SAESOL TECH V2X PKI SERVICE

CERTIFICATE POLICY

Version 1.0.0

July 28, 2026

Author

SAESOL Tech Certificate Policy Authority

Table of Contents

Revision History

Version	Approval date	Changes
1.0.0	2026. 7. 28	Initial version

1 Introduction

This document is the SAESOL Tech V2X RootCA Certificate Policy. It describes the certificate management for all components of the V2X ecosystem operated in the United States. It follows the approach described in IETF RFC 3647.

1.1 Overview

This Certificate Policy establishes the implementation-specific requirements for deploying an SCMS in accordance with IEEE 1609.2.1 [1]. The provisions of IEEE 1609.2.1 [1] shall be considered normative in addition to the requirements specified herein, even where not explicitly referenced. References to selected clauses of IEEE 1609.2.1 [1] are provided only for convenience and to facilitate consistent interpretation. Although this policy is primarily intended for SCMS Providers, it also includes requirements applicable to other participants, such as the SCMS Manager, in order to define the overall governance framework of the SCMS ecosystem(Electors, Certificate Authorities, Sub-Certificate Authorities, End-Entities, and End-Entity Operators).a

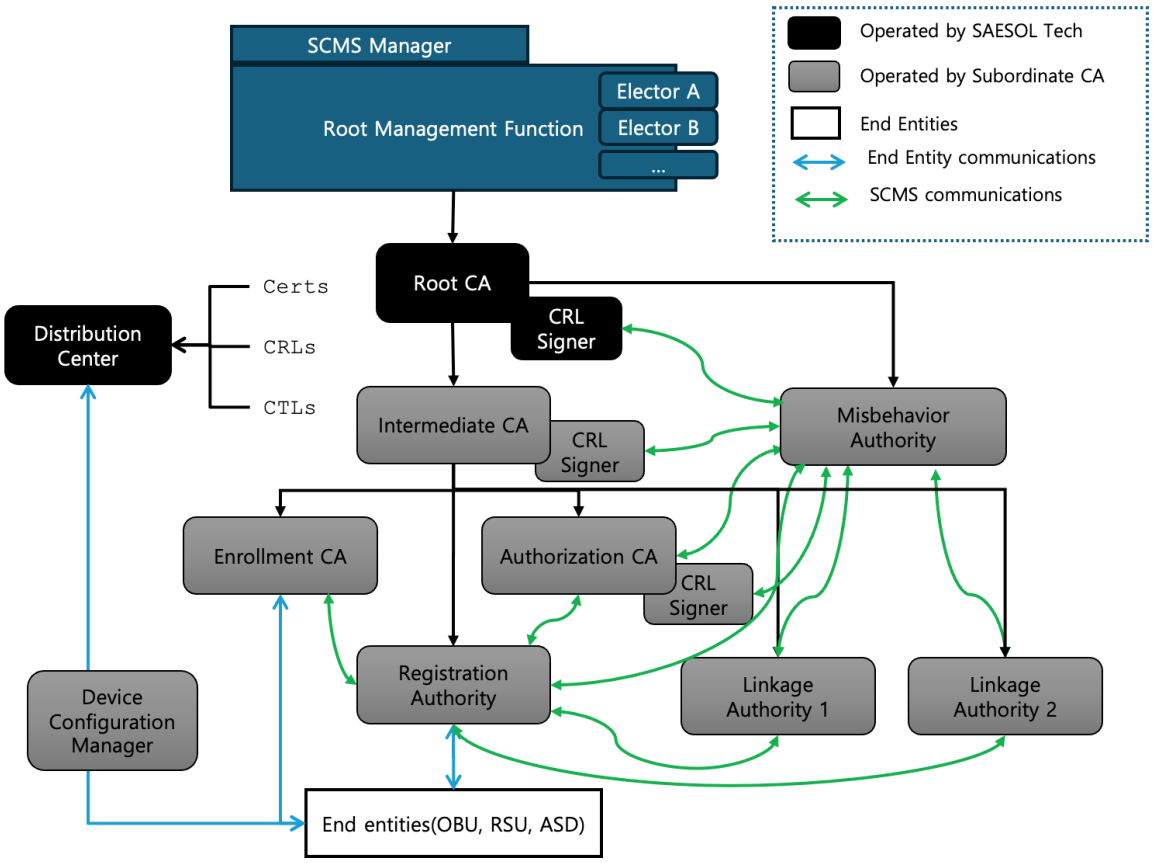

Figure 1-1 SCMS Architecture

1.2 Document Name and Identification

Issuer	SAESOL Tech
Document name	V2X PKI Service Certificate Policy
Version	1.0
Effective date	August 31, 2026

1.3 PKI Participants

1.3.1 SCMS Manager

(1) The SCMS Manager manages other aspects of overall system operation and security, including the publication of the Certificate Trust List (CTL) which includes the certificates of Electors.

1.3.1.1 Publication Center(Pub)

(2) The publication center is a functional component of the SCMS Manager that is a platform where the entity publishes its certificate policy, CTL and optional additional information. The details of the publication center are the subject of the respective SCMS Manager's certificate policy.

1.3.2 Electors

(3) The Electors are responsible for signing the CTL upon an authenticated request from SCMS Manager.

(4) Creation of a validly signed CTL requires a quorum of electors. The maximum number of electors is set at five. The SCMS Manager will use best efforts to ensure that maximum number of electors is always active, and all electors sign each CTL. The number required to establish a quorum is three. SCMS Manager will ensure that at least a quorum of electors is available and sign each CTL. SCMS Manager reserves the right to change the number of electors or the quorum but has no plans to do so.

1.3.3 Accredited PKI Auditor

(5) Accredited PKI Auditor is authorized for auditing SCMS Providers and Electors as stated in Section 8:

(6) shall audit the Electors and the SCMS Providers, which are operating Root CAs or a SubCAs.

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

(8) shall be responsible to distribute the audit results to audited entity. The audited entity shall provide these results to SCMS Manager for validation for inclusion of Elector or SCMS Providers' Root CA.

1.3.4 SCMS Provider

(9) An 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.

(10) 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).

(11) 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.

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

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

(14) An SCMS Provider shall cooperate with MAs.

1.3.4.1 Root CA

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

1.3.4.2 Intermediate CA(ICA)

(16) 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.

1.3.4.3 Enrollment CA(ECA)

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

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

(19) Enrollment CA

(a) shall support:

- IEEE 1609.2.1 enrollment certificates for enrollment certificate request,

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

- X.509 certificates for enrolment certificate request,
- OAuth access token for enrollment certificate request at the ECA

1.3.4.4 Authorization CA(ACA)

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

1.3.4.5 CRL Signer

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

1.3.4.6 Distribution Center

(22) SCMS Provider can have a Distribution Center, where the following public information could be available, where applicable:

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

(b) Composite certificate files (CCF)

(c) Certificate revocation lists (CRL)

(d) Certificate Trust Lists (CTL)

(e) Composite CRLs, including their CTL according to IEEE 1609.2.1 [1

1.3.4.7 Linkage Authority (LA)

(23) As stated in IEEE 1609.2.1 A component of the Security Credential Management System (SCMS) 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 (EE) against the Authorization Certificate Authority (ACA).

