Microsec ltd.

SCMS V2X PKI Service Certificate Policy

Version: 1.0

Date of effect: 2025-05-06

Object identifier: 1.3.6.1.4.1.21528.4.1.1.10

Version tracking

Version	Approval date	Changes
V1.0	2025-05-06	Initial version

Formatting, numbering

This document uses numbered lines in brackets to reference requirements; any new addition of requirements may break the external references.

It is therefore recommended that when an update of a requirement happens, the old requirement content will become Void, and the modified requirement gets a letter after the number (A to Z).

1. INTRODUCTION

1.1. Overview

The present document is a Certificate Policy (CP) for the V2X PKI services of Microsec ltd., intended to be used in the Security Credential Management System (SCMS).

This Certificate Policy sets out the specific, detailed ruleset for the implementation of the IEEE 1609.2.1 [1] standard, thus the requirements of the standard shall be applied in addition to present policy, even where not specified. Some details of IEEE 1609.2.1 [1] are referenced for ease of reading and uniform understanding.

The requirements in this Certificate Policy primarily concern the SCMS Providers, but the document also contains requirements for other actors (e.g. SCMS Manager) to provide a comprehensive overview of the ecosystem and the rules that apply to it.

The content structure of this CP complies with RFC 3647 [17].

1.2. Document name and Identification

Issuer	Microsec ltd.
Document name	SCMS V2X PKI Service Certificate Policy
Version	1.0
Date of effect	2025-05-06
OID	1.3.6.1.4.1.21528.4.1.1.10

1.3. PKI Participants

1.3.1. Introduction

Public key infrastructure (PKI) participants play a role in the PKI as defined by the present policy. Unless explicitly prohibited, a participant can assume multiple roles at the same time. Participants may be prohibited from assuming multiple specific roles at the same time to avoid conflicts of interest or to ensure a segregation of duties.

The hierarchy for the SCMS model is described in IEEE 1609.2.1 [1].

The PKI model participants are the participants described in the present Policy (see PKI Participants subsection). The reference architecture of IEEE 1609.2.1 [1] is presented in Figure 1.

