committee.

(133) The Elector's enrollment process is based on a signed application that shall be securely delivered to the SCMSMO by the Elector's authorized representative.

(134) The Elector's application shall be signed by its authorized representative.

(135) In addition to the application, the Elector's authorized representative shall provide a copy of the Elector's CPS and its audit results to the SCMSMO. If approved, the SCMSMO generates and sends a certificate of conformity to the corresponding Elector.

(136) The addition of the Elector to the CTL is an SCMSMO-defined internal process handled by the CTL Committee.

4.1.2.2 Root CAs

(137) After being audited, Root CAs may apply for insertion of their certificate(s) in the CTL.

(138) The enrolment process is based on a signed application that shall

be securely delivered to the SCMSMO by the Root CA's authorized representative.

(139) The Root CA's application form shall be signed by its authorized representative.

(140) In addition to the application form, the Root CA's authorized representative shall provide its audit results to the SCMSMO for approval. If approved, the SCMSMO generates and sends a certificate of conformity to the corresponding Root CA.

(141) The addition of the Root CA to the CTL is an SCMSMO-defined internal process handled by the CTL Committee.

4.1.2.3 ICA

(142) After being audited, the ICA may request a certificate from the Root CA.

(143) If the ICA is owned by a different entity than the Root CA, before issuing an ICA certificate request, the ICA's entity shall have a contract with the Root CA service.

4.1.2.4 ECA, RA, ACA, LA, MA, CRL Signer, DC

(144) After being audited, the ECA, RA, ACA, LA, MA, CRL Signer, DC may request a certificate from the ICA.

(145) If the ECA, RA, ACA, LA, MA, CRL Signer, DC is owned by a different entity than the ICA, before issuing a certificate request, the Sub-CA or other SCMS element entity shall have a contract with the ICA service provider.

4.1.2.5 End Entity

(146) The EE subscriber shall store the proof of certification for each device type that is enrolled at an ECA or X.509 CA.

(147) The EE subscriber can use multiple methods of authorization described in Section 1.3.5.3.

(148) The EE may generate an enrollment certificate key pair and create an enrollment certificate request in accordance with IEEE 1609.2.1.

(149) During the enrollment of a normal EE (as opposed to a special mobile or fixed EE), the Enrollment CA shall verify that the permissions in the initial request are not for governmental use. Such permissions are defined by the corresponding governmental entity. The detailed procedure for EE subscriber registration at the Enrollment CA shall be set out in the corresponding CPS of the ECA.

(150) Regular EEs should be enrolled at a single Enrollment CA and therefore bound to a single RA for all certificates with a particular set of permissions. Special-purpose vehicles (such as police cars and other vehicles with specific rights) may be processed by an additional Enrollment CA or enroll for authorization within the scope of the 'special purpose'. Vehicles to which such an exemption applies shall be defined by the responsible

governmental entity. Permissions for special mobile and fixed EEs shall be granted only with the approval of a jurisdictionally relevant government entity. The CPS of Root CAs or Sub-CAs issuing certificates for such special-purpose EEs shall determine the applicable enrollment process.

(151) If the EE is in the process of migrating from one Enrollment CA to another, it is permitted to be enrolled at two CAs simultaneously for that period.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

4.2.1.1 Identification and authentication of Elector/Root CAs

(152) The SCMSMO is responsible for authenticating the Elector/Root CA's authorized representative and approving its application. The application approval shall be done by the CTL committee.

(153) The SCMSMO shall confirm its positive validation of the application to the Root CA/Elector. The Elector/Root CA may then send its 'self-signed' certificate to the SCMSMO, which shall add the certificate of Root CA/ Elector to the CTL.

4.2.1.2 Identification and authentication of the ICA

(154) The corresponding Root CA is responsible for authenticating the ICA's authorized representative and approving its application.

(155) The Root CA shall confirm its positive validation of the application to the ICA. The ICA may then send a certificate request to the Root CA, which shall issue the certificate to the corresponding ICA.

4.2.1.3 Identification and authentication of ECA, RA, ACA, LA, MA, DC

(156) The corresponding ICA is responsible for authenticating the Sub-CA's or other SCMS element authorized representative and approving its application.

(157) The ICA shall confirm its positive validation of the application to the respective Sub-CA or other SCMS element. The Sub-CA or other SCMS element may then send a certificate request to the ICA, which shall issue the certificate to the corresponding Sub-CA or other SCMS element.

4.2.1.4 Identification and authentication of CRL signer

(158) The corresponding CRACA is responsible for authenticating the CRL Signer's authorized representative and approving its application.

(159) The corresponding CRACA shall confirm its positive validation of the application to the respective CRL Signer. The CRL Signer may then send a

request to the CRACA which shall issue the certificate to the corresponding CRL Signer.

4.2.1.5 Identification and authentication of EE subscriber

(160) The ECA is responsible for authenticating the EE subscriber. The Enrollment CA (SCMS ECA or X.509 CA) shall describe in its CPS the processes for EE subscriber authentication.

(161) The ECA shall confirm its positive validation of the application to the respective EE subscriber. The EE may then send a certificate request to the ECA, which shall issue the certificate to the corresponding EE.

4.2.1.6 Identification and authentication of EE

(162) During enrollment-stage certificate requests, in accordance with IEEE 1609.2.1, the ECA shall use at least one of the authentication options mentioned in Section 1.3.5.3.

(163) During successor enrollment certificate requests and downloads, in accordance with IEEE 1609.2.1, the RA shall use at least one of the authentication options for both EE and RA mentioned in Section 1.3.5.3

(164) During authorization certificate requests and downloads, in accordance with IEEE 1609.2.1, the RA shall verify the EE's enrollment certificate and authenticate the ECA or X.509 CA from which the EE received its enrollment certificate. If the RA is not able to authenticate the EE and ECA or X.509 CA, the request shall be rejected. The RA shall use at least one of the authentication options for both EE and RA mentioned in Section 1.3.5.9.

(165) During misbehavior report submission, in accordance with IEEE 1609.2.1, the RA shall use at least one of the authentication options mentioned in Section 1.3.5.9.

4.2.2 Approval or rejection of certificate applications

4.2.2.1 Approval or rejection of Elector/Root CA certificates

(166) The SCMSMO CTL Committee adds/removes the Root CA/Elector certificate to/from the CTL, when it is clear from the audit results and the CPS that the Root CA/Elector is in compliance with this CP.

4.2.2.2 Approval or rejection of ICA certificates

(167) The Root CA shall verify the ICA certificate request based on its audit results. If this verification leads to a positive result, the Root CA may issue a certificate to the requesting ICA.

4.2.2.3 Approval or rejection of ECA, RA, ACA, LA, MA, DC certificates

(168) The ICA shall verify the Sub-CAs or other SCMS element certificate request based on its audit results. If this verification leads to a positive result, the

ICA may issue a certificate to the requesting entity.

4.2.2.4 Approval or rejection of CRL Signer certificates

(169) The CRACA shall verify the CRL Signer certificate request based on its audit results. If this verification leads to a positive result, the CRACA may issue a certificate to the requesting entity.

4.2.2.5 Approval or rejection of enrollment certificate

(170) The Enrollment CA shall verify and validate enrollment certificate requests. If this verification leads to a positive result, the ECA may issue a certificate to the requesting entity.

4.2.2.6 Approval or rejection of authorization certificate

(171) The RA shall verify and validate authorization certificate requests. If this verification leads to a positive result, the ACA may issue a certificate to the requesting entity.

(172) The RA and the ACA shall accept and approve authorization requests if the following are fulfilled:

(a) actual, valid and relevant CRL and CTL are available at RA / DC,

(b) the Root CA certificate and ICA certificate of the CA's certificate chain were not revoked,

(c) Root CA certificate is listed on the actual, valid and relevant CTL.

4.2.3 Time to process the certificate application

4.2.3.1 ELECTOR, ROOT CA certificate application

(173) The time to process the identification and authentication process of an Elector/Root CA certificate application is 60 working days.

4.2.3.2 ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC certificate application

(174) The time to process the identification and authentication process of a certificate application is during working days in accordance with the agreement and contract between the Root CA and the ICA, and between the ICA and the SubCA or other SCMS element.

4.2.3.3 Enrollment certificate application

(175) The processing of enrollment certificate applications shall be subject to a maximum time limit laid down in the ECA's CPS.

4.2.3.4 Authorization certificate application

(176) The processing of authorization certificate applications shall be subject to a maximum time limit laid down in the RA's and ACA's CPS.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

4.3.1.1 Elector certificate issuance

(177) The Elector shall issue its own self-signed Elector certificate in IEEE 1609.2.1 format and shall send it to the SCMSMO.

(178) The SCMSMO shall take care that the Elector certificate is made available as soon as possible via PUB.

(179) An Elector shall sign the CTL prepared for them by the SCMSMO's CTL Committee.

4.3.1.2 Root CA certificate issuance

(180) The Root CA shall issue its own self-signed Root CA certificate in IEEE 1609.2.1 format and may send it to the SCMSMO for publication on the CTL.

(181) The SCMSMO's CTL Committee shall check the audit results and the CPS of the Root CA before adding the Root CA to the CTL.

(182) The SCMSMO shall take care that the root certificate is made available as soon as possible via CTL at PUB, cf. Section 2.5.1.

4.3.1.3 ICA certificate issuance

(183) The Root CAs shall issue ICA certificates in IEEE 1609.2.1 format.

(184) The Root CA shall check the audit results of the ICA before issuing a certificate for it.

(185) The Root CA shall take care that the ICA certificate is made available via RA repository or DC as soon as needed.

4.3.1.4 CRL Signer certificate issuance

(186) The CRACA may issue CRL Signer certificates in IEEE 1609.2.1 format.

(187) The CRACA shall check the audit results of the CRL Signer before issuing a certificate for it.

(188) The CRACA shall take care that relevant CRL Signer certificates are made available via RA and DC if the CRL Signer certificate is not included in the CRL itself.

4.3.1.5 ECA, RA, ACA, LA, MA, DC certificate issuance

(189) The ICA shall issue ECA, RA, ACA, LA, MA, DC certificates in IEEE 1609.2.1 format.