1.3.4.8 Misbehavior Authority (MA)

(24) As stated in IEEE 1609.2.1: A component of the Security Credential Management System (SCMS) that receives reports of malicious or potentially malicious application activities, analyzes them, and determines whether or not to take mitigating actions.

(25) MA operates in cooperation with LA, RA and ACA.

(26) An MA shall cooperate with all SCMS Providers published on the CTL.

(27) An MA shall provide linking information for reported ACs.

(28) An MA shall support the end entity revocation requests from other MAs and shall support forwarding of requests to other MAs as appropriate.

1.3.4.9 Registration Authority (RA)

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

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

(31) Supporting the authorization certificate provision to valid end entities,

(32) Supporting the successor enrollment certificate provision to valid end entities,

(33) Providing system information for end entities (CTL, Certificate chain certificates, CRL, CCF)

(34) Forwards misbehavior reports for MA.

(35) With regard to 오류! 참조 원본을 찾을 수 없습니다. 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.

1.3.4.10 Device Configuration Manager(DCM)

(36) 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)

1.3.5 End Entity (EE)

(37) The End Entities are on board unit(OBU), road-side unit(RSU) or aftermarket safety device(ASD) which use certificates and related keys to sign and/or encrypt messages for different applications.

1.4 Certificate Usage

1.4.1 Applicable domains of use

(38) IEEE 1609.2 certificates issued under the present CP are intended to be used to validate digital signatures and encryption/decryption in the SCMS V2X communication context.

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

1.4.2 Limits of responsibility

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

- circumstances that offend, breach or contravene any applicable law, regulation, decree or government order,
- circumstances that breach, contravene or infringe the rights of others,
- breach of this CP or the relevant subscriber agreement,
- 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),
- circumstances that contravene the overall objectives of greater road safety and more efficient road transport.

1.5 Policy Administration

1.5.1 Organization Administrating the Document

(41) The SAESOL Tech V2X Root CA PA approves this CP and related operational documents and legal agreements.

1.5.2 Contact Person

(42) Communications regarding CA policies and certification practices should be sent to the PA by registered mail or electronic mail to v2x.pa@saesol.tech

1.5.3 Person Determining CPS Suitability for the Policy

(43) Members of the Policy Authority are listed in the internal SAESOL Tech V2X Root CA organizational roster and also included in the v2x.pa@saesol.tech mailing list.

(44) The SAESOL Tech V2X PA is responsible for determining the suitability of policies illustrated within this CPS. The SAESOL Tech V2X PA is also responsible for determining the suitability of proposed changes to the CPS prior to the publication of an amended edition.

1.5.4 Updating of CPSs of CAs listed in the CTL

(45) 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.

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

(47) 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 security-relevant changes to the CP.

(48) 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.

(49) The Root CA shall notify the SCMS Manager EAC of any change made to the CPS with at least the following information:

- an exact description of the change,
- the rationale for the change,
- contact details of the person responsible for the CPS,
- planned timescale for implementation.

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

1.5.5 CPS approval procedures

(51) 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.

(52) Based on the audit results of Root CA/Elector, the SCMS Manager EAC will decide about the addition of Root CA/Elector to the CTL.

(53) 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

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

For easy read, they are referenced bellow:

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 (EE) 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 (SCMS) 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 butterfly key expander (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 Security Credential Management System (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 Security Credential Management System (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 Security Credential Management System (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 Security Credential Management System (SCMS) that is responsible for bootstrapping an end entity (EE) 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 end entity (EE) device contains a proof that the device is entitled to that enrollment certificate.

distribution center (DC): A component of the Security Credential Management System (SCMS) that distributes public information such as certificates and certificate revocation lists. Contrast: registration authority (RA).

elector: A component of the Security Credential Management System (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 end entity (EE) and the Security Credential Management System (SCMS). Contrast: authorization certificate.

enrollment certificate authority (ECA): A certificate authority (CA) that issues enrollment certificates.

(55) **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 uniform resource locator (URL) 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 end entity (EE) device does not contain a proof that the device is entitled to that enrollment certificate, and the proof is instead provided to the enrollment certificate authority (ECA) by some other means.

individual certificate request: A request for a certificate authority (CA) to issue a single certificate. The request may come from the relevant end entity (EE) or from the registration authority (RA). Contrast: butterfly key certificate request.

intermediate certificate authority (ICA): A certificate authority (CA) whose certificate was issued by another CA and whose main responsibility is to issue certificates to another CA, that is, an authorization certificate authority (ACA), an enrollment certificate authority (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 end entity (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 Security Credential Management System (SCMS) that provides inputs to the linkage value calculation process to enable efficient revocation of pseudonym certificates while preserving the privacy of an end entity (EE) against the authorization certificate authority (ACA).

location obscurer proxy (LOP): A component of the Security Credential Management System (SCMS) that is responsible for hiding location information of an end entity (EE) from the registration authority (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 Security Credential Management System (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 end entity (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 Security Credential Management System (SCMS) that is the main point of contact for an end entity (EE), and is responsible for provisioning the EE with authorization and successor enrollment certificates. Contrast: distribution center (DC), IEEE Registration Authority (IEEE RA).

root certificate authority (Root CA): A certificate authority (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 (SCMS) manager: A component of the Security Credential Management System (SCMS) whose role is to govern the entire SCMS, including defining and enforcing the certificate and security policies to be applied to Electors and Root CAs.

Subordinate Certificate Authority(SubCA): A **Subordinate CA** is a Certificate Authority that operates under the authority of a **Root Certificate Authority** (Root CA). It is issued a certificate by the Root CA (or another higher-level intermediate CA), allowing it to issue digital certificates to end entities such as servers, devices, or users.

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
API	Application Programming Interface
ASD	Aftermarket Safety Device
AT	Access Token
CA	Certificate Authority
CCF	Certificate Chain File
CRACA	Certificate Revocation Authorizing Certificate Authority
CRL	Certificate Revocation List
CTL	Certificate Trust List
DC	Distribution Center
DCM	Device Configuration Manager
DER	Distinguished Encoding Rules
DNS	Domain Name System
ECA	Enrollment Certificate Authority
ECC	Elliptic Curve Cryptography
EE	End Entity
FQDN	Fully Qualified Distinguished Name
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
ITS	Intelligent Transportation Systems
LA	Linkage Authority
MBR	MisBehavior Report

Acronym or abbreviation	Meaning
OBU	OnBoard 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
PDU	Protocol Data Unit
PKI	Public Key Infrastructure
PSID	Provider Service Identifier
RA	Registration Authority
RFC	Request for Comments
RSU	RoadSide Unit
SCMS	Security Credential Management System
SSP	Service Specific Permissions
TLS	Transport Layer Security
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
V2X	vehicle to everything

Table 1-1 Acronym or abbreviation

2 Publication and Repository Responsibilities

2.1 Repositories

(56) The CA should maintains a repository which is accessible to relevant PKI participants and other stakeholders.