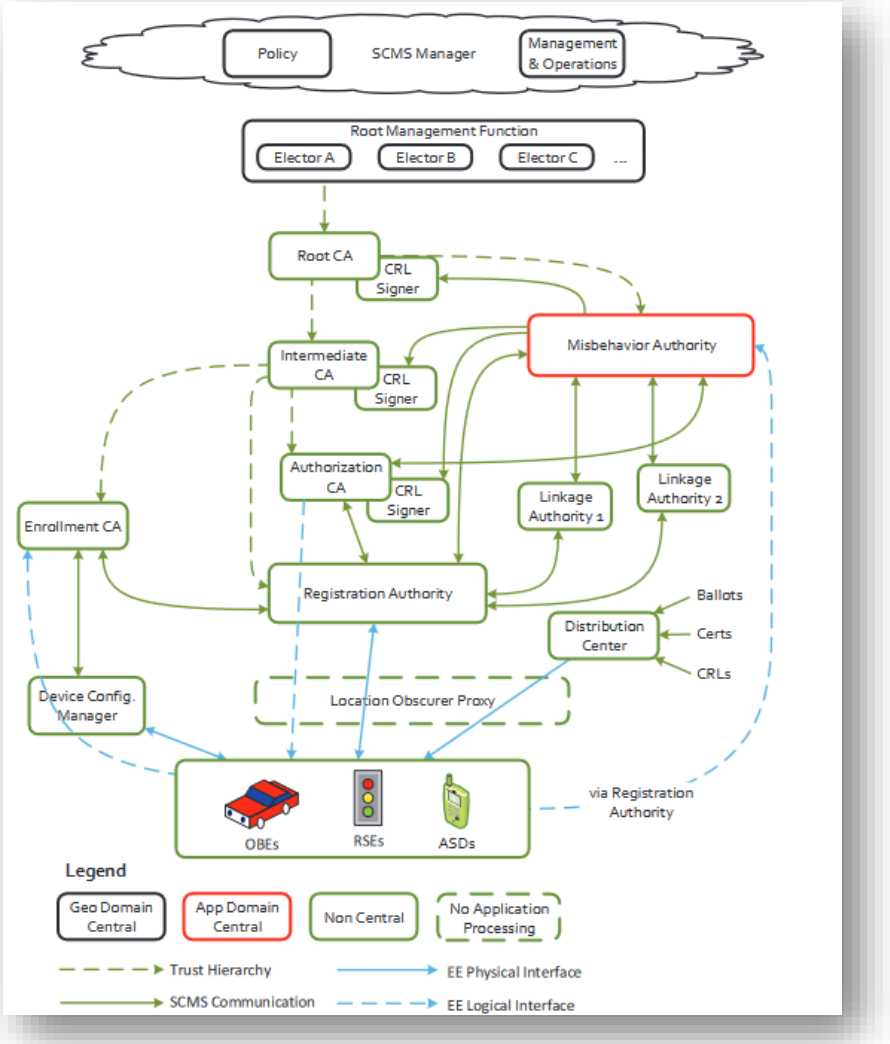

Figure 1: IEEE 1609.2.1 [1] reference architecture

1.3.2. SCMS Manager Organization

The SCMS Manager is a component of the SCMS whose role is to govern the entire SCMS, including defining the certificate and security policies and managing Electors and Root CAs.

As per IEEE 1609.2.1 [1], *"The ElectorGroupId is intended to allow multiple SCMS Managers each to maintain their own "panel" of Electors"*, there is no single SCMS Manager entity (in opposition to the CCMS model's CPOC), but there may be multiple organizations that take on this role..

1.3.2.1. Electors

Electors have the task to sign the *to be signed* certificate trust list (CTL), which is approved by the SCMS Manager.

The quorum of electors is the subject of the respective SCMS Manager's certificate policy, which shall be adhered to regarding the corresponding SCMS hierarchy.

1.3.2.2. Publication Center (PUB)

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.

1.3.3. Accredited PKI auditor

(1) The accredited PKI auditor is either:

(a) accredited for auditing SCMS participants as stated in Section 8 of present policy. The accredited PKI auditor:

- audits the SCMS Providers and Electors,
- verifies the CPS of the audited entity,
- is responsible for distributing – through the audited entity - the audit results to the CTL Committee of the SCMS Manager for validating the Electors' or SCMS Providers' Root CA inclusion in the CTL,
- decides if a CP modification requires a supplementary audit for the audited entity,

(b) accredited to certify end entity devices according to Section 8 of the present Certificate Policy.

1.3.4. SCMS Provider

(2) An SCMS Provider is an entity that operates one or more elements from the following list: Root CA, ICA, ECA, ACA, LA, RA, MA, CRL Signer, based on IEEE 1609.2.1 [1]. Where applicable, the SCMS Provider shall offer PKI services which are needed for revocation checking of certificates.

(3) The certification practice statement (CPS) of the SCMS Provider shall be compliant with the applicable certificate policy or policies (CP). The SCMS

Provider shall make its CPS and the applicable certificate policies available for its subscribers. The SCMS Provider shall manage its SCMS Services (including CAs) according to its CPS.

(4) The SCMS Provider shall be audited against the applicable CP and its CPS. The SCMS Provider may apply for the inclusion of its Root CA certificate on the CTL compiled by an SCMS Manager.

(5) The SCMS Provider should submit regular audit results to the SCMS Manager. The frequency of the audits is defined in Section 8.2 of the present Policy.

(6) If an 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, to get trusted Sub-CA certificates.

(7) An SCMS Provider should cooperate with Misbehavior Authorities (MAs).

1.3.4.1. Root CA

(8) As stated in IEEE 1609.2.1 [1], a Root CA (RCA) is 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)

(9) As stated in IEEE 1609.2.1 [1], an Intermediate CA (ICA) is a CA whose certificate was issued by another CA and whose main responsibility is to issue certificates to other subordinate CAs, like Authorization CAs (ACA) and Enrollment CAs (ECA).