(190) The ICA shall check the audit results of the ECA, RA, ACA, LA, MA, before issues certificate for it.

(191) The ICA shall take care that relevant ECA, RA, ACA, LA, MA, DC certificates are made available via RA repository or DC.

4.3.1.6 Enrollment certificate issuance

(192) The Enrollment CA shall issue enrollment certificates in IEEE 1609.2.1 or X.509 format following RFC 5280 and RFC 5480.

(193) The Enrollment CA shall evaluate the enrollment certificate request to ensure that all fields are correct and valid. After successful validation, the Enrollment CA shall issue the certificate or otherwise reject the certificate request.

(194) Enrollment certificate requests and responses shall be encrypted to ensure confidentiality, and signed to ensure authentication and integrity.

4.3.1.7 Authorization certificate issuance

(195) The ACA shall issue authorization certificates in IEEE 1609.2.1 format.

(196) The ACA shall make available the authorization certificates to the EE via RA interface.

(197) Authorization certificate requests and responses shall be encrypted to ensure confidentiality, and signed to ensure authentication and integrity.

4.3.2 CA's notification to subscriber of issuance of certificates.

Not applicable.

4.4 Certificate acceptance

4.4.1 Conducting certificate acceptance

4.4.1.1 Elector

Not applicable.

4.4.1.2 Root CA

Not applicable.

4.4.1.3 ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC

(198) The Sub-CA or other SCMS model element shall verify the certificate type, the signature and the information in the received certificate. The Sub-CA or other SCMS model element shall discard all enrollment/authorization certificates that are not correctly verified and issue a new request.

4.4.1.4 End Entity

(199) The EE shall verify the received enrollment and authorization certificates

against its original request, including the signature and certificate chain. It shall discard all EC/AC responses that are not correctly verified. In such cases, it should send a new enrollment/authorization certificate request.

4.4.2 Publication of the certificate

(200) Elector and Root CA certificates shall be made available to all participants through CTLs via the SCMSMO's PUB.

(201) Sub-CAs' or other SCMS model element certificates shall be published by the issuing CA.

(202) Enrollment and authorization certificates shall not be published.

(203) ICA, ACA, and CRL Signer certificates may be published by the EE via P2PCD according to IEEE 1609.2.1.

4.4.3 Notification of certificate issuance

There are no notifications of issuance.

4.5 Key pair and certificate usage

4.5.1 Private key and certificate usage

4.5.1.1 Private key and certificate usage for Elector

(204) The Elector shall use its Elector private keys to sign its own (Elector) certificates and the CTL.

(205) The Elector certificate shall be used by PKI participants to verify the CTL.

4.5.1.2 Private key and certificate usage for Root CA

(206) The Root CA shall use its Root CA private keys to sign its own (Root CA) certificates, CRLs, and Sub-CAs.

(207) The Root CA certificate shall be used by PKI participants to verify the CRL and the Sub-CAs certificate.

4.5.1.3 Private key and certificate usage for ICA

(208) The ICA shall use its CA private keys to sign its own CSR and the certificates for ECA, RA, ACA, LA, MA, CRL Signer, DC, and CRLs.

(209) The ICA certificates shall be used by SCMS model elements and EEs to verify certificates and CRLs where the ICA is the issuer.

4.5.1.4 Private key and certificate usage for ECA

(210) The ECA shall use its CA private keys to sign its own CSR and enrollment certificates.

(211) According to IEEE 1609.2.1, the ECA can use an X.509 certificate for authentication in session-based communications.

(212) ECA certificates shall be used by SCMS model elements and end entities to verify enrollment certificates and SPDUs from the ECA.

4.5.1.5 Private key and certificate usage for RA

(213) The RA shall use its private keys to sign its own CSR and decrypt SPDUs. Also, this certificate may be used by the RA to authenticate itself in communication with other SCMS model elements and EEs.

(214) RA certificates shall be used by SCMS model elements and EEs to encrypt SPDUs for the RA.

4.5.1.6 Private key and certificate usage for ACA

(215) The ACA shall use its CA private keys to sign its own CSR, authorization certificates, CRL Signer certificates, CRLs.

(216) ACA certificates shall be used by SCMS model elements and end entities to verify authorization certificates, CRL Signer certificates, CRLs where the ACA is the issuer.

4.5.1.7 Private key and certificate usage for LA

(217) The Linkage Authority (LA) shall use its private keys to sign its own CSR.

(218) LA certificates may be used by SCMS model elements to authenticate the LA.

4.5.1.8 Private key and certificate usage for MA

(219) The Misbehavior Authority (MA) shall use its private keys to sign its own CSRs and decrypt misbehavior reports.

(220) MA certificates may also be used by SCMS model elements to authenticate the MA in communication.

4.5.1.9 Private key and certificate usage for CRACA and CRL Signer

(221) The CRACA and CRL Signer shall use its private keys to sign its own CSRs and CRLs.

(222) CRACA and CRL Signer certificates shall be used by SCMS model elements and EEs to verify the CRLs.

4.5.1.10 Private key and certificate usage for End Entity

(223) If direct authorization is used for initial EE enrollment, the EE shall use the canonical private key to sign initial enrollment certificate requests as defined in IEEE 1609.2.1.

(224) The EE shall use its private key(s) to sign successor enrollment certificate requests and authorization certificate requests.

(225) The private key corresponding to a new enrollment certificate shall be used to sign the request to prove possession of the private key corresponding to the new enrollment public key.

(226) The private key corresponding to a new authorization certificate shall be used to sign the request to prove possession of the private key corresponding to the new authorization public key.

(227) The EE shall use its authorization certificate's private key to sign messages defined in IEEE 1609.2 and IEEE 1609.2.1.

4.6 Relying party public key and certificate usage

(228) Parties relying on the public keys use the trusted certification path for the purposes referred to in the certificates and to authenticate the trusted common identity of enrollment/authorization certificates.

(229) Certificates in the SCMS model shall not be used without a preliminary check by a party replying on them.

4.7 Certificate renewal

Not allowed.

4.8 Certificate re-key

4.8.1 Circumstances for certificate re-key

(230) Certificate re-key shall be processed when a certificate reaches the end of its lifetime or a private key reaches the end of operational use, but the trust relationship with the CA still exists. A new key pair and the corresponding certificate shall be generated and issued in all cases.

4.8.2 Who may request re-key

4.8.2.1 Elector and Root CA

(231) The Elector and Root CA does not request a re-key. The re-keying process is an internal process for the Elector and Root CA because its certificate is self-signed.

4.8.2.2 ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC

(232) The CA issuing the Sub-CA or other SCMS element certificate shall specify in its CPS whether re-keying is supported or not.

(233) The re-keying request shall be submitted well before the current Sub-CA or other SCMS element certificate expires, allowing enough time for the new certificate and operational key pair to be approved and issued.

4.8.2.3 End Entity

(234) The EE shall re-key its enrollment certificate according to IEEE 1609.2.1.

4.8.3 Re-keying process

4.8.3.1 Elector and Root CA

Not applicable.

4.8.3.2 ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC

(235) The Sub-CA or other SCMS element may request a new certificate or a re-key certificate as follows:

The Sub-CA or other SCMS element shall generate a new key pair to replace the expiring key pair and sign the re-key request containing the new public key with the current valid private key ('re-keying'). The Sub-CA or other SCMS element shall generate a new key pair and sign the request with the new private key (inner signature) to prove possession of the new private key. The whole request shall be signed ('oversigned') with the current valid private key (outer signature) to ensure the integrity and authenticity of the request.

4.8.3.3 End Entity certificates

(236) The EE shall re-key its enrollment certificate according to IEEE 1609.2.1.

4.9 Certificate modification

Not allowed.

4.10 Certificate revocation and suspension

4.10.1 Circumstances for revocation

(237) Certificate revocation may be performed for the following circumstances:

(a) if the SCMSMO has reason to believe or strongly suspects that the corresponding Elector/Root CA private key has been compromised,

(b) if the issuing CA (Root CA or Sub-CA) has a reason to believe that the private key associated with that certificate has been compromised,

(c) if the audit (see Section 8) leads to a negative result,

(d) if the Sub-CA/End Entity is no longer associated with the EE subscriber or the organization managing the Sub-CA,

(e) if there is incorrect information included in the certificate which may cause it to be used or relied upon inappropriately,

(f) if the subscriber agreement has been terminated,

(g) if the subscriber has violated its license or certificate usage agreements,

(h) if ordered by a court or entity with contractual or legal jurisdiction.

(238) Enrollment certificates and authorization certificates shall be revoked for loss or suspected compromise of the EE, application or private key.

4.10.2 Who can request revocation

(239) SCMSMO can trigger the removal of an Elector or Root CA from the CTL.

(240) The Elector and Root CA is a self-signed certificate, so removal from the CTL can only be requested by these entities via the SCMSMO.

(241) The Sub-CA representative can request the revocation of its own Sub-CA certificates.

(242) The issuing CA can trigger the revocation of the certificates issued by itself.

(243) The EE subscriber representative can request the revocation of certificates requested by itself.

(244) EE subscriber and MA can request the revocation of EE certificates which they are responsible for.

(245) CAs shall accept revocation requests from all authorized and authenticated parties, such as an authorized representative of the United States Department of Transportation (USDOT).

(246) CAs may establish procedures that allow other entities to request certificate revocation for fraud or misuse. A CA Provider may revoke a certificate of its own volition to safeguard the trust in the SCMS Manager ecosystem even if no other entity has requested revocation, after a three-day notice to the Subscriber and the SCMSMO, unless a shorter time period is necessary due to critical/urgent circumstances.

(247) Demonstrated key compression can be reported by anyone.

4.10.3 Procedure for revocation request

4.10.3.1 Removal of an Elector

(248) An Elector shall be removable from the CTL. In the event of removal, the SCMSMO shall publish a new CTL as soon as possible and without undue delay.

(249) The Elector removal from the CTL is the responsibility of SCMSMO's CTL Committee, as defined in its internal processes.

(250) The Elector shall immediately notify the SCMSMO of a known or suspected compromise of its private key. It must be assured that only authenticated requests result in certificate removal.