2.2 Publication of Certification Information

(57) The repository identified in Section 2.1 should publish the following information:

- A reference to the Certification Practices Statements
- The information listed in the Section 1.3.4.9 Distribution Center

2.3 Time or Frequency of Publication

(58) SCMS Provider shall publish their newly issued CAs' certificates as it starts its operation via DC and RA. CRLs including composite-CRL-CTL are published within 24 hours after a status change via DC and RA. CCF-CTL are published within 6 hours after CCFs including other SCMS's and CTL are changed.

(59) Certificate Practice Statements shall be published within 15 days after accepted modification from PA.

(60) Individual CRLs shall be also published at PKI website within 5 days after it is published by CRL signer.

(61) CA's certificates shall be also published at PKI website within 5 days after it starts operating.

2.4 Access Controls on Repositories

(62) The repositories are hosted within an access-controlled portal managed by SAESOL Tech, in accordance with the security policies of the SAESOL Tech V2X network platform. Updates can only be made by authorized SAESOL Tech

portal administrators or programmatically by the CA. Portal administration secured using mutually authenticated HTTPS or SSH connections. CRL distribution points within the CA hierarchy are readable by PKI participants. Subscribers and other PKI participants can access other areas of repositories using credentials which are made when they sign up.

3 Identification and Authentication

3.1 Naming

3.1.1 Type of Names

3.1.1.1 Names for Electors and Root CAs

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

3.1.1.2 Names for ICA

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

3.1.1.3 Names for ACA

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

3.1.1.4 Names for ECA

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

(67) 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

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

(69) 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

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

(71) 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 Certificate

(72) 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 Ids.

(73) 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.

(74) 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

(75) 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 or Pseudonymity of Subscribers

(76) 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

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

(78) The Enrollment CA shall be able to distinguish the identities of all client End Entities.

(79) SCMS Manager ensures that a Root CA 3-byte hash certificate identifier (HashedId3) is unique in the scope of the overall trust model.

(80) 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.

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

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

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

(83) 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
Root CA	SCMS Manager organization	self-signed IEEE1609.2 certificate

Key owner	The actor responsible for the verification	Comments
ICA	Root CA	
ECA	ICA	
RA	ICA	
ACA	ICA	
LA	ICA	
MA	Root CA	
CRL-Signer	corresponding CA such as RootCA, ICA or ACA	
DC	ICA	

3.2.2 Authentication of Organization Identity

3.2.2.1 Authentication of Elector Organization Identity

(84) The Elector shall provide to SCMS Manager evidence of the identification and accuracy of the name and associated data. The EAC is responsible for validation of the Elector.

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

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

3.2.2.2 Authentication of Root CA's Organization Identity

(87) In an application form to SCMS Manager, 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 sub CAs.

(88) SCMS Manager checks 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.

(89) SCMS Manager collects 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.

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

(91) 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

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

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

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

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

(a) determine that the organization exists by using at least one third-party identity proofing service or 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 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.

3.2.2.4 Authentication of End Entities' Subscriber Organization

(96) Before the subscriber of End-Entities (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 hardware and software versions of the EE) meets all the following compliance assessment criteria:

(97) Attestation of compliance with SCMS Manager's CP.

(98) Confirm standards compliance and interoperability validation via by OmniAir.

(99) At a minimum, the ECA shall:

(a) determine that the organization exists by using at least one third-party identity proofing service or 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.

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

3.2.3 Authentication of Individual Entity

(101) Subscribers shall provide the names of the individuals who are authorized ("Authorized Individuals") to act on behalf of the Applicant/Subscribers for correspondence with the SCMS Provider.

3.2.3.1 Authentication of Elector/SubCA/Other SCMS Model Elements In dividual Identity

(102) 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.

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

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

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

3.2.3.2 Authentication of End Entities' Subscriber Identity

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

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

3.2.3.3 Authentication of the End Entities' Identity

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

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

(109) EE subjects of authorization certificate shall authenticate themselves when requesting authorization certificate 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

(110) 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

(111) 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

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

3.2.6 Criteria for Interoperation

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

(114) 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 Routine Re-Key

3.3.1.1 Elector certificates

Not applicable.

3.3.1.2 Root CA certificates

Not applicable.

3.3.1.3 ICA, ECA, RA, ACA, LA, MA, CRL signer, DC Certificate Renewal or Re-keying

(115) Prior to the expiry of a Sub-CA or other SCMS model elements certificate, 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 signs 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. If an encryption and decryption key pair is used, possession of private decryption keys shall be proven.

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

3.3.1.4 End Entity's Enrollment Credentials

(117) 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 key pair and request a successor certificate containing the new public key; the request shall be signed with the current valid enrollment certificate private key.

(118) The EE shall sign the enrollment certificate request with the newly created private key (inner signature) to prove possession of the new private key. 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 Entity's Authorization Credentials

(119) 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

(120) The identification and authentication for a Root CA and a SubCA certificate re-keying after revocation is handled in the same way as the initial issuance of that certificate

3.3.2.2 End Entities Certificates

(121) The authentication of an end entity for enrollment or authorization certificate re-keying after revocation is handled in the same way as the initial issuance of that certificate.

3.4 Identification and Authentication for Revocation Request

3.4.1 Elector and Root CA Certificates

(122) If an Elector or a Root CA decides to request its removal from the CTL, the request to remove itself from the CTL shall be authenticated by the Elector / Root CA to SCMS Manager.

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

(a) a written and signed message on corporate letterhead, or a digitally/electronically signed message (including email or electronic official correspondence) 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.

3.4.2 ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC Certificates

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

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

(a) a written and signed message on corporate letterhead, or a digitally/electronically signed message (including email or electronic official correspondence) 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.

3.4.3 End Entity Enrollment Certificates and Authorization

(126) Request to revoke an EE enrollment certificate can originate from the EE subscriber or from MA. If initiated by the subscriber, the requester shall authenticate themselves to the MA.

(127) (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 to the MA.Certificate Life-Cycle Operational Requirements

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

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

(a) registration and setup of a trust relation between the Electors and the SCMS Manager Organization including the insertion of the Elector certificate in the CTL;

(b) registration and setup of a trust relation between the Root CA and the SCMS Manager Organization, including the insertion of the first Root CA certificate in the CTL;

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

(d) registration and setup of a trust relation 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 entities request for enrollment certificate and authorization certificate.