1.3.4.3. Enrollment CA (ECA)

(10) As stated in IEEE 1609.2.1 [1], an Enrollment CA (ECA) is a CA whose main responsibility is to issue enrollment certificates.

(11) The initial enrollment certificate shall be provisioned via the Device Configuration Manager (DCM) or directly by the ECA or RA, while the successor enrollment certificate shall be provisioned by the Registration Authority (RA).

(12) Enrollment CAs:

(a) shall support:

- IEEE 1609.2.1 [1] enrollment certificates for enrollment certificate request,

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

- X.509 certificates for enrollment certificate request,
- OAuth access token for enrollment certificate request.

1.3.4.4. Authorization CA (ACA)

(13) As stated in IEEE 1609.2.1 [1], an Authorization CA (ACA) is a CA whose main responsibility is to issue authorization certificates.

1.3.4.5. CRL Signer

(14) A CA's certificate revocation list (CRL) shall be signed by the CA itself or by a dedicated CRL Signer.

1.3.4.6. Distribution Center

(15) Every SCMS Provider shall have a Distribution Center, where the following public information shall 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)

(16) As stated in IEEE 1609.2.1 [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)

(17) As stated in IEEE 1609.2.1 [1], a Misbehavior Authority (MA) is a component of the SCMS that receives reports of malicious or potentially malicious application activities, analyzes them, and determines whether to take mitigating actions.

MAs operate in cooperation with Linkage Authorities (LA), Registration Authorities (RA) and Authorization CAs (ACA).

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

(19) An MA should provide linking information for reported authorization certificates.

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

1.3.4.9. Registration authority (RA)

(21) Based on IEEE 1609.2.1 [1], a Registration Authority (RA) is a component of the SCMS that is generally the main point of contact for an End Entity (EE) and is responsible for provisioning the EE with authorization certificates. The RA also provides system information and forwards misbehavior reports for the MA.

(22) In accordance with (12), the RA:

(a) shall support:

- IEEE 1609.2.1 [1] enrollment certificates for authorization certificate request,

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

- X.509 certificates for authorization certificate request,
- CAMP certificates,
- OAuth access token for authorization certificate request at RA.

1.3.4.10. Device Configuration Manager (DCM)

(23) A Device Configuration Manager (DCM) is 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 IEEE 1609.2.1 [1]).

1.3.5. End Entity

(24) The End Entities (EE) are on-board units (OBU) or road-side units (RSU) which use certificates and the related cryptographic keys to sign and/or encrypt messages for different applications.

1.4. Certificate usage

1.4.1. Applicable domains of use

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

(26) The certificate profiles defined in IEEE 1609.2.1 [1] determine the certificate usages of the SCMS ecosystem entities.

1.4.2. Limits of responsibility

(27) 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,
- circumstances that breach 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 in North America, Australia, Korea, Japan or another jurisdiction.

1.5. Policy administration

1.5.1. Updates of this certificate policy

(28) The present Certificate Policy is managed by Microsec ltd. according to its internal quality and information security management policies.

(29) In case a change to present Certificate Policy is necessary or desirable, Microsec will provide a 30-day review period to all current subscribers to which certificates have been issued and which have not expired or been revoked.

1.5.2. Updates of CPSs of CAs listed in the CTL

(30) Each Root CA listed in the CTL of an SCMS Manager shall publish its own CPS, which must follow the CP of the SCMS Manager. A Root CA may add additional requirements but shall ensure that all requirements of the applicable CPs are always met.

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

(32) The change process shall ensure that all changes to the 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.

(33) 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. The SCMS Providers shall send the amended CPS (with the modified version of the applicable CPs) to their subscribers for information at least 30 days before the amended CPS comes into effect.

(34) The Root CA shall notify the SCMS Manager 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.

(35) The Root CA shall notify and send its CPS to its accredited auditor if any significant change has been made to the CPS.