4.10.3.2 Removal of a Root CA

(251) A Root CA shall be removable from CTL. In the event of removal, the SCMSMO shall publish a new CTL as soon as possible and without undue delay.

(252) The Root CA removal from the CTL is the responsibility of SCMSMO's CTL Committee, as defined in its internal processes.

(253) The Root CA shall immediately notify the SCMSMO of a known or suspected compromise of their private key. It must be assured that only authenticated requests result in certificate removal.

4.10.3.3 Revocation of ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC certificates

(254) An ICA, ECA, RA, ACA, LA, MA, CRL Signer, and DC certificate shall be revocable. The Root CA shall process the revocation request, under normal conditions, within 5 days. If the revocation cause is the compromise of the key, this revocation shall be done as soon as possible. Revoked certificates shall be published on a CRL within 24 hours.

(255) The CRACA or CRL Signer shall update, sign and publish the CRL within 24 hours to the DC.

(256) The Sub-CA and the other SCMS element shall immediately notify the issuing CA of a known or suspected compromise of its private key. It must be assured that only authenticated requests result in revoked certificates.

4.10.3.4 Revocation of enrollment certificates

(257) An enrollment certificate can be blocked. If the certificate is blocked by the ECA or RA or supplementary Authorization Server, it shall not be accepted for any usage.

(258) The ECA shall process the blocking/revocation request, under normal conditions, within 5 days. If the blocking/revocation cause is the compromise of the key, this revocation shall be done as soon as possible.

(259) If an EE is determined by an MA to be not working correctly, the ECA, RA or supplementary Authorization Server shall change its status to 'blocked' and it shall not be accepted for any usage.

4.10.3.5 Revocation of authorization certificates

(260) Revocation of the authorization certificates can be initiated by the CRACA using linkage Id-based revocation information or hash Id-based revocation information according to IEEE 1609.2.1 in the following cases:

(a) requested by an EE subscriber,

(b) terminated EE subscriber,

(c) requested by the MA,

(d) ordered by a court decision.

(261) The ACA shall process the revocation request, under normal conditions, within 5 days. If the revocation cause is the compromise of the key, this revocation shall be done as soon as possible.

(262) Activation Codes for Pseudonym Certificates (ACPC) can be used to lock authorization certificates. A locked certificate cannot be used until the (re) activation code is received by the EE.

4.10.4 Processing of misbehavior reports

(263) MA shall process misbehavior reports only if the following requirements are fulfilled:

(a) the signature of the reporting End Entity on the MBR is valid,

(b) valid and relevant Elector certificates are available,

(c) valid and relevant CRL and CTL are available,

(d) the Root CA certificate and the ICA certificate of the MA certificate chain are valid,

(e) on the basis of the MA's own root certificate list.

4.11 Certificate status services

4.11.1 Operational characteristics

Not applicable.

4.11.2 Service availability

Not applicable.

4.11.3 Optional features

Not applicable.

4.12 End of subscription

Not applicable.

4.13 Key escrow and recovery

Not applicable.

5 Facility, management and operational controls

(264) In this section, the entity responsible for an element of the PKI is identified by the element itself. In other words, the sentence 'the CA is responsible for executing the audit' is equivalent to 'the entity or personnel managing the CA is responsible for executing …'.

(265) The term 'SCMS model elements' includes the Elector, Root CA, ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC and the secure network.

5.1 Physical controls

(266) All SCMS model element operations shall be conducted in a physically protected environment that deters, prevents and detects unauthorized use of, access to or disclosure of sensitive information and systems. SCMS model elements shall use physical security controls in compliance with ISO 27001 or TISAX.

(267) The entities managing the trust model elements shall describe the physical, procedural and personnel security controls in their CPS.

(268) If entities managing the trust model elements do not use their own physical environment, they shall ensure and document that the outsourced environment fulfills the requirements.

5.1.1 Site location and construction

5.1.1.1 Elector and Root CA

(269) The location and construction of the facility housing the Elector, Root CA equipment and data (HSM, activation data, backup of key pair, computer, log, key ceremony script, certificate request, etc.) shall be consistent with facilities used to house highvalue and sensitive information. Root CA shall be operated in a dedicated physical area separated from other PKI components' physical areas.

(270) Elector and Root CA shall implement policies and procedures to ensure that a high level of security is maintained in the physical environment in which the Elector and Root CA equipment is installed, so as to guarantee that:

(a) it is isolated from public networks,

(b) the physical environment contains a series of (at least two) progressively more secure physical zones and the Elector and Root CA shall be in the most secure zone,

(c) sensitive data (HSM, key pair backup, activation data, etc.) are stored in a

dedicated safe set aside in a physical area protected by multiple access controls.

(271) The security techniques employed shall be designed to resist a large number and combination of different forms of attack. The mechanisms used shall include at least:

(a) perimeter alarms, closedcircuit television, reinforced walls and motion detectors,

(b) two-factor authentication (e.g. smartcard and PIN) for every person and badge to enter and leave the Root CA facilities and safe physical secured area.

(272) The Elector and Root CA shall use authorized personnel to monitor the facility housing core equipment. The personnel of the operational environment shall never have access to the secure areas of Root CAs or sub-CAs unless authorized.

5.1.1.2 Sub-CAs and other SCMS model elements

(273) The location and construction of the facility housing the Sub-CA (ICA, ECA, ACA) and other SCMS model elements (RA, LA, MA, CRL Signer, DC) equipment and data (HSM, activation data, backup of key pair, computer, log, key ceremony script, certificate request, etc.) shall be consistent with facilities used to house high-value and sensitive information. These can be in secure cloud environment based on risk analysis and with certified HSM.

(274) Sub-CAs and other SCMS model elements shall implement policies and procedures to ensure that a high level of security is maintained in the physical environment in which the Sub-CA and other SCMS model elements equipment are installed, to guarantee that sensitive data (key pair backup, activation data, etc.) are stored in a dedicated safe set aside in a physical area protected by multiple access controls.

(275) The security techniques employed shall be designed to resist a large number and combination of different forms of attack. The mechanisms used shall include at least:

(a) perimeter alarms, closed circuit television, reinforced walls and motion detectors,

(b) two-factor authentication (e.g. smartcard and PIN) for every person and badge to enter and leave the Root CA facilities and safe physical secured area.

(276) Sub-CAs and other SCMS model elements use authorized personnel to monitor the facility housing equipment. The personnel of the operational environment shall never have access to the secure areas of Root CAs or sub-CAs unless authorized.

5.1.2 Physical access

5.1.2.1 Elector, Root CA

(277) Equipment and data (HSM, activation data, backup of key pair, computer, log, key ceremony script, certificate request, etc.) shall always be protected from unauthorized access. The physical security mechanisms for equipment shall at least:

(a) monitor, either manually or electronically, for unauthorized intrusion at all times,

(b) ensure that no unauthorized access to the hardware and activation data is permitted,

(c) ensure that all removable media and paper containing sensitive plain-text information are stored in a secure container,

(d) ensure that any individual entering secure areas who is non-authorized on a permanent basis shall not be left without supervision by an authorized employee of the Elector and Root CA facilities,

(e) ensure that an access log is maintained and inspected periodically,

(f) provide at least two layers of progressively increasing security, e.g. at perimeter, building and operational room level,

(g) require two trustedrole physical access controls for the cryptographic HSM and activation data.

(278) A security check of the facility housing equipment shall be carried out if it is to be left unattended. At a minimum, the check shall verify that:

(a) the equipment is in a state that is appropriate for the current mode of operation,

(b) for off-line components, all equipment is shut down,

(c) any security containers (tamperproof envelope, safe, etc.) are properly secured,

(d) physical security systems (e.g. door locks, vent covers, electricity) are functioning properly;

(e) the area is secured against unauthorized access.

(279) Removable cryptographic modules shall be deactivated prior to storage. When not in use, such modules and the activation data used to access or enable them shall be placed in a safe. Activation data shall either be memorized or recorded and stored in a manner commensurate with the security afforded to the cryptographic module. They shall not be stored with the cryptographic module, so as to avoid only one person having access to the private key.

(280) A person or group of trusted roles shall be made explicitly responsible for making such checks. Where a group of people is responsible, a log shall be maintained that identifies the person performing each check. If

the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date/time and confirms that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC

(281) Sub-CAs and other SCMS model elements may be operated in a secure cloud environment based on risk analysis and with certified HSM.

5.1.3 Power and air conditioning

(282) Secure facilities of critical SCMS model elements (Root CA, Elector) shall be equipped with reliable access to electric power to ensure operation with no or minor failures. Primary and backup installations are required in the event of external power failure and smooth shutdown of the CITS trust model equipment in the event of a lack of power. These SCMS model element facilities shall be equipped with heating/ventilation/ airconditioning systems to maintain the temperature and relative humidity of the equipment within operational range.

5.1.4 Water exposures

(283) Secure facilities of critical SCMS model elements (Root CA, Elector) should be protected in a way that minimizes impact from water exposure. For this reason, water and soil pipes shall be avoided.

5.1.5 Fire prevention and protection

(284) To prevent damaging exposure to flame or smoke, the secure facilities critical SCMS model elements (Root CA, Elector) shall be constructed and equipped accordingly, and procedures shall be implemented to address firerelated threats. Media storage should be protected against fire in appropriate containers.

5.1.6 Media management

(285) SCMS model elements shall protect physical media holding backups of critical system data or any other sensitive information from environmental hazards and unauthorized use of, access to or disclosure of such media.

(286) Media used in the SCMS model elements are securely handled to protect them from damage, theft and unauthorized access. Media management procedures are implemented to protect against obsolescence and deterioration of media in the period for which records have to be retained.

(287) Sensitive data shall be protected against being accessed as a result of re-used storage objects (e.g. deleted files), which may make the sensitive data accessible to unauthorized users.

(288) An inventory of all information assets shall be maintained and requirements set out for the protection of those assets that are consistent with the risk analysis.