(129) 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

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

4.1.1.2 Root CA

(131) 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 SCMS Manager.

4.1.1.3 ICA

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

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

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

4.1.1.5 CRL Signer

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

4.1.1.6 End Entities

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

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

(137) Each EE may send authorization certificate requests without requestingrequiring 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 Enrollment Process and Responsibilities

(138) Permissions for root-CAs and SubCAs issuing certificates for special (governmental) purposes (i.e. special mobile and fixed EEs) where restricted by law may be granted only by the relevant authority having jurisdiction granted by legislation to authorize the requested credentials.

4.1.2.1 Electors

(139) After being audited and selected the Elector is responsible to sign the to be signed CTL prepared by SCMS Manager.

(140) The Elector’s enrollment process is based on a signed application that shall be securely delivered to SCMS Manager by the Elector’s authorized representative.

(141) The Elector’s application shall be signed by its authorized representative.

(142) In addition to the application, the Elector's authorized representative shall provide a copy of the Elector's CPS and its audit results to SCMS Manager. In case of positive approval, SCMS Manager generates and sends a certificate of conformity to the corresponding Elector.

(143) The Elector addition to the CTL is SCMS Manager internal process, processed by the EAC.

4.1.2.2 Root CAs

(144) After being audited by accredited 3rd party auditor, Root CA apply for insertion of its certificate in the CTL.

(145) The Enrollment process is based on a signed application that shall be securely delivered to SCMS Manager by the Root CA's authorized representative.

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

(147) In addition to the application form, the Root CA's authorized representative provide its audit results to SCMS Manager for approval. In case of positive approval, SCMS Manager generates and sends a certificate of conformity to the corresponding Root CA.

(148) The Root CA addition to the CTL is an SCMS Manager defined internal process, processed by the Ecosystem Audit Committee(EAC).

4.1.2.3 ICAs

(149) After being audited, the ICA can request certificate from the Root CA.

(150) Before an Intermediate Certificate Authority (ICA) is allowed to participate in the SAESOL Tech V2X PKI, the ICA must complete a formal enrollment process. This process includes the following steps:

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

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

(152) If the ECA, RA, ACA, LA, MA, CRL Signer, DC is owned by an entity different than the entity that owns the ICA, before issuing a SubCA or other SCMS elements certificate request, the SubCA's or other SCMS elements entity shall have a contract with the ICA service provider.

4.1.2.5 End Entity

(153) The EE subscriber shall store the proof of certification for each device type that is enrolled at an ECA.

(154) The EE subscriber can use multiple methods of authorization described in Section 1.3.4.2 Enrollment CA(ECA)

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

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

(157) Regular EEs should be enrolled at a single ECA and therefore bound to a single RA for all of its certificates with a particular set of permissions. Special-purpose vehicles (such as police cars and other special-purpose vehicles with specific rights) may be enrolled at an additional ECA or have one additional enrollment for authorizations 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 SubCAs issuing certificates for such special-purpose EEs shall determine how the enrollment process applies to such EEs.

(158) If the EE is in the process of migrating from one ECA to another ECA, the EE may be enrolled at two ECAs.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

4.2.1.1 Identification and Authentication of Elector / Root CA

(159) SCMS Manager is responsible for authenticating the Elector /Root CA's authorized representative and approving its application. The application approval is done by the EAC.

(160) SCMS Manager confirms its positive validation of the application to the Root CA/Elector. The Elector/Root CA may then send its self-signed certificate to SCMS Manager, which adds the certificate of Root CA/Elector to the CTL.

4.2.1.2 Identification and Authentication of ICA

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

(162) he 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

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

(164) 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.I

4.2.1.4 dentification and Authentication of CRL Signer

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

(166) The corresponding CRACA shall confirm its positive validation of the application to the respective CRL Signer. The CRL Signer may then send a certificate request to the CRACA, which shall issue the certificate to the corresponding CRL Signer.

4.2.1.5 Identification and Authentication of EE Subscriber

(167) 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.

(168) 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

(169) During enrollment certificate requests, in accordance with IEEE 1609.2.1, the ECA shall use at least one of the authentication options mentioned in Section 1.3.4.3

(170) During successor enrollment certificate requests and successor enrollment certificate 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 1.3.4.3

(171) During authorization certificate requests and authorization certificate 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 1.3.4.9.

(172) 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 1.3.4.9.

4.2.2 Approval or Rejection of Certificate Applications

4.2.2.1 Approval or Rejection of Elector / Root CA Certificates.

(173) SCMS Manager EAC adds the Root CA/Elector certificate to the CTL, when it is clear from the audit results and the CPS that the Root CA/Elector is in compliance with this CPS.

4.2.2.2 Approval or Rejection of ICA certificates

(174) The Root CA shall verify the ICA certificate request based on its audit results. If this verification leads to 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

(175) The ICA shall verify the Sub-CAs or other SCMS elements certificate request based on its audit results. If this verification leads to positive result, the ICA may issue a certificate to the requesting entity.

4.2.2.4 Approval or Rejection of CRL Signer Certificates

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

4.2.2.5 Approval or rejection of enrollment certificate

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

4.2.2.6 Approval or rejection of authorization certificate

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

(179) 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

(180) 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

(181) 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 sub-CA or other SCMS element.

4.2.3.3 Enrollment Certificate Application

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

4.2.3.4 Authorization Certificate Application

(183) The processing of authorization certificate applications should 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

(184) The Elector shall issue its own self-signed Elector certificate in IEEE 1609.2.1 format and shall send it to SCMS Manager.

(185) SCMS Manager makes the Elector certificate is available as soon as possible via PUB.

(186) An Elector shall sign the to be signed CTL which was prepared for them by SCMS Manager EAC.

4.3.1.2 Root CA Certificate Issuance

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

(188) The SCMS Manager EAC checks the audit results and the CPS of the Root CA, before it includes the Root CA on the CTL.

(189) SCMS Manager makes the root certificate available as soon as possible via CTL at PUB, cf. Section 2.5.1.

4.3.1.3 ICA Certificate Issuance

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

(191) The Root CA shall check the audit results of the ICA, before issues certificate for it.

(192) 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

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

(194) The CRACA shall check the audit results of the CRL Signer, before issues certificate for it.

(195) 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

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

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

(198) 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

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

(200) 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 shall reject the certificate request.

(201) 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

(202) The ACA shall issue authorization certificates in IEEE 1609.2 format.

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

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

4.3.2 Notification to Subscriber of Issuance of Certificates by the CA

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

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

4.4.1.4 End Entity

(206) The end entity shall verify the received enrollment certificates and authorization certificates against its original request, including the signature and the certificate chain. It shall discard all EC/AC responses that are not correctly verified. In such cases, it should send a new enrollment certificate / authorization certificate request.