1.5.3. CPS approval procedures for Root CA inclusion into a CTL

(36) 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 the CPS to an accredited auditor as part of the compliance audit.

(37) Based on the audit results of Root CA/Elector, the SCMS Manager Organization's CTL Committee can decide about the addition of Root CA/Elector to the CTL.

1.6. Definitions and acronyms

(38) The definitions and acronyms of IEEE 1609.2.1 [1] (sections 3.1 and 3.2) apply.

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.

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.

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

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

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

Acronym or abbreviation	Meaning
ACPC	Activation Codes for Pseudonym Certificates
ACA	authorization certificate authority
AES	Advanced Encryption Standard
APDU	application protocol data unit
API	application programming interface
APrV	Activation Codes for Pseudonym Certificates (ACPC) private activation value
APuV	Activation Codes for Pseudonym Certificates (ACPC) public activation value
ASD	aftermarket safety device
AT	access token
CA	certificate authority
CAM	certificate access manager

Acronym or abbreviation	Meaning
CAMP	Crash Avoidance Metrics Partners LLC
CAL	certificate access list
CCF	certificate chain file
CCG	client credentials grant
C-OER	canonical octet encoding rules
CRACA	certificate revocation authorizing certificate authority
CRL	certificate revocation list
CTL	certificate trust list
DC	distribution center
DCM	device configuration manager
DER	distinguished encoding rules
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
ECA	enrollment certificate authority
ECC	elliptic curve cryptography
EE	end entity
HTTP	Hypertext Transfer Protocol
I2V	infrastructure to vehicle
IETF	Internet Engineering Task Force
IP	Internet Protocol
ITS	intelligent transportation systems
JSON	JavaScript Object Notation
JWKS	JavaScript Object Notation (JSON) web key set
JWT	JavaScript Object Notation (JSON) web token

Acronym or abbreviation	Meaning
LA	linkage authority
LOP	location obscurer proxy
LV	linkage value
M2M	machine to machine
NAT	Network Address Translation
OAS	OAuth authorization server
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
PKI	public key infrastructure
PLV	prelinkage value
PSID	Provider Service Identifier
RA	registration authority
REST	representational state transfer
RFC	Request for Comments
RSU	roadside unit
SAS	Supplementary Authorization Server
SCMS	Security Credential Management System
SPDU	secured protocol data unit
SSME	security services management entity

Acronym or abbreviation	Meaning
SSP	service specific permissions
TLS	Transport Layer Security
URL	uniform resource locator
USDOT	United States Department of Transportation
UTC	Coordinated Universal Time
V2I	vehicle to infrastructure
V2V	vehicle to vehicle
V2X	vehicle to everything
WAVE	Wireless Access in Vehicular Environments
WSA	Wireless Access in Vehicular Environments (WAVE) Service Advertisements

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. Methods for the publication of certificate information

(39) The publication methods described in Section 2.5 of the present CP shall be supported by the respective entities.

2.2. Time or frequency of publication

(40) The SCMS Manager shall publish its CTL within 15 days after the addition of a new entry. In the case of removal of an entry, a new CTL shall be published in 24 hours.

a) The SCMS Manager shall publish its CP within 15 days after the accepted modification.

b) The SCMS Manager shall publish the new Elector certificates when they start their operation.

(41) SCMS Providers shall publish their newly issued CA certificates, associated CRLs and CTLs via a publicly accessible DC and/or RA when they start their operation. The latest CTL and certificate chain file (CCF) shall always be publicly available.

a) SCMS Providers shall publish their CPS within 15 days after any approved modification.

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

2.3. Repositories

(43) The SCMS Manager shall operate a repository for its Publication Center (PUB)

(44) The SCMS Provider shall operate a repository for its Distribution Center or its RA.

2.4. Access controls on repositories

(45) The Publication Center (PUB) of the SCMS Manager shall be publicly available.

(46) The Distribution Center (DC) or the certificate information function of the RA shall be publicly available.