5.1.7 Waste disposal

(289) SCMS model elements shall implement procedures for the secure and irreversible disposal of waste (paper, media or any other waste) to prevent the unauthorized use of, access to or disclosure of waste containing confidential/private information. All media used for the storage of sensitive information, such as keys, activation data or files, shall be destroyed before being released for disposal.

5.1.8 Off-site backup

(290) Backups of SCMS model elements, sufficient to recover from system failure, are made offline after SCMS model elements deployment and after each new keypair generation. Backup copies of essential business information (key pair, CRL, CTL, certificate, configuration) and software are made regularly. Adequate backup facilities are provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Backup arrangements for individual systems are regularly tested to ensure that they meet the requirements of the business continuity plan. At least one full backup copy is stored at an offsite location (disaster recovery). The backup copy is stored at a site with physical and procedural controls commensurate to that of the operational PKI system.

(291) Backup data are subject to the same access requirements as the operational data. Backup data shall be stored offsite. In the event of complete loss of data, the information required for putting the SCMS model elements back into operation shall be completely recovered from the backup data.

(292) Private key material SCMS model elements shall not be backed up using standard backup mechanisms but using the backup function of the cryptographic module.

5.2 Procedural controls

This section describes requirements for roles, duties and identification of personnel.

5.2.1 Trusted roles

(293) Employees, contractors and consultants who are assigned to trusted roles shall be considered 'trusted persons'. Anyone seeking to become trusted persons for obtaining a trusted position shall meet the screening requirements of this certificate policy.

(294) Trusted persons have access to or control authentication/cryptographic operations that may materially affect:

(a) the validation of information in certificate applications,

(b) the acceptance, rejection or other processing of certificate applications, revocation requests or renewal requests,

(c) the issuance or revocation of certificates, including personnel having access to restricted portions of its repository or the handling of subscriber information or requests.

(295) Trusted roles shall include those that involve the following responsibilities:[20]

(a) Security Officers: Overall responsibility for administering the implementation of the security practices.

(b) System Administrators: Authorized to install, configure and maintain a SCMS model element's trustworthy systems for service management (including recovery of the system),

(c) System Operators: Responsible for operating the SCMS model element's trustworthy systems on a day-to-day basis, and authorized to perform system backup,

(d) System Auditors: Authorized to view archives and audit logs of the SCMS model element entity's trustworthy systems.

(296) The trust model elements shall provide clear descriptions of all trusted roles in its CPS.

5.2.2 Number of persons required per task

(297) SCMS model elements shall establish, maintain and enforce rigorous control procedures to ensure the separation of duties based on trusted roles and to ensure that multiple trusted persons are required to perform sensitive tasks.

(298) Policy and control procedures are in place to ensure separation of duties based on job responsibilities. The most sensitive tasks, such as access to and the management of CA cryptographic hardware (HSM) and its associated key material, must require the authorization of multiple trusted persons.

(299) These internal control procedures shall be designed to ensure that at least two trusted persons are required to have physical or logical access to the device. Restrictions on access to CA cryptographic hardware must be strictly enforced by multiple trusted persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction.

5.2.3 Identification and authentication for each role

(300) All persons assigned a role, as described in this document, are identified and authenticated so as to guarantee that the role enables them to perform their PKI duties.

(301) SCMS model elements shall verify and confirm the identity and

[20] Based on the ETSI EN 319401 REQ-7.2-15 requirement.

authorization of all personnel seeking to become trusted persons before they are:

(a) issued with their access devices and granted access to the required facilities,

(b) given electronic credentials to access and perform specific functions on CA systems.

(302) The CPS describes the mechanisms used to identify and authenticate individuals.

5.2.4 Roles requiring separation of duties

(303) Roles requiring separation of duties include (but are not limited to):

(a) the acceptance, rejection and revocation of requests, and other processing of CA certificate applications,

(b) the generation, issuing and destruction of a CA certificate.

(304) Segregation of duties may be enforced using PKI equipment, procedures, or both. No individual shall be assigned more than one identity unless approved by the Root CA.

(305) The part of the SCMS model elements concerned with certificate generation and revocation management shall be managed independently for its decisions relating to the establishing, provisioning, maintaining and suspending of services in line with the applicable certificate policies. In particular, each SCMS Provider shall have its own senior executives, senior staff and personnel in trusted roles.

(306) The SCMS Provider that serves mobile EEs shall separate logically and on the level of trusted roles the ACA from ECA and RA. These entities shall not exchange any data which breaks the pseudonymity. Other protocols may be used, provided that IEEE 1609.2.1 is implemented.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

(307) SCMS model elements employ a sufficient number of personnel with the expert knowledge, experience and qualifications necessary for the job functions and services offered. PKI personnel fulfil those requirements through formal training and credentials, actual experience, or a combination of the two. Trusted roles and responsibilities, as specified in the CPS, are documented in job descriptions and clearly identified. PKI personnel and sub-contractors have job descriptions defined to ensure separation of duties and privileges, and position sensitivity is determined on the basis of duties and access levels, background screening, and employee training and awareness.

5.3.2 Background check procedures

(308) SCMS model elements shall conduct background checks on personnel seeking to become trusted persons. Background checks shall be repeated for personnel holding trusted positions at least every five years.

(309) The factors revealed in a background check that may be considered reasons for rejecting candidates for trusted positions or for taking action against an existing trusted person include (but are not limited to) the following:

(a) misrepresentations made by the candidate or trusted person,

(b) highly unfavorable or unreliable professional references,

(c) certain criminal convictions,

(d) indications of a lack of financial responsibility.

(310) Reports containing such information shall be evaluated by human resources personnel, who shall take reasonable action in the light of the type, magnitude and frequency of the behavior uncovered by the background check. Such action may include measures up to and including cancelling offers of employment made to candidates for trusted positions or terminating the employment of existing trusted persons. The use of information revealed in a background check as a basis for such action shall be subject to applicable law.

(311) Background investigation of persons seeking to become a trusted person includes but is not limited to:

(a) confirmation of previous employment,

(b) a check of professional references covering their employment over a period of at least five years,

(c) a confirmation of the highest or most relevant educational degree obtained,

(d) a search of criminal records.

5.3.3 Training requirements

(312) SCMS model elements shall provide their personnel with the requisite training to fulfill their responsibilities relating to CA operations competently and satisfactorily.

(313) Training programs shall be reviewed periodically, and modules shall address matters that are relevant to functions performed by their personnel.

(314) Training programs shall address matters that are relevant to the particular environment of the trainee, including:

(a) security principles and mechanisms of the SCMS model elements,

(b) all duties the person is expected to perform, and internal and external reporting processes and sequences,

(c) PKI business processes and workflows,

(d) incident and compromise reporting and handling,

(e) disaster recovery and business continuity procedures,

(f) configuration and access management of the PKI system,

(g) sufficient IT knowledge.

5.3.4 Retraining frequency and requirements

(315) The persons assigned to trusted roles are required to refresh the knowledge they have gained from training on an ongoing basis. Training must be repeated whenever deemed necessary and at least every two years.

(316) SCMS model elements shall provide their staff with refresher training and updates to the extent and with the frequency required to ensure that they maintain the required level of proficiency to fulfill their job responsibilities competently and satisfactorily.

(317) Individuals in trusted roles shall be aware of changes in the PKI operations, as applicable. Any significant change to the operations shall be accompanied by a training (awareness) plan and the execution of that plan shall be documented.

5.3.5 Job rotation frequency and sequence

(318) No stipulation as long as the technical skills, experience and access rights are ensured. The administrators of the SCMS model elements shall ensure that changes in staff do not affect the security of the system.

5.3.6 Sanctions for unauthorized actions

(319) Each SCMS model element must develop a formal disciplinary process to ensure that unauthorized actions are appropriately sanctioned. In severe cases, the role assignments and corresponding privileges must be withdrawn.

5.3.7 Independent contractor requirements

(320) SCMS model elements may permit independent contractors or consultants to become trusted persons only to the extent necessary to accommodate clearly defined outsourcing relationships and on condition that the entity trusts the contractors or consultants to the same extent as employees, and that they fulfill the requirements applicable to employees.

(321) Otherwise, independent contractors and consultants shall have access to SCMS PKI secure facilities only if escorted and directly supervised by trusted persons.

5.3.8 Documentation supplied to personnel

(322) SCMS model elements shall provide their personnel with requisite

training and access to the documentation they need to fulfill their job responsibilities competently and satisfactorily.

5.4 Audit logging procedures

(323) This section sets out requirements as regards the types of events to be recorded and the management of audit logs.

5.4.1 Types of events to be recorded and reported by Electors and SCMS Providers

(324) The system auditor of the Elector/SCMS Provider shall regularly review their logs, events and procedures.

(325) SCMS model elements shall record the following types of audit event (if applicable):

(a) physical facility access – access by physical persons to the facilities shall be recorded; an event shall be created every time a record is created,

(b) trusted roles management – any change in the definition and level of access of the different roles shall be recorded, including modification of the attributes of the roles; an event shall be created every time a record is created,

(c) logical access – an event shall be generated when an entity (e.g. a program) has access to sensitive areas (i.e. networks and servers),

(d) backup management – an event shall be created every time a backup is completed, either successfully or unsuccessfully,

(e) log management – logs shall be stored. An event shall be created when the log size exceeds a specific size,

(f) data from the authentication process for subscribers and trust model elements – events shall be generated for every authentication request by subscribers and trust model elements,

(g) acceptance and rejection of certificate requests, including certificate creation and renewal – an event shall be generated periodically with a list of accepted and rejected certificate requests in the previous seven days,

(h) manufacturer registration – an event shall be created when a manufacturer is registered,

(i) end entity events – an event shall be created when an end entity is registered and every time when registration status is changed/updated,

(j) HSM management – an event shall be created when an HSM security breach is recorded,

(k) IT and network management, as they pertain to the PKI systems – an event shall be created when a PKI server is shut down or restarted,

(l) security management – covers successful and unsuccessful PKI system access attempts, PKI and security system actions performed, security profile changes, system crashes, hardware failures and other anomalies, firewall and router activities; and entries to and exits from the PKI facilities.

(326) Where possible, security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

(327) Each event related to certificate lifecycle is logged in such a way that it can be attributed to the person that performed it.