4.4.2 Publication of the Certificate

(207) Elector and Root CA certificates shall be made available to all participants through CTLs via the PUB of SCMS Manager

(208) SubCAs' or other SCMS model elements certificates is published by the issuing CA.

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

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

4.4.2.1 Notification of Certificate Issuance

There are no notifications of issuance.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

4.5.1.1 Private Key and Certificate Usage for Elector

(211) (204)(203)The Elector shall use its Elector private keys to sign its own (Elector) certificates and the CTL.

4.5.1.2 Private Key and Certificate Usage for Root CA

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

(213) 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

(214) 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.

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

4.5.1.4 Private Key and Certificate Usage for ECA

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

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

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

4.5.1.5 Private Key and Certificate Usage for RA

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

(220) RA certificates shall be used by SCMS model elements and end entities to encrypt PDUs for the RA..

4.5.1.6 Private Key and Certificate Usage for ACA

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

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

4.5.1.7 Private Key and Certificate Usage for LA

(223) The LA shall use its private keys to sign its own CSR.

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

4.5.1.8 Private Key and Certificate Usage for MA

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

(226) MA certificates may also be used by SCMS model elements to authenticate the MA in communication and to encrypt the key which is used to encrypt misbehavior reports.

4.5.1.9 Private Key and Certificate Usage for CRACA and CRL Signer

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

(228) CRACA and CRL Signer certificates shall be used by SCMS model elements and end entities to verify the CRLs.

4.5.1.10 Private key and certificate usage for End Entity

(229) 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.

(230) The end entity shall use its private key(s) to sign successor enrollment certificate requests and authorization certificate requests.

(231) 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.

(232) 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.

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

4.5.2 Relying Party Public Key and Certificate Usage

(234) Relying parties use the trusted certification path and associated public keys for the purposes referred to in the certificates and to authenticate the trusted common identity of enrollment certificates and authorization certificates.

(235) Certificates in the SCMS model shall not be used without a preliminary check by a relying party.

4.6 Certificate Renewal

not applicable.

4.6.1 Circumstance for Certificate Renewal

not applicable.

4.6.2 Who May Request Renewal

not applicable.

4.6.3 Processing Certificate Renewal Requests

not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

not applicable.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

not applicable.

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

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

4.7.2 Who May Request Certification of a New Public Key

4.7.2.1 Elector and Root CA

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

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

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

(239) The Sub-CA's or other SCMS element's certificate re-keying request shall be submitted in due time in order to be sure to have a new Sub-CA or other SCMS element certificate and operational Sub-CA or other SCMS element key pair before expiry of the current certificate. The date of submission must also take account of the time required for approval..

4.7.2.3 End Entity

(240) The end entity shall rekey its enrollment certificate according to IEEE 1609.2.1

4.7.3 Processing Certificate Re-Keying Requests

4.7.3.1 Elector and Root CA

Not applicable.

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

(241) The SubCA or other SCMS element may request a new certificate or a rekey certificate as follows:

(242) The SubCA 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 SubCA or other SCMS element should generate a new key pair and signs the request with the new private key (inner signature) to prove possession of the new private key. The whole request should be signed (oversigned) with the current valid private key (outer signature) to ensure the integrity and authenticity of the request.

4.7.3.3 End Entity

(243) The end entity shall rekey its enrollment certificate according to IEEE 1609.2.1.

4.8 Certificate Modification

Not applicable.

4.8.1.1 Circumstance for Certificate Modification

Not applicable.

4.8.1.2 Who May Request Certificate Modification

Not applicable.

4.8.1.3 Processing Certificate Modification Requests

Not applicable.

4.8.1.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.1.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.1.6 Publication of the Modified Certificate by the CA

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

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

(a) If SCMS Manager has reason to believe or strongly suspect that the corresponding Elector / Root CA private key has been compromised,

(b) If The issuing CA (Root CA or SubCA) has reason to believe that the private key associated with the certificate has been compromised.

(c) If the audit (see Section 8) leads to a negative result.

(d) If the SubCA or end entity is no longer associated with the EE subscriber or the organization managing the SubCA.

(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.

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

.

4.9.2 Who Can Request Revocation

(246) SCMS Manager Organization can trigger the removal of an Elector or Root CA from the CTL.

(247) The Elector and Root CA is aare self-signed certificates, so only the removal from the CTL can be requested by them from the SCMS Manager Organization.

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

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

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

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

(252) CAs shall accept revocation requests from all authorized and authenticated parties, such as an authorized US-DOT representative.

(253) CAs may establish procedures that allow other entities to request Certificate revocation for fraud or misuse. A 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 SCMS Manager Organization, unless the Provider determines a shorter time period is necessary due to criticality.

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

4.9.3 Procedure for Revocation Request

4.9.3.1 Removal of an Elector

(255) An Elector is removable from CTL. In the case of removal, SCMS Manager publishes a new CTL as soon as possible and without undue delay.

(256) The Elector removal from the CTL is the responsibility of the SCMS Manager EAC, as defined in its internal processes.

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

4.9.3.2 Removal of a Root CA

(258) A Root CA shall be removable from CTL. In the case of removal, SCMS Manager publishes a new CTL as soon as possible and without undue delay.

(259) The Root CA removal from the CTL is the responsibility of SCMS Manager EAC, as defined in its internal processes.

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

4.9.3.3 Revocation of ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC Certificates

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

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

(263) (256)(255)The Sub-CA and the other SCMS elements 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.

4.9.3.4 Revocation of Enrollment Certificates

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

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

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

4.9.3.5 Revocation of Authorization Certificates

(267) 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) EE subscriber requests the revocation

(b) EE subscriber termination,

(c) MA requested it,

(d) when a court decision orders,

(268) The ACA shall process the revocation request – at normal conditions – in 5 days. If the revocation cause is the compromise of the key, this revocation is done as soon as possible.

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

4.9.4 Processing of misbehavior reports

(270) An SCMS 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 relevant and valid CTL root certificate of the MA is listed

4.9.5 Revocation Request Grace Period

(271) No fixed revocation request grace period is specified. Authorized Revocation Requesters shall submit a revocation request without undue delay after

obtaining sufficient information indicating that certificate revocation may be required.

4.9.6 Time Within Which CA Must Process the Revocation Request

(272) Upon receipt of a revocation request, the CA shall promptly evaluate the request and initiate any necessary investigation. A certificate shall be revoked only after sufficient evidence has been obtained to support the revocation. Accordingly, the time required to process a revocation request may vary depending on the nature and complexity of the investigation.

4.9.7 Revocation Checking Requirement for Relying Parties

(273) Relying Parties' devices and application software must check relevant CRLs and certification paths prior to relying upon a certificate.

4.9.8 CRL Issuance Frequency

(274) The CRL shall be published on a CA's own schedule and in all cases prior to the expiration of the current CRL. Each CRL is also issued no later than the '`nextCrl`' time specified in the previously published CRL for the same scope.