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

2.5. Publication of certificate information

2.5.1. Publication of information by the SCMS Manager Organization

(48) The SCMS Manager shall publish in its Publication Center (PUB) the information listed in subsection 1.3.2.2 of this CP.

2.5.2. Publication of information by an SCMS Provider

(49) Every SCMS Provider shall publish either in its Distribution Center (DC) or in the RA the information listed in subsection 1.3.4.6 of this CP.

2.5.3. Publication of Information by a RA

(50) The RA shall publish the information listed in subsection 1.3.4.6 of this CP.

3. IDENTIFICATION AND AUTHENTICATION

3.1. Naming

(51) Void

(52) The SCMS Manager, at its sole discretion, may refuse to issue a Certificate with a subject name not meeting these requirements.

3.1.1. Types of names

3.1.1.1. Names for Electors and Root CAs

(53) The Elector and Root CA certificate shall contain a single and unique UTF8String value based on their request and approved by the SCMS Manager as a *CertificateId* attribute of type *name* in accordance with IEEE 1609.2.1 [1]. The SCMS Manager is responsible for the uniqueness of names within its system.

(54) The host function identifier should be *elector* for an Elector and *rootca* for a Root CA.

(55) If a Root CA follows the X.509 structure, it should use conventional subject names.

3.1.1.2. Names for ICA

(56) 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 [1].

(57) The host function identifier should be *ica* for an ICA.

3.1.1.3. Names for ACA

(58) The ACA certificate shall contain a single and unique value allocated by the SCMS Provider's issuing ICA as *CertificateId* attribute of type *name* in accordance with IEEE 1609.2.1 [1].

(59) The host function identifier should be *aca* for an ACA.

3.1.1.4. Names for ECA

(60) The ECA certificate shall contain a single and unique value allocated by the SCMS Provider's issuing ICA as *CertificateId* attribute of type *name* in accordance with IEEE 1609.2.1 [1].

(61) The ECA shall have an identifying URL as defined in IEEE 1609.2.1 [1]. The *Id* field should be equal to the identifying URL.

(62) The host function identifier should be *eca* for an ECA.

3.1.1.5. Names for RA

(63) The RA certificate shall contain a single and unique value allocated by the SCMS Provider as *CertificateId* attribute of type *name* in accordance with IEEE 1609.2.1 [1].

(64) The RA shall have an identifying URL as defined in IEEE 1609.2.1 [1]. The *Id* field should be equal to the identifying URL.

3.1.1.6. Names for DC

(65) Void.

(66) The DC shall have an identifying URL as defined in IEEE 1609.2.1 [1].

3.1.1.7. Names for MA and LA

(67) The host function identifiers should be *ma* for a MA.

3.1.1.8. Names for end entity certificates

(68) The enrollment certificates of end entities may contain a single *CertificateId* attribute in accordance with IEEE 1609.2.1 [1]. The ECA is responsible for the uniqueness of these *Id*s.

(69) The authorization shall be direct: a unique identifier, known as the canonical identifier, 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 [1].

(70) The authorization certificates of end entities, in accordance with IEEE 1609.2.1 [1], may contain a single *CertificateId* attribute of type *linkageData* for Linkage-based certificate identifiers and *binaryId*, or none for Hash ID-based certificate identifiers.

3.1.1.9. Identification of certificates

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

3.1.2. Need for names to be meaningful

(72) All hostnames and subject names shall be meaningful.

3.1.3. Anonymity and pseudonymity of end-entities

(73) A pseudonym authorization certificate shall not contain any name or information that links the subject to its real identity. The ACA and the RA are responsible for ensuring that this requirement is met.

3.1.4. Rules for interpreting various name forms

No stipulation.

3.1.5. Uniqueness of names

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

(75) The canonical IDs for end entities shall be unique within the SCMS Provider's system.

(76) Each Root CA proposes its name to the SCMS Manager.

(77) The SCMS Manager shall ensure that a Root CA's 3-byte hash certificate identifier (*HashedId3*) is unique in the scope of the overall trust model.