(328) All data shall be protected against non-authorized access.

(329) At a minimum, each audit record includes the following (recorded automatically or manually for each auditable event):

(a) trusted date and time the event occurred,

(b) result of the event – success or failure where appropriate,

(c) identity of the entity and/or operator that caused the event if applicable,

(d) identity of the entity for which the event is addressed.

5.4.2 Frequency of processing log

(330) Audit logs shall be reviewed in response to alerts based on irregularities and incidents within the Elector/SCMS Provider systems.

(331) Auditlog processing shall consist of a review of the audit logs and documenting the reason for all significant events in an auditlog summary. Auditlog reviews shall include a verification that the log has not been tampered with, an inspection of all log entries and an investigation of any alerts or irregularities in the logs. Action taken on the basis of auditlog reviews shall be documented.

(332) The audit log shall be archived at least weekly. An administrator shall archive it manually if the free disk space for audit log is below the expected amount of auditlog data produced that week.

(333) Electors shall report its activities quarterly to the SCMSMO.

5.4.3 Retention period for audit log

(334) Log records relating to certificate lifecycles are kept for at least five years after the corresponding certificate expires.

5.4.4 Protection of audit log

(335) The integrity and confidentiality of the audit log is guaranteed by a role-based access control mechanism. Internal audit logs shall be accessed only by personnel holding trusted roles with the proper authorization; certificate lifecycle-related audit logs may also be accessed by users with

the appropriate authorization via a web page with user login. Access shall only be granted with multifactor authentication. It must be technically ensured that users cannot access their own log files.

(336) Electronic audit log entries shall be signed with a secure method.

(337) Events are logged in such a way that they cannot be easily deleted or destroyed (except for transfer to longterm media) within the period for which the logs have to be held.

(338) Event logs are protected in such a way as to remain readable for the duration of their storage period.

5.4.5 Audit log backup procedures

(339) Audit logs and summaries are backed up via enterprise backup mechanisms, under the control of authorized trusted roles. Auditlog backups are protected with the same level of trust that applies to the original logs.

5.4.6 Audit collection system (internal or external)

(340) The equipment of the SCMS model elements shall activate the audit processes at system startup and deactivate them only at system shutdown. If audit processes are not available, the SCMS model element shall suspend its operation.

(341) At the end of each operating period and at the rekeying of certificates, the collective status of equipment should be reported to the operations manager and operation governing body of the respective PKI element.

5.4.7 Notification to event-causing subject

(342) Where an event is logged by the audit collection system, it guarantees that the event is linked to a trusted role, if applicable.

5.4.8 Vulnerability assessment

(343) The role in charge of conducting audits and roles in charge of realizing PKI system operation in the SCMS model elements shall explain all significant events in an auditlog summary. Such reviews involve verifying that the log has not been tampered with and that there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Action taken as a result of these reviews is documented.

(344) Assessment of trust model elements shall include:

(a) implement organizational and/or technical detection and prevention controls under the control of the SCMS model elements to protect PKI systems against viruses and malicious software,

(b) document and follow a vulnerability correction process that addresses the identification, review, response and remediation of vulnerabilities,

(c) undergo or perform a vulnerability scan:

(1) after any system or network changes determined by the SCMS model elements as significant for PKI components,

(2) at least quarterly, on public and private IP addresses.

(d) undergo a penetration test on the PKI's systems on at least an annual basis and after infrastructure or application upgrades or modifications determined by the SCMS model elements,

(e) for online systems, record evidence that each vulnerability scan and penetration test was performed by a person or entity (or collective group thereof) with the skills, tools, proficiency, code of ethics and independence necessary to provide a reliable vulnerability or penetration test,

(f) track and remediate vulnerabilities in line with enterprise cybersecurity policies and risk mitigation methodology.

5.5 Record archiving

5.5.1 Types of record archiving

(345) SCMS model elements shall archive records detailed enough to establish the validity of a signature and of the proper operation of the PKI. At a minimum, the following PKI events records shall be archived (if applicable):

(a) physical facility access log of SCMS model elements,

(b) trusted roles management log for SCMS model elements,

(c) IT access log for SCMS model elements,

(d) SCMS model elements key creation, use and destruction log,

(e) SCMS model elements certificate creation, use and destruction log,

(f) activation data management log for SCMS model elements,

(g) IT and network log for SCMS model elements,

(h) PKI documentation for SCMS model elements,

(i) security incident and audit report for SCMS model elements,

(j) system configuration.

(346) The SCMS model elements shall retain the following documentation relating to certificate requests and the verification thereof, and all SCMS model elements certificates, CTL and revocation thereof:

(a) PKI audit documentation kept by SCMS model elements,

(b) CPS documents kept by SCMS model elements,

(c) contract between SCMSMO and other entities kept by SCMS model

elements,

(d) certificates (or other revocation information) kept by the CA,

(e) certificate request records in Root CA/Sub-CA system,

(f) other data or applications sufficient to verify archive contents,

(g) all work related to or from the SCMS model elements and compliance auditors.

(347) The SCMS model element entity shall retain all documentation relating to certificate requests and the verification thereof, and all certificates and revocation thereof, for at least seven years after any certificate based on that documentation ceases to be valid.

5.5.2 Retention period for archive

(348) Without prejudice to regulations requiring a longer archival period, SCMS model elements shall keep all records for at least five years after the corresponding certificate has expired.

5.5.3 Protection of archive

(349) SCMS model elements shall store the archive of records in a safe/secure storage facility separate from the SCMS model element's equipment, with physical and procedural security controls equivalent to or better than those of the PKI.

(350) The archive shall be stored in a trustworthy environment, protected against unauthorized viewing, modification, deletion or other tampering.

(351) The media holding the archive data and the applications required to process them shall be maintained to ensure that they can be accessed for the period set in this document.

5.5.4 System archive and storage

(352) SCMS model elements shall incrementally back up system archives of such information on at least daily basis and perform full backups on at least weekly basis. Copies of paper-based records shall be maintained in a secure offsite facility.

5.5.5 Requirements for time-stamping of records

(353) SCMS model elements managing a revocation database shall ensure that the records contain information as to the time and date when revocation records are created.

(354) SCMS model elements shall be synchronized to an UTC time source.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

(355) All SCMS model elements shall allow only authorized/trusted persons to access the archive.

(356) SCMS model elements shall verify the integrity of the information before it is restored.

5.6 Key changeover for trust model elements

(357) SCMS model elements shall delete their private key (including backup keys) on expiry of the corresponding certificate. The Elector and Root CA shall generate a new key pair and issue a new self-signed certificate before expiration of the current valid certificate.

(358) Sub-CA or other SCMS model elements shall generate new key pairs and request a new certificate before expiration of their current valid certificate. The validity period of the new Sub-CA or other SCMS model element certificates shall start prior to the planned deletion of the current private keys. The Sub-CA or other SCMS model elements shall take care that the new certificate is distributed to relevant subscribers and parties relying on it before the start of its validity period. The SCMS model element shall activate the new private key when the corresponding certificate becomes valid.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling

(359) SCMS model elements shall monitor their equipment on an ongoing basis, so as to detect potential hacking attempts or other forms of compromise. If compromise is detected the trust model element shall perform an investigation to determine the nature and the degree of damage.

(360) If the personnel responsible for the management of the Root CA or Elector detect a potential hacking attempt or other form of compromise, they shall investigate in order to determine the nature and the degree of damage. In the event of the private key being compromised, the affected Root CA or Elector certificate shall be removed from the CTL. The IT security experts of the SCMSMO shall assess the scope of potential damage in order to determine whether the PKI needs to be rebuilt, whether only some certificates must be revoked and/or whether the whole PKI has been compromised. In addition, the SCMSMO determines which services are to be maintained (revocation) and how.

(361) Incident, compromise and business continuity shall be covered in the CPS.

(362) If the personnel responsible for the management of a Sub-CA or SCMS model elements detect a potential hacking attempt or other form of compromise, they shall investigate in order to determine the nature and degree of damage. The personnel responsible for the management of the CA entity shall assess the scope of potential damage to determine whether the PKI component needs to be rebuilt, whether only some certificates must be revoked and/or whether the PKI component has been compromised. In addition, the sub-CA or SCMS model elements entity determines which services are to be maintained and how, in accordance with the Sub-CA entity business continuity plan. In the event of a PKI component being compromised, the Sub-CA or SCMS model elements entity shall alert its own superior CA (Root CA or ICA) and the SCMSMO.

5.7.2 Corruption of computing resources, software and/or data

(363) If a disaster is discovered that prevents the proper operation of an SCMS model element, its operation shall be self-suspended until it can be determined whether a private key has been compromised.

(364) The corruption of computing resources, software and/or data shall be reported to the superior CA (Root CA or ICA) within 24 hours for the highest levels of risk. All other events shall be included in the periodic SCMS model element audit results.

5.7.3 Entity private key compromise procedures

(365) If the private key (or its backup) of an Elector or a Root CA is compromised, lost, destroyed or suspected of being compromised, the Elector/Root CA shall:

(a) suspend its operation,

(b) start the disaster recovery and migration plan,

(c) investigate the 'key issue' that generated the compromise and notify the SCMSMO, which will remove it from the CTL,

(d) alert all subscribers with which it has an agreement.

(366) If Sub-CA's or other SCMS model element's private key (or its backup) is compromised, lost, destroyed or suspected of being compromised, the Sub-CA or other SCMS model element shall:

(a) suspend its operation,

(b) investigate the issue and notify the superior CA (Root CA or ICA), which will revoke the certificate with the responsible CRACA or CRL Signer,

(c) alert subscribers with which it has an agreement.

(367) If an enrollment certificate private key or authorization certificate private key is compromised, lost, destroyed or suspected of being compromised, the RA and ECA to which the End Entity is subscribed shall revoke the enrollment certificate of the affected EE.

(368) Where any of the algorithms or associated parameters used by the Elector, Root CA, Sub-CA or other SCMS model element or EE become insufficient for its remaining intended usage, the SCMSMO (with a recommendation from cryptographic experts) shall inform the Elector, Root CA, Sub-CA or other SCMS model element entity about which algorithms shall to be discontinued.