4.9.9 Maximum Latency for CRLs

(275) Each CA that issues CRLs shall define the CRL issuance frequency in its CPS. The defined frequency shall be appropriate to the certificate types, operational environment, and associated risk.

4.9.10 On-Line Revocation/Status Checking Availability

No stipulation.

4.9.11 On-Line Revocation Checking Requirements

No stipulation.

4.9.12 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.13 Special Requirements Re Key Compromise

(276) Actual or suspected key compromise is recognized as a critical security event. This CP does not prescribe specific response procedures for such events. Each CA should assess the associated risks and, where appropriate, establish procedures for handling key compromise in accordance with its operational requirements and applicable CPS.

4.9.14 Circumstances for Suspension

Not applicable.

4.9.15 Who Can Request Suspension

Not applicable.

4.9.16 Procedure for Suspension Request

Not applicable.

4.9.17 Limits on Suspension Period

Not applicable.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Not applicable.

4.10.2 Service Availability

Not applicable.

4.10.3 Optional Features

Not applicable.

4.11 End of Subscription

Not applicable.

4.12 Key Escrow and Recovery

Not applicable.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session key Encapsulation and Recovery Policy and Practices

Not applicable.

5 Facility, Management, and Operational Controls

(277) 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 …'.

(278) 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

(279) 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.

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

(281) 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

(282) 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 high-value and, sensitive information. Root CA shall be operated in a dedicated physical area separated from other PKI components’ physical areas.

(283) 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 located in a dedicated physical area under multiple access control.

(284) 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.

(285) Elector and Root CA 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.

5.1.1.2 SubCAs and other SCMS model elements

(286) The location and construction of the facility housing the Sub-CA's (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 highvalue and sensitive information. These can be in secure cloud environment based on risk analysis and with certified HSM.

(287) 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 is installed, so as to guarantee that sensitive data (key pair backup, activation data, etc.) are stored in a dedicated safe located in a dedicated physical area under multiple access control.

(288) 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.

(289) SubCAs 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

(290) 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 trusted-role physical access controls for the cryptographic HSM and activation data.

(291) 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 (tamper-proof 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.

(292) 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.

(293) 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 and 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

(294) SubCAs and other SCMS model elements may be operated in secure cloud environment based on risk analysis and with certified HSM.

5.1.3 Power and Air Conditioning

(295) 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 back-up installations are required in the event of external power failure and smooth shutdown of the C-Smooth shutdown of the C-ITS trust model equipment in the event of a lack of power. These SCMS model elements facilities shall be equipped with heating/ventilation/air-conditioning systems to maintain the temperature and relative humidity of the SCMS model element's equipment within operational range.

5.1.4 Water Exposures

(296) 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

(297) 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 fire-related threats. Media storage should be protected against fire in appropriate containers.

5.1.6 Media management

(298) 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.

(299) 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.

(300) 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.

(301) 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

(302) 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

(303) Back-ups of SCMS model elements, sufficient to recover from system failure, are made offline after SCMS model elements deployment and after each new key-pair generation. Back-up copies of essential business information (key pair, CRL, CTL, certificate, configuration) and software are made regularly. Adequate back-up facilities are provided to ensure that all essential business information and software can be recovered following a disaster or media failure. Back-up 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 back-up copy is stored at a site with physical and procedural controls commensurate to that of the operational PKI system.

(304) 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.

(305) 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

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

(307) Trusted persons have access to or control authentication or 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.

(308) Trusted roles shall include roles that involve the following responsibilities: [1]

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

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

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

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

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

5.2.1.1 Number of Persons Required per Task

(310) 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.

---

[1] based on the ETSI EN 319401 REQ-7.2-15 requirement

(311) 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.

(312) 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.

5.2.1.2 Identification and Authentication for Each Role

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

(314) SCMS model elements shall verify and confirm the identity and 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.

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

5.2.1.3 Roles Requiring Separation of Duties

(316) 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.

(317) 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.

(318) 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 staff in trusted roles.

(319) The SCMS Provider that serve 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

(320) 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 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

(321) 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.

(322) 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.

(323) 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.

(324) 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

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

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

(327) 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

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

(329) 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 fulfil their job responsibilities competently and satisfactorily.

(330) 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

(331) 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

(332) 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

(333) 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 if they were employees and that they fulfil the requirements applicable to employees.

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

5.3.8 Documentation Supplied to Personnel

(335) SCMS model elements shall provide their personnel with requisite training and access to the documentation they need to fulfil their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

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

5.4.1.1 Types of Events to be recorded and reported by Electors and S CMS Providers

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

(338) 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 (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).

(339) 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.

(340) Each event related to certificate life-cycle is logged in such a way that it can be attributed to the person that performed it.

(341) All logs shall be protected against non-authorized access.

(342) 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

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

(344) Audit log processing shall consist of a review of the audit logs and documenting the reason for all significant events in an audit log summary. Audit log 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 audit log reviews shall be documented.

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

(346) Each elector shall report its activities quarterly to SCMS Manager.

5.4.2.1 Retention Period for Audit Log

(347) Log records relating to certificate life cycles are kept for at least five years after the corresponding certificate expires.

5.4.3 Protection of Audit Log

(348) 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 life-cycle 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 multi-factor authentication. It must be technically ensured that users cannot access their own log files.

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

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

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

5.4.4 Audit Log Backup Procedures

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

5.4.5 Audit collection system (internal or external)

(353) 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.

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

5.4.6 Notification to Event-Causing Subject

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

5.4.7 Vulnerability Assessment

(356) The role in charge of conducting audit and roles in charge of realizing PKI system operation in the SCMS model elements explain all significant events in an audit-log 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.

(357) 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:

A. after any system or network changes determined by the SCMS model elements as significant for PKI components; and

B. 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 Records Archival

5.5.1 Types of Record Archiving

(358) SCMS model elements shall archive CA 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.

(359) 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 SCMS Manager 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/SubCA 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

(360) 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

(361) 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

(362) 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.

(363) The archive shall be protected against unauthorized viewing, modification, deletion or other tampering by storage in a trustworthy system.

(364) 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 CP.

5.5.4 System archive and storage

(365) SCMS model elements shall incrementally backed 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 an offsite secure facility.

5.5.5 Requirements for Timestamping of Records

(366) 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.

(367) 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

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

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

5.6 Key Changeover for trust model elements

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

(371) SubCA 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 elements certificate shall start prior to the planned deletion of the current private keys. The SubCA or other SCMS model elements shall take care that the new certificate is distributed to relevant subscribers and relying parties 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 Procedures

(372) 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.

(373) If theIf 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 certificate or Elector certificate shall be removed from the CTL. SCMS Manager 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 PKI has been compromised. In addition, SCMS Manager determines which services are to be maintained (or revoked) and how.