(78) The SCMS manager shall maintain the registry of Root CA names upon notification of approval, revocation, removal of a Root CA.

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

(80) Subject name CertificateIDs in certificates shall be limited to 32 bytes.

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

3.2. Initial identity validation

3.2.1. Method to prove possession of private key

(82) The participant shall prove that it holds the private key corresponding to the public key included in its certificate by submitting a self-signed Certificate Signing Request (CSR) and this proof shall be verified by the relevant entity. Table 1 shows which actor is relevant for checking the key ownership of each actor.

Key owner	**The actor responsible for the verification**	**Comments**
Elector	SCMS Manager	self-signed IEEE 1609.2 certificate
Root CA	SCMS Manager	self-signed IEEE 1609.2 certificate
ICA	Root CA	-
ECA	ICA	-
ACA	ICA	-
RA	ICA	-
MA	ICA	-
CRL Signer	corresponding CA	-

Table 1: Key ownership verification

3.2.2. Authentication of organization identity

3.2.2.1. Authentication of Elector organization identity

(83) The Elector shall provide the SCMS Manager with evidence of the identification and accuracy of the name and associated data. The SCMS manager shall validate this evidence.

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

(85) The organization evidence provided shall be the same as for Root CAs, as specified in Section 3.2.2.2 of the present Policy.

3.2.2.2. Authentication of Root CAs' organization identity

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

(a) The name of the Root CA organization,

(b) The postal address of the Root CA organization,

(c) The e-mail address of the Root CA organization,

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

(e) The telephone number of the Root CA organization,

(f) The digital fingerprint (i.e., SHA-256 hash value) of the Root CA's certificate,

(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 its subordinate CAs.

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

(88) The SCMS Manager shall collect either direct evidence, or an attestation from an appropriate and authorized source (e.g., company registration document), of the organizational identity (e.g., name) and, if applicable, any specific attributes of subjects whose RCA is to be added to the CTL. Submitted evidence may be in paper or electronic form.

(89) Void

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

(a) the full name of the organizational entity,

(b) the nationally recognized registration number or other attributes of the organizational entity that can be used to distinguish the organizational entity from others with the same name.

3.2.2.3. Authentication of Sub CAs organization identity

(91) The Root CA shall check the identity of the organization (name, address, and documentation of their status as a legal entity) and other registration information provided by certificate applicants for ICA certificates.

(92) The ICA shall check the identity of the organization (name, address, and documentation of their status as a legal entity) and other registration information provided by certificate applicants for ACA, ECA, LA, MA, RA certificates.

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

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

- determine that the organization exists by using at least one third-party identity proofing service or database or, alternatively, organizational documentation issued or filled out by the relevant government agency or recognized authority that confirms the existence of the organization,
- Void

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

3.2.2.4. Authentication of End-Entities' subscriber organization

(96) Before the subscriber (manufacturer or operator) of end-entities can register with a trusted ECA to enable its end-entities for sending EC certificate requests, the ECA shall:

- check the identity of the subscriber organization and other registration information provided by the certificate applicant,
- check that the EE type (i.e. the concrete product based on brand, model and version of the EE) meets all of the following compliance assessment criteria:
    - Certificate of conformance with the relevant SCMS Manager Organization's relevant CP requirements on device certification and cryptographic module certification if applicable.
    - Declaration of full conformity with all relevant standards for interoperability based on a list of interoperability requirements from relevant profiles.

      Generally, if the SCMS Manager has defined no specific certification criteria, conformity with C2C-CC BSP 1.6 [2][1] or newer, or C-ROADS Release 2.0 [3][2] or newer are acceptable.

(97) At a minimum, the ECA shall:

[1] https://www.car-2-car.org/documents/basic-system-profile
[2] https://www.c-roads.eu/platform/about/news/News/entry/show/release-20-of-c-roads-harmonised-c-its-specifications.html

- determine that the organization exists by using at least one third-party identity proofing service or database or, alternatively, organizational documentation issued or filled out by the relevant government agency or recognized authority that confirms the existence of the organization,
- 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.