5.7.4 Business continuity capabilities after a disaster

(369) The SCMS model elements operating secure facilities for CA operations shall develop, test, maintain and implement a disaster recovery plan designed to mitigate the effects of any natural or man-made disaster. Such plans address the restoration of information systems services and key business functions.

(370) After an incident above a certain risk level, the compromised CA must be reaudited by an accredited PKI auditor (see Section 8).

(371) The SCMSMO shall have an action plan for the case when a compromised Root CA, Sub-CA or SCMS model element is no longer able to operate/ function (e.g. following a severe incident).

5.8 Termination and transfer

5.8.1 Elector

(372) The Elector may terminate its operation.

(373) When an Elector is planning to terminate its operation, it shall notify the SCMSMO 90 days before the planned termination date.

(374) In the event of a termination, the Elector shall:

(a) request the SCMSMO to remove the Elector certificate from the CTL,

(b) destroy the Elector private key including key backups,

(c) archive all audit logs and other records prior to termination of the Elector,

(d) transfer archived records to the SCMSMO.

(375) The SCMSMO shall remove the corresponding Elector certificate from the CTL.

(376) The SCMSMO shall invite a new Elector into the ecosystem.

5.8.2 Root CA

(377) The Root CA shall not terminate/start its operation without establishing a migration plan (set out in the relevant CPS) that guarantees ongoing operation for all subscribers.

(378) In the event of a termination of service, the Root CA shall:

(a) notify the superior CA about the plan 90 days before the termination date and request the revocation of its certificate at the end of service,

(b) request the SCMSMO to remove the Root CA certificate from the CTL,

(c) alert Root CAs with which it has an agreement for the re-keying of ICA certificates and CRL Signer certificates (for transfer of services to another SCMS Provider),

(d) destroy the Root CA private key including key backups,

(e) communicate the changed status information (CRL signed by Root CA) to parties relying on the keys, indicating clearly that it is the 'latest revocation' information,

(f) archive all audit logs and other records prior to termination of the Root CA service,

(g) transfer archived records to the SCMSMO.

(379) The SCMSMO shall remove the corresponding Root CA certificate from the CTL.

5.8.3 ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC

(380) In the event of termination, the Sub-CA or other SCMS model elements shall provide notice at least to the superior CA and the related EEs 90 days prior to the termination. A Sub-CA or other SCMS model elements shall not terminate operation without establishing a migration plan that guarantees ongoing operation for all subscribers.

(381) In the event of termination, the Sub-CA or other SCMS model elements shall:

(a) notify the superior CA about the plan 90 days before the termination date and request the revocation of its certificate at the end of service,

(b) destroy the Sub-CA or other SCMS model elements private key including key backups,

(c) archive all audit logs and other records prior to termination of Sub-CA or other SCMS model elements,

(d) transfer archived records to the superior CA.

(382) The superior CA shall revoke the corresponding Sub-CA or other SCMS model elements certificate.

6 Technical security controls

6.1 Key pair generation and installation

(383) The SCMS model elements and End Entities shall be able to generate their own key pairs in accordance with Section 6.1.1.

(384) The process of deriving symmetric encryption keys and message authentication code (MAC) keys shall be carried out in line with IEEE 1609.2.

(385) The key pair generation process shall be subject to the requirements of Section 6.1.2.

(386) The Root CAs and their subscribers (Sub-CAs and End Entities) shall ensure that the integrity and authenticity of their public keys and any associated parameters are maintained during request generation, request distribution, request processing, and response distribution.

(387) The RA, ACA and EEs shall also support the butterfly key mechanism specified in the IEEE 1609.2.1. and may support the non-butterfly key mechanism.

(388) The End Entities shall perform the butterfly private key derivation inside their cryptographic module.

6.1.1 Cryptographic requirements

(389) The following table shows the mandatory algorithm implementations for certificate type and for usages:

(Specified by NIST FIPS 186-4 and RFC 5639, defined in IEEE 1609.2 and IEEE 1609.2.1)

	ecdsaBrainpool P256r1 WithSha256	**ecdsaBrainpool P384r1 WithSha384**	**ecdsaNist P256 WithSha256**	**ecdsaNist P384 WithSha384**
Elector	not allowed	signing/verification	not allowed	signing/verification
Root CA	signing/verification	signing/verification	signing/verification	signing/verification
ICA	signing/verification	signing/verification	signing/verification	signing/verification
ECA	signing/verification	signing/verification	signing/verification	signing/verification
ACA	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption
CRL Signer	signing/verification	signing/verification	signing/verification	signing/verification
RA	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption
LA	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption

	ecdsaBrainpool P256r1 WithSha256	ecdsaBrainpool P384r1 WithSha384	ecdsaNist P256 WithSha256	ecdsaNist P384 WithSha384
MA	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption
DC	signing/verification	signing/verification	signing/verification	signing/verification
EC	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption
AC	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption	signing/verification encryption/decryption

6.1.1.1 Crypto-agility

(390) Requirements on key lengths and algorithms must be changed over time to maintain an appropriate level of security. The SCMSMO shall monitor the need for such changes in the light of actual vulnerabilities and state-of-the-art cryptography. It will draft, approve and publish an update of this certificate policy if it decides that the cryptographic algorithms should be updated. Where a new issue of this CP signals a change of algorithm and/or key length, the SCMSMO will adopt a migration strategy, which includes transition periods during which old algorithms and key lengths must be supported.

(391) In order to enable and facilitate the transfer to new algorithms and/or key lengths, it is recommended that all PKI participants implement hardware and/or software that is capable of a changeover of key lengths and algorithms, and implement an update mechanism to adopt to new vulnerabilities or threats.

6.1.2 Secure storing of private keys

(392) SCMS model elements and End Entities shall use validated hardware security modules from the following list:

(a) NIST validated to FIPS 140-2 Level 3 physical cryptographic module,

(b) Common Criteria EAL4 (or higher) certified for the following profiles by an accredited auditor (accredited by Common Criteria or EA MLA member):

(1) CEN EN 419 221-2: Protection profiles for TSP cryptographic modules – Part 2: Cryptographic module for CSP signing operations with backup,

(2) CEN EN 419 221-4: Protection profiles for TSP cryptographic modules – Part 4: Cryptographic module for CSP signing operations without backup,

(3) CEN EN 419 221-5: Protection profiles for TSP cryptographic modules – Part 5: Cryptographic module for trust services,

(4) CEN EN 419 211-2: Protection profiles for secure signature creation device – Part 2: Device with key generation,

(5) CEN EN 419 211-3: Protection profiles for secure signature creation device — Part 3: Device with key import,

(6) Hardware Protected Security for Ground Vehicles J3101_202002.

(393) The validated cryptographic module shall be used for:

(a) generating, using, administering and storing private keys,

(b) generating and using random numbers (assessment of the random number generation function shall be part of the security evaluation and certification),

(c) creating backups of private keys,

(d) deletion of private keys.

(394) The implementation of a cryptographic module shall ensure that keys are not accessible outside the cryptographic module. The cryptographic module shall include an access control mechanism to prevent unauthorized use of private keys.

(395) Manual access to the stored keys cryptographic module of a SCMS model element shall require two-factor authentication from two trusted persons.

(396) At least two authorized persons are required to sign the CTL at Elector.

(397) At least two authorized persons are required to sign the CRL with the Root CA.

(398) The Sub-CAs can perform automatic signature, after a manual key activation.

(399) The cryptographic module of a SCMS model element or an EE shall be protected against unauthorized removal, replacement and modification.

(400) A cryptographic module for EEs shall be used for:

(a) generating, using, administering and storing private keys,

(b) generating and using random numbers (assessment of the random number generation function shall be part of the security evaluation and certification),

(c) secure deletion of a private key.

6.1.3 Backup of private keys

(401) The generation, storage and use of private key backups shall fulfill the requirements of at least the security level required for the original keys.

(402) SCMS model elements shall back up their private keys.

(403) Backups of private keys shall not be made for ECs and ACs.

6.1.4 Destruction of private keys

(404) SCMS model elements and End Entities shall destroy their private key and any corresponding backups, if a new key pair and corresponding certificate has been generated and successfully installed, and the overlap time (if any – CA only) has passed. The private key shall be destroyed using the mechanism offered by the cryptographic module used for the key storage or as described in the corresponding supporting documents.

(405) A private key should only be deleted after the expiration or revocation of its certificate.

6.2 Activation data

(406) Activation data refer to authentication factors required to operate cryptographic modules to prevent unauthorized access. The usage of the activation data of a SCMS model element cryptographic device shall require action by two authorized persons.

6.3 Computer security controls

(407) The Electors and CAs' computer security controls shall be designed in accordance with 'high security' level by adhering to the requirements of ISO/IEC 27002 or the policies set by WebTrust for CA or SOC2 Trust Services.

6.4 Lifecycle technical controls

(408) The Electors' and CAs' technical controls shall cover the whole lifecycle of the CA. In particular, this includes the requirements of Section 6.1.1.1 on crypto-agility.

6.5 Network security controls

(409) The Elector and Root CA shall operate in isolation from public networks.

(410) The networks of the CAs (Root CA, ICA, ECA and ACA) shall be hardened against attacks in line with the requirements and implementation guidance of ISO/IEC 27001 and ISO/IEC 27002 or TISAX.

(411) The availability of the CAs' networks shall be designed in the light of the estimated traffic.

7 Certificate profiles, CRL, CTL

7.1 Certificate profile

(412) The Root CA, ICA, ECA and ACA certificates shall indicate the permissions for which these CAs are allowed to issue certificates.

(413) The IEEE 1609.2 certificates shall indicate the permissions for the types of usage.

(414) For X.509 certificates the following requirements are mandatory:

(a) The X.509 certificate shall follow the RFC 5280 defined PKIX profile.

(b) In the case of ECDSA keys, the key shall be RFC 5480 encoded.