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

(375) If the personnel responsible for the management of a SubCA 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 in order 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 SubCA or SCMS model elements entity determines which services are to be maintained and how, in accordance with the SubCA entity business continuity plan. In the event of a PKI component being compromised, the SubCA or SCMS model elements entity shall alert its own superior CA (Root CA or ICA) and SCMS Manager.

5.7.2 Corruption of computing resources, software and/or data

(376) If a disaster is discovered that prevents the proper operation of a SCMS model element, the SCMS model element shall suspend its operation and investigate whether a private key has been compromised.

(377) 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

(378) 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 SCMS Manager, which will remove it from the CTL,

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

(379) If SubCA'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.

(380) 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 end entity.

(381) Where any of the algorithms or associated parameters used by the Elector, Root CA, SubCA or other SCMS model element or end entity becomes insufficient for its remaining intended usage, SCMS Manager (with a

recommendation from cryptographic experts) shall inform the Elector, Root CA, SubCA or other SCMS model element entity about which algorithms shall to be used.

5.7.4 Business Continuity capabilities after a disaster

(382) 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.

(383) After an incident above a certain risk level, the compromised CA must be re-audited by an accredited PKI auditor (see section 8).

(384) SCMS Manager shall have an action plan for the case when a compromised Root CA, SubCA or SCMS model element is unable to operate any longer (e.g. following a severe incident).

5.8 Termination and transfer

5.8.1 Elector

(385) The Elector may terminate its operation.

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

(387) In the event of the termination of the Elector, the Elector shall:

(a) request SCMS Manager 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 SCMS Manager.

(388) SCMS Manager then remove the corresponding Elector certificate from the CTL.

(389) SCMS Manager then adds a new Elector into the ecosystem.

5.8.2 Root CA

(390) 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.

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

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

(b) request SCMS Manager 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 last revocation status information (CRL signed by root CA) to the relying party 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 SCMS Manager.

(392) SCMS Manager then removes the corresponding Root CA certificate from the CTL.

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

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

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

(a) notice superior CA about the termination of services 90 days before the planed termination date and request of 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.

(395) The superior CA shall revoke the corresponding SubCA or other SCMS model elements certificate.

6 Technical Security Controls

6.1 Keypair Generation and Installation

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

(397) The process of deriving symmetric encryption keys and a MAC keys shall be carried out in line with IEEE 1609.2.

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

(399) 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.

(400) The RA, the ACA, and the end entities shall also support the butterfly key mechanism specified in the IEEE 1609.2.1. and my support the non-butterfly key mechanism.

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

6.1.1 Cryptographic Requirements

(402) 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

	ecdsaBrainpool P256r1 WithSha256	ecdsaBrainpool P384r1 WithSha384	ecdsaNist P256 WithSha256	ecdsaNist P384 WithSha384
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
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

(403) Requirements on key lengths and algorithms must be changed over time to maintain an appropriate level of security. SCMS Manager monitors 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, SCMS Manager will provide a migration strategy, which includes transition periods during which old algorithms and key lengths must be supported.

(404) (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 adapt to new vulnerabilities or new threats.

6.1.2 Secure storing of private keys

(405) SCMS model elements and end entities shall use validated HSM from the following list:

(a) 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)

A. CEN EN 419 221-2: Protection profiles for TSP cryptographic modules – Part 2: Cryptographic module for CSP signing operations with backup;

B. CEN EN 419 221-4: Protection profiles for TSP cryptographic modules – Part 4: Cryptographic module for CSP signing operations without backup;

C. CEN EN 419 221-5: Protection profiles for TSP cryptographic modules – Part 5: Cryptographic Module for trust services;

D. CEN EN 419 211-2: Protection profiles for secure signature creation device – Part 2: Device with key generation;

E. CEN EN 419 211-3: Protection profiles for secure signature creation device — Part 3: Device with key import.

F. Hardware Protected Security for Ground Vehicles J3101_202002

(406) 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

(407) 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.

(408) The manual access to, the cryptographic module stored keys of a SCMS model element shall require two-factor authentication from two trusted personnel.

(409) At least two authorized personnel is required for signing the CTL at Elector.

(410) At least two authorized personnel required for signing the CRL with the Root CA.

(411) The SubCAs can perform automatic signature, after a manual key activation.

(412) the cryptographic module of a SCMS model element or an end entity shall be protected against unauthorized removal, replacement and modification.

(413) A cryptographic module for end entities 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

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

(415) SCMS model elements shall backup their private keys.

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

6.1.4 Destruction of private keys

(417) 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.

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

6.2 Activation Data

(419) 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 elements cryptographic device shall require action by two authorized persons.

6.3 Computer Security Controls

(420) The Electors and CAs' computer security controls shall be designed in accordance with the 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

(421) The Electors' and CA's technical controls shall cover the whole life-cycle of the CA. In particular, this includes the requirements of section 6.1.1.1'Crypto-agility'.

6.5 Network Security Controls

(422) The Elector and Root CA shall be operated isolated from public networks.

(423) 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.

(424) The availability of the CA's networks shall be designed in the light of the estimated traffic.

7 Certificate profiles, CRL, CTL

7.1 Certificate Profiles

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

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

(427) 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.

(428) 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

SCMS element (certificate profile)	X.509 or IEEE 1609.2.1	IEEE 1609.2.1 type (Explicit and/or implicit)
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

(429) 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 generated in good time before expiry.

(430) The SCMS model elements 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

(431) 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 relying parties. During the overlap time, the old certificate shall be used only for verification of End entity.

(432) The end entity certificates should have the following time parameters:

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

(433) The Time-Period base parameters are the following:

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

7.3 Certificate revocation list

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

(435) The CRL shall be issued no later than the 'nextCrl' date in the current CRL. The interval between CRLs should be no more that four weeks..

7.4 Certificate trust list

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

(437) The CTL is valid until:

(a) a new CTL was issued,

(b) one of the Electors certificates used to sign the CTL is expired.

8 Compliance Audit and Other Assessments

8.1 Topics covered by audit and audit basis

8.1.1 SCMS Providers and Electors

(438) 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 SCMS Manager and used as a basis for deciding on the application for inclusion. Throughout this document references to an 'accredited PKI auditor' means a WebTrust accredited auditor.

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

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

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

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

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

(441) The accredited PKI auditor shall provide the results of the audit to the issuing CA or to the SCMS Manager EAC, as applicable.

8.1.2 End Entity devices

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

(a) Validated against the SCMS Manager "End-Entity Security Requirements, Design Guidance, and Validation Approach"

(b) Omniair Consortium certification

(c) for RSUs: ITE RSU Standard 1.0

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

(a) HSM modules validations defined in Section 6.1.2

8.1.3 End entity device operator

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

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

(a) this CP,

(b) and against ISO/IEC 27001 or TISAX, and

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

8.2 Frequency of the audits

8.2.1.1 SCSMS Providers and Electors

(446) Electors and SCMS Providers shall order a Webtrust 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 SCMS Manager requires it,

(c) every year during their operation.