(415) The certificate profiles allowed for SCMS elements (defined in IEEE 1609.2.1) are summarized in the following table:

SCMS element (certificate profile)	**X.509 or IEEE 1609.2.1**	**IEEE 1609.2.1 type (explicit and/or implicit)**
Elector	IEEE 1609.2.1	explicit
Root CA	IEEE 1609.2.1	explicit
ICA	IEEE 1609.2.1	explicit
ECA	X.509 or IEEE 1609.2.1	explicit
ACA	IEEE 1609.2.1	explicit
CRL Signer	IEEE 1609.2.1	explicit
RA	X.509 or IEEE 1609.2.1	explicit
LA	X.509 or IEEE 1609.2.1	explicit
MA	X.509 or IEEE 1609.2.1	explicit
DC	X.509 or IEEE 1609.2.1	explicit
EC	X.509 or IEEE 1609.2.1	implicit or explicit
AC	IEEE 1609.2.1	implicit

7.2 Certificate validity

7.2.1 SCMS model elements

(416) All certificates shall include an issue and an expiry date, which represent the validity time of the certificate. At each PKI level, certificates shall be replaced in good time before expiry.

(417) The SCMS model element certificates should have the following time parameters:

Certificate profile	Pre-availability maximum time	Maximum validity	Comment
Elector	12 months before validity	15 years	self-signed
Root CA	12 months before validity	30 years	self-signed
ICA	no requirement	until the validity of Root CA	shall not exceed the validity of issuer CA
ECA	no requirement	until the validity of ICA	shall not exceed the validity of issuer CA
ACA	no requirement	until the validity of ICA	shall not exceed the validity of issuer CA
CRL Signer	no requirement	until the validity of ICA	shall not exceed the validity of issuer CA
RA	no requirement	until the validity of ICA	shall not exceed the validity of issuer CA
LA	no requirement	until the validity of ICA	shall not exceed the validity of issuer CA
MA	no requirement	until the validity of ICA	shall not exceed the validity of issuer CA
DC	no requirement	until the validity of ICA	shall not exceed the validity of issuer CA

(418) When a SCMS Provider certificate is going to expire, the SCMS Provider shall prepare its successor certificate. At the beginning of the overlap time, the successive CA certificates shall be issued (if applicable), distributed to and installed by the correspondent parties relying on them. During the overlap time, the old certificate shall be used only for verification of End Entities.

(419) The End Entity certificates should have the following time parameters:

Certificate	Max. preloading time	Max. validity	Min. no. of parallel ACs/ PSID-SSP	Max. no. of parallel ACs/ PSID-SSP	Comment
pseudonym AC (OBE)	3 years (-validity)*	1 w + 1 h overlap time	10	100	* when IEEE 1609.2.1 ACPC not used
AC (RSE)	3 years (-validity)*	1 w + 1 h overlap time	1	2	* when IEEE 1609.2.1 ACPC not used
EC	3 months	3 years	1	1	

7.2.1.1 Time-period parameters

(420) The time-period base parameters are the following:

Parameter	Value	Comment
iPeriodLength	1 week	-
iPeriodEpoch	4 am Eastern Time on Tuesday, 6 January 2015	The value defined in Section 4.3.2.2 of IEEE1609.2.1 was accepted as the base value.
iPeriodInit	0	-

7.3 Certificate revocation list

(421) The format and content of the CRL issued by a CA or CRL Signer shall be as laid down in IEEE 1609.2.1.

(422) The CRL shall be issued at least monthly with 4 days overlap.

7.4 Certificate trust list

(423) The format and content of the CTL issued by the SCMSMO (and signed by Electors) shall be as laid down in in IEEE 1609.2.1.

(424) The CTL is valid until a new CTL was issued or one of the Electors certificates used to sign the CTL is expired.

8 Compliance audit and other assessments

8.1 Topics covered by auditor and audit basis

8.1.1 SCMS Providers and Electors

(425) A compliance audit is ordered by a SCMS Provider for itself and for its own subordinate CAs. The audit submitted as part of the Root CA inclusion process is reviewed by the SCMSMO and used as a basis for deciding on the application for inclusion.

(426) An accredited PKI auditor shall perform a compliance audit on one of the following levels:

(a) conformity of the CPSs of the Electors and SCMS Providers with this CP,

(b) conformity of the intended practices of the Electors and SCMS Providers with their CPSs prior to operation,

(c) conformity of the practices and operational activities of the Electors and SCMS Providers with their CPSs during operation.

(427) The audit shall cover all requirements of this CP to be fulfilled by the Elector and SCMS Provider to be audited. The scope of the audit shall cover all processes mentioned in its CPSs, the premises and responsible persons.

(428) The accredited PKI auditor shall provide the results of the audit to the issuing CA or to the SCMSMO's CTL Committee, as applicable.

8.1.2 End Entity devices

(429) The device audit shall be based on one of the following:

Validated against the SCMS Manager 'End-Entity Security Requirements, Design Guidance, and Validation Approach':

(a) OmniAir Consortium certification,

(b) for RSUs: ITE RSU Standard 1.0.

(430) Until the SCMSMO Policy Committee agrees on a more specific requirement, the device HSM audit shall be based on the HSM module validations defined in Section 6.1.2 (requirement (392)).

8.1.3 End entity device operator

(431) A compliance audit shall be ordered by an End Entity device operator for itself.

(432) The audit shall examine the conformance of device operators against:

(a) the present document (CP),

(b) ISO/IEC 27001 or TISAX,

(c) used TLS settings for the latest recommendations (e.g. the use of TLS 1.3).

8.2 Frequency of the audits

8.2.1 SCSMS Providers and Electors

(433) Electors and SCMS Providers shall order a compliance audit for themselves in the following cases:

(a) at their first setting-up (point-in-time audit),

(b) at every material change of the CP, if the SCMSMO requires it,

(c) regularly at least every 3 years during their operation.

8.2.2 End Entity devices

(434) End Entity devices shall be certified and have certified HSM for cryptographic functions. New devices shall only be installed if they have a valid certification.

(435) The devices and HSMs are usable for 15 years from the start date of their certification.

(436) If a device or HSM was recertified, the recertification date starts a new period for (434) and (435)

8.2.3 End Entity device operator

(437) End Entity device operators shall order a compliance audit for themselves in the following cases:

(a) before entering a contractual agreement with a SCMS Provider,

(b) regularly at least every 3 years during their operation.

8.3 Identity/qualifications of auditor

8.3.1 SCMS Providers and Electors

(438) The Electors, SCMS Providers shall select an accredited PKI auditor to audit themselves in accordance with this CP.

(439) The auditing body shall be accredited and certified for one or more of the following:

(a) WebTrust for CA V2.1

(b) ETSI EN 319411 or ETSI EN 319403 or ETSI TS 119403 (accredited by a

member of EAB),[21]

(c) SOC2 Trust Services.

8.3.2 End Entity devices

(440) The manufactures of the devices shall select an accredited auditor to audit their products in accordance with this CP.

(441) The device auditing body shall be accredited and certified for one or more of the following:

(a) ISO/IEC 15408,

(b) ISO/IEC 19790,

(c) Common Criteria,

(d) OmniAir schemes.

(442) The HSMs shall be certified by accredited auditors in accordance with this CP.

(443) The HSM auditing body shall be accredited and certified for 'Common Criteria'.

8.3.3 End Entity device operator

(444) The End Entity device operator shall select an accredited auditor to audit their organization and ensure they are in accordance with this CP and ISO/IEC 27001 or TISAX.

(445) The auditing body shall be accredited and certified for ISO/IEC 27001 or TISAX.

8.4 Auditor's relationship to audited entity

(446) The accredited PKI auditor shall be independent from the audited entity.

8.5 Action taken as a result of deficiency

8.5.1 SCMS Providers and Electors

(447) If an Elector or a SCMS Provider makes an application with non-compliant audit results, the SCMSMO shall reject the application.

(448) If an Elector receives a non-compliant audit result, the SCMSMO shall order the Elector to take immediate preventive/corrective action, and prepare for the replacement of that Elector.

[21] Members of the European Accreditation Body are listed at: http://www.european-accreditation.org/ea-members

(449) If a Root CA receives a non-compliant audit result, the SCMSMO shall order the Root CA to take immediate preventive/corrective action. In such cases, the Root CA may be suspended or revoked, based on the decision of the CTL Committee. The Root CA shall not be allowed to issue certificates during the suspension period.

(450) In the event of suspension, the Root CA must take corrective action, re-order a full audit and make a new request for SCMSMO for approval.

(451) In the event of a Sub-CA (ICA, ECA, ACA) audit, the SCMS Provider of the issuing CA shall decide whether or not to accept the report. Depending on the audit results, the SCMS Provider of the issuing CA shall decide whether to revoke the Sub-CA's certificate in accordance with rules in the issuing CA's CPS. The Root CA shall at all times ensure the Sub-CA's (ICA, ECA, ACA) compliance with this CP.

8.5.2 End Entity devices

(452) The End Entity subscriber shall regularly monitor the certification status of the HSMs and devices, and shall take action if one of the certifications has been revoked.

(453) If a device or HSM certification is revoked, the following steps need to be executed:

(a) EE subscriber shall identify the affected devices and contact the issuing CA in preparation for revoking them,

(b) The issuing CA shall revoke the affected certificates.

8.5.3 End Entity device operator

(454) The End Entity device operator shall report to the SCMS Provider if the certification status of the operator has expired and was not renewed (or was revoked).

(455) If a device operator's certification has expired and has not been renewed or has been revoked the SCMS Provider shall not issue new certificates to that EE device operator nor allow registration of new devices.

8.6 Communication of results

8.6.1 SCMS Providers and Electors

(456) The Elector and the SCMS Provider of the Root CA shall send the audit results to the SCMSMO. The Elector and the SCMS Provider of the Root CA shall store all audit results. The SCMSMO's CTL Committee shall send a corresponding approval/acceptance or rejection notice to the Elector or SCMS Provider of the Root CA. If approved, the CTL Committee prepares a new CTL and sends it to the Electors for signing.

(457) The SCMS Provider of the Root CA shall share its certificate of conformity

with the corresponding Sub-CA/SCMS model participants (ICA, ECA, ACA, RA, LA, MA, CRL Signer, DC).

8.6.2 End Entity devices

(458) The device operators should publish their certifications on a publicly available URL.

(459) The EE subscribers shall present the certification results of their devices to the SCMS Provider before enrolling a new kind of device.

8.6.3 End Entity device operator

(460) The device operators should publish their certification audit results on a publicly available URL.

(461) The device operators shall present their audit results to the SCMS Provider.

9 Other provisions

9.1 Fees

(462) The members of the SCMSMO together fully finance the regular recurrent costs of operation of the SCMSMO and the central elements (PUB) relating to the activities set out in this CP.

(463) The SCMS Providers are entitled to take fees from their Sub-CAs.

9.2 Financial responsibility

(464) Each SCMS Provider must demonstrate the financial viability of the legal entity implementing it for at least 3 years to the accredited PKI auditor. The fulfilment of this requirement shall be part of the audit results.

9.3 Confidentiality of business information

(465) The following shall be kept confidential and private:

(a) Root CA, ICA, ACA, ECA, RA, MA, LA, DC, CrlSigner application records – whether approved or rejected,

(b) audit results of the SCMS model participants,

(c) disaster recovery plans of the SCMS model participants,

(d) private keys of the SCMS model participants,

(e) any other information identified as confidential by the SCMS model participants.

9.4 Privacy of personal information

(466) The CPSs of the SCMS Providers shall set out the plan and any requirements for the treatment of personal information and privacy based on the applicable legislative (e.g. national) frameworks.

10 Appendix

10.1 Root CA/Elector inclusion process

This section describes the inclusion process of a Root CA/Elector certificate into CTL.

10.1.1 Who can apply?

An official representative of Root CA/Elector shall make the formal request for the inclusion or update of their Root CA/Elector certificates.

10.1.2 Process overview

This process is used if an applicant requests to include a new Root CA/Elector certificate, even if the Root CA/Elector already has relevant certificate(s) included in the CTL.

Approval of one Root CA/Elector certificate does not imply that other certificates owned by the same SCMS Provider/Elector would be accepted.

The steps of the Root CA/Elector certificate inclusion and update process are the following:

1. The representative of Root CA/Elector submits an inclusion request to the tracking system of SCMSMO.
2. The representative of Root CA/Elector provides the audit results and CPS through the tracking system of SCMSMO. The results and CPS shall be publicly available.
3. After all information is available, a member of the CTL Committee confirms all information provided by the applicant (time limit: 4 weeks).
4. Then public discussion starts (time limit: 4 weeks) on the mailing list of SCMSMO.

   During the public discussion phase, any member of SCMSMO may perform a detailed review of the applicant's CPS and audit results. During this phase, the applicant may be required to update its CPS and audit results to become fully aligned with SCMSMO Certificate Policy. In this case, a member of CTL Committee confirms the completion of the action items and continues public discussion if needed.
5. At the end of the public discussion period, a member of the CTL Committee provides a summary within 5 business days (if there are no objections or open questions that did not receive a response from the applicant) and states the public discussion period has concluded.

   If there are outstanding issues that need to be addressed (e.g. a need for further information, or concerns about the applicants' practices) then the request may be closed, moved back to Step 3 or put on hold pending future discussions.

   If there is no unanimous decision by the CTL Committee, the matter is put

to a vote among members and a majority decision is adopted.

6. Following public discussion, a member of the CTL Committee will post on the SCMSMO list its intent to either approve or reject the inclusion request, which is also signals a last call for objection.
7. After one week, if no further questions or concerns are raised, then the CTL Committee approves the request, prepares the new CTL update and sends a copy to the Electors for signing.

10.2 Policy modification

10.2.1 Submission of the change request

The Policy change process is initialized by a member of SCMSMO. Every member can submit a change request. The request form shall contain:

(a) a description of the change,

(b) a rationale for the change,

(c) the exact proposal including the line/paragraphs to be changed, the old text and the new text,

(d) the requester's contact information.

The change requester should be prepared to answer queries and/or defend the change proposal at the Policy Committee.

10.2.2 Processing the change

Within 1 (one) working day after receiving the change request, the Policy Committee shall confirm reception of the change request. Within 2 weeks after receiving a change request, the Policy Committee shall start processing the change. Processing a change request means:

(a) assessing the applicability of the change request,

(b) assessing the completeness of the change request,

(c) assessing the criticality of the change request,

(d) assessing the impact of the change.

The change processing phase is concluded with the scheduling of the request for decision in the next change approval meeting of the Policy Committee.

10.2.3 Change approval

The Policy Committee conducts change approval meetings to discuss and finally decide if a change request is accepted. Given that change requests have been received, the Policy Committee shall conduct a change approval meeting at least quarterly. The Policy Committee may invite change requestor contacts and stakeholder experts to participate in the discussion. After discussion, the change approval meeting can decide to:

1. Fully accept the change request without any changes and proceed directly to the change publication and announcement step.
2. Partially accept the change request and proceed to the change publication and announcement step.
3. Decide on a modified change request and proceed to the change publication and announcement step.
4. Request modification of the change request by the initial change requestor and resubmission of the change request.
5. Fully reject the change request.

10.2.4 Change publication and announcement

Once a change request is approved by the Policy Committee during its change approval meeting, it shall publish an updated provisional version of the CP and announce a due date to become effective and an implementation time frame for the transition once the new policy becomes effective to all SCMS elements. Any root CAs/Electors listed on the CTL shall make appropriate preparations to ensure that the implementation can be achieved during this stated time frame.

Members may submit change requests to modify announced 'changes for decision' at the next change approval meeting. Members may also submit change request limits or specifics affecting the due date or the implementation time frame. Changes to increase the time periods shall be scheduled before the next change approval meeting.

10.2.5 Change Implementation

Within the announced implementation period, each Root CA/Elector listed on the CTL shall implement the changes and provide appropriate evidence that it has fulfilled the changed requirements to the SCMSMO.

After implementation, the Policy Committee updates the CP to match the provisional CP as published in the previous step. At this time, the updated CP replaces the previous version of the CP.

11 References

11.1 Sources

The documents leveraged for the creation of this CP were: *European Union, 2019, C-ITS Certificate Policy [please insert a hyperlink to the respective EU Certification Policy], © European Union, 2019. This material is shared under the Creative Commons Attribution 4.0 International (CC BY 4.0) license. This material is provided 'as-is' and 'as-available' without any representation or warranties of any kind, either express, implied, statutory or other as set out under the Creative Commons Attribution 4.0 International (CC BY 4.0) license.*

11.2 Changes compared to C-ITS

The copyright of European Union, 2019, C-ITS Certificate Policy requires that if it is used, the changes must be attributed.

The initial 0.9 version adopted sections without change and sections with modifications. These changes are listed in the next sections. Later modifications will be published/ noted in the version tracking section.

11.2.1 Adopted modified sections

Sections of the European Union, 2019, C-ITS CP adopted with amendments:

1.4.1, 1.4.2, 3.1.1.1, 3.1.1.2, 3.2, 3.2.1, 3.2.2, 3.2.2.1, 3.2.2.2, 3.2.2.3, 3.2.2.4, 3.2.3.1, 3.2.3.2, 3.2.3.3, 3.2.5.1, 3.2.5.2, 3.2.5.3, 3.2.6, 3.3.1.3, 3.3.1.4, 3.3.2, 3.4.1.1, 3.4.1.2, 4.1, 4.1.1.1, 4.1.1.2, 4.1.1.3, 4.1.1.4, 4.1.1.5, 4.1.1.6, 4.1.2, 4.1.2.1, 4.1.2.2, 4.1.2.3, 4.1.2.4, 4.1.2.5, 4.2.1.1, 4.2.1.2, 4.2.1.3, 4.2.1.4, 4.2.1.5, 4.2.1.6, 4.2.2.1, 4.2.2.2, 4.2.2.3, 4.2.2.4, 4.2.2.5, 4.2.2.6, 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4,4.2.3.1,4.2.3.2,4.2.3.3,4.2.3.4, 4.3.1.1, 4.4.2, 4.5.1.1, 4.6, 4.8.1, 4.8.2.1, 4.8.2.2, 5, 5.1, 5.1.1, 5.1.1.1, 5.1.1.2, 5.1.2, 5.1.2.1, 5.1.2.2, 5.1.3, 5.1.4, 5.1.5, 5.1.6, 5.1.7, 5.1.8, 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.3.1, 5.3.2, 5.3.3, 5.3.4, 5.3.5, 5.3.6, 5.3.7, 5.3.8, 5.4.2, 5.4.6, 5.4.8, 5.5.1, 5.5.2, 5.5.3, 5.5.4, 5.5.5, 5.5.6, 5.5.7, 5.7.1, 5.7.2, 5.7.3, 5.7.4, 5.8.1, 5.8.2, 5.8.3, 6.1, 6.1.1, 6.1.1.1, 6.1.2, 6.1.3, 6.1.4, 6.3, 6.4, 6.5, 7.1, 7.2, 7.3, 7.4, 8.1, 8.2, 8.3, 8.4, 8.5, 8.6, 9.1, 9.2, 9.3, 9.4, 10.2

The nature of modifications:

- adding sections of description and requirements for the SCMS model elements not present in the CCMS,
- modification of the requirements to align with the SCMS requirements,
- merge of the audit and auditor requirements to support the interoperability.

11.2.2 Adopted unchanged sections

Sections of the European Union, 2019, C-ITS CP adopted unchanged:

4.8.3.2, 4.8.3.3, 4.10.3.3, 4.10.3.4, 5.2, 5.4, 5.4.3, 5.4.4, 5.4.5, 5.4.7, 5.5.6, 6.2

The 5G Automotive Association (5GAA) is a global, cross-industry organisation of over 115 members, including leading global automakers, Tier-1 suppliers, mobile operators, semiconductor companies, and test equipment vendors.
5GAA members work together to develop end-to-end solutions for future mobility and transport services.
5GAA is committed to helping define and develop the next generation of connected mobility, automated vehicles, and intelligent transport solutions based on C-V2X.
For more information, please visit https://5gaa.org


5GAA
Automotive Association