8.2.2 End Entity devices

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

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

(b) If a device or HSM was recertified, the lifetimes in the (447)(a) shall be recalculated.

8.2.3 End entity device operator

(448) 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 three years during their operation.

8.3 Identity/qualifications of auditor

8.3.1 SCMS Providers and Electors

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

(450) The auditing body shall be accredited and certified for:

(a) WebTrust for CA V2.2

8.3.2 End Entity devices

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

(452) The device auditing body shall be accredited and certified for:

(a) ISO/IEC 15408, or

(b) ISO/IEC 19790, or

(c) Common Criteria, or

(d) Omniair schemas

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

(454) The HSM auditing body shall be accredited and certified for:

(a) Common Criteria

8.3.3 End Entity device operator

(455) The End Entity device operator shall select an accredited auditor to audit their organization to ensure they are in accordance with this CP and ISO/IEC 27001 or TISAX.

(456) The auditing body shall be accredited and certified for:

(a) ISO/IEC 27001 or TISAX

8.4 Auditor's relationship to audited entity

(457) 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

(458) If an Elector or a SCMS Provider makes an application with non-compliant audit results, SCMS Manager shall reject the application.

(459) If an Elector receives a non-compliant audit result, SCMS Manager shall order the Elector to take immediate preventive/corrective action and also shall prepare for the replacement of that Elector with a new one.

(460) If a Root CA receives a non-compliant audit result, SCMS Manager 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 EAC. The Root CA shall not be allowed to issue certificates during the suspension.

(461) In case of suspension the Root CA must take corrective action, re-order a full audit and make a new request for SCMS Manager for approval.

(462) In case of a sub-CAs (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

(463) The end entity subscriber shall regularly monitor the certification status of the HSMs and the devices and shall do actions if one of the certifications has been revoked.

(464) If a device or a HSM certification is revoked the following steps needs to be executed:

(a) The end entity subscriber shall identify the affected devices and contact the issuing CA in preparation for revocation of them,

(b) The issuing CA shall revoke the reported affected certificates.

8.5.3 End Entity device operator

(465) 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 has been revoked.

(466) If a device operators' certification has expired and has not been renewed or has been revoked the SCMS Provider shall not issue new certificates to that end entity device operator and shall not allow registration of new devices.

8.6 Communication of Results

8.6.1 SCMS Providers and Electors

(467) The Elector and the SCMS Provider of the Root CA shall send the audit results to SCMS Manager. The Elector and the SCMS Provider of the Root CA shall store all audit results. The SCMS Manager EAC sends a corresponding approval or rejection of acceptance to the Elector or SCMS Provider of the Root CA. In case of approval the EAC prepares a new CTL and sends it to the Electors for signing.

(468) The SCMS Provider of the Root CA shall share its certificate of conformity with the corresponding SubCAs/SCMS model participants. (ICA, ECA, ACA, RA, LA, MA, CRL Signer, DC)

8.6.2 End Entity devices

(469) The device operators of the devices should publish their certifications of devices on a publicly available URL.

(470) The end entity subscribers shall present the certification results of their devices to the SCMS Provider before enrolling a new kind of devices.

8.6.3 End Entity device operator

(471) The device operators should publish their certification audit results on a publicly available URL.

(472) The device operators shall present their audit results to the SCMS Provider.

9 Other provisions

9.1 Fees

(473) The members of SCMS Manager together fully finance the regular recurrent costs of operation of the SCMS Manager and the central elements (PUB) relating to the activities set out in this CP.

(474) The SCMS Providers are entitled to take fees from their Sub-CAs.

9.2 Financial responsibility

(475) Each SCMS Provider must demonstrate the financial viability of the legal entity implementing it for at least three years to the accredited PKI auditor. The fulfilment of this requirement shall be part of the audit results.

9.3 Confidentiality of business information

(476) 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

(477) The CPSs of the SCMS Providers shall set out the plan and the requirements for the treatment of personal information and privacy based on the applicable legislative 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 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 Root CA / Elector certificate(s) included in 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 SCMS Manager.

2. The representative of Root CA / Elector provides the audit results and CPS through the tracking system of SCMS Manager. The results and CPS shall be publicly available.

3. After all information is available for the EAC, a member of the EAC 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 SCMS Manager.

   During the public-discussion phase, any member of the EAC 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 the SCMS Manager Certificate Policy (CP). In this case a member of the EAC 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 EAC provides a summary within 5 business days in case no any 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 the step 3. or put on hold pending future discussions.

   If there is no unanimous decision in the EAC, the matter is put to a vote among the EAC members and a majority decision is adopted.

6. Following public discussion, a member of EAC will post on the SCMS Manager EAC list to indicate EAC's intent to either approve or reject the inclusion request, which is also last call for objection.

7. After one week, if no further questions or concerns are raised, then the EAC approves the request, prepares the new CTL update, and sends the tbsCTL 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 SCMS Manager. Every member can submit a change request. The request form shall contain:

- The description of change,
- A rationale for the change,
- The exact proposal including the line/paragraphs to be changed, the old text and the new text,
- The requester contact information.

The change requester should be prepared to answer requests for additional information and/or defend the change proposal at the Policy Committee.

10.2.2 The change processing

Within one working day after receiving the change request, the EAC confirms reception of the change request. Within 2 weeks after receiving a change request, the EAC starts processing the change. Processing of a change request means:

- Assessing the applicability of the change request.
- Assessing the completeness of the change request.
- Assessing the criticality of the change request.

- Assessing the impact of the change.

The change processing phase is concluded with scheduling the processed change request for decision in the next change approval meeting of the Policy Committee.

10.2.3 Change Approval

The EAC conducts change approval meetings to discuss and finally decide if a change request is accepted. Given that change requests have been received, the EAC conducts a change approval meeting at least quarterly. The EAC 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 the partial acceptance of the change 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 to 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 change approval meeting, the EAC publishes an updated provisional version of the CP and announces the implementation with a due date to become effective and an implementation time frame for the transition beginning once the new policy becomes effective to all SCMS elements.

Any root CAs / Electors listed on the CTL shall take appropriate preparation to ensure that the implementation can be achieved during the implementation time frame.

Member may submit change requests to modify announced changes for decision on the next change approval meeting. Members may also submit change request limited on the due-date or the implementation time-frame. Changes increasing the time periods can be decided to be scheduled before the next change approval meeting.

1. Change Implementation

Within the announced implementation period, each root CA / Elector listed on the CTL shall implement the changes and provide appropriate evidence to fulfil the changed requirements to SCMS Manager.

After implementation, the EAC 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.