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

3.2.3. Authentication of individual entities

(99) 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/Sub-CA/other SCMS model elements individual entity

(100) For the authentication of an individual entity (physical person) identified in association with a legal person or other organizational entity, evidence shall be provided of:

- The full name of the individual entity (including surname and given name(s), in line with the applicable law and national identification practices),
- Date and place of birth, reference to a nationally recognized identity document or other attributes of the individual entity that may be used, as far as possible, to distinguish the person from others with the same name,
- Full name and legal status of the associated legal person or other organizational entity,
- Any relevant registration information of the associated legal person or other organizational entity,
- Evidence that the individual entity is associated with the legal person or other organizational entity.

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

(101) To verify their identity, the authorized representative of the respective SCMS model element shall provide documentation proving that the authorized individuals work for the organization (certificate of authorization). The authentication of the individual entity shall be based on his/her nationally recognized identity document (official ID).

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

(103) The personnel at the Root CA / ICA shall verify the identity of the certificate applicant representative and all associated documents.

3.2.3.2. Authentication of End Entities' subscriber identity

(104) 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 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 End Entities' identity

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

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

(107) EE subjects of authorization certificates shall authenticate themselves when requesting authorization certificates by using their unique enrollment certificate or X.509 certificate.

3.2.4. Non-verified subscriber information

No stipulation.

3.2.5. Validation of authority and End Entity

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

(108) 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

(109) At least one representative role (device operator/operator manager) responsible for the registration (requests) of End Entities shall be known to and approved by the Enrollment CA.

3.2.5.3. Validation of End Entities

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

3.2.6. Criteria for interoperation

(111) For communication between EEs and SCMS model element interfaces defined by the IEEE 1609.2.1 [1] shall be implemented.

(112) The ECA, RA and ACA shall support certificate requests and responses that comply with IEEE 1609.2.1 [1].

3.3. Identification and authentication for re-key requests

3.3.1. Identification and authentication for standard re-key requests

3.3.1.1. Elector certificates

Not applicable.

3.3.1.2. Root CA certificates

Not applicable.

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

(113) Void.

(114) Void.

3.3.1.4. End-Entities' enrolment credentials

(115) 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.

(116) 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 with the current valid private key (outer signature) and encrypt the request to the receiving RA or ECA as specified in IEEE 1609.2.1 [1], to ensure its confidentiality, integrity and authenticity.

3.3.1.5. End-Entities' authorization certificates

(117) 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

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

3.3.2.2. End-entity certificates

(119) The authentication of an end entity for enrollment or authorization certificate re-key after revocation shall be handled in the same way as the initial issuance of that certificate.

3.4. Identification and authentication for revocation request

(120) Requests to remove an Elector or Root CA from the CTL shall be authenticated by the Elector or Root CA to the SCMS Manager.

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

(122) Requests to revoke an EE enrollment certificate may originate from the EE subscriber or the MA. Both shall authenticate themselves.

(123) Requests to revoke an EE authorization certificate may originate from the EE subscriber or the MA. Both shall authenticate themselves.

(124) The procedure for authenticating revocation requests shall guarantee proper identification of the responsible party of the Subscriber. The procedure shall be described in the CPS of the SCMS Provider.

(125) The SCMS Provider contact information shall be listed in the Certificate Practice Statement (CPS).

(126) In case of CA revocation requests, the SCMS Provider shall confirm the written request details with at least one of the Authorized Individuals and the senior executive prior to acting on the revocation request.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. Certificate application

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

(a) Registration and setup of a trust relation between the Electors and the SCMS Manager including the insertion of an Elector certificate to 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 to 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, DC and the ICA, including the issuance of a new certificate for ECA, RA, ACA, LA, MA, 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.

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

(129) The SCMS Provider may refuse to issue a certificate at its sole discretion.

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 the SCMS Manager.

4.1.1.2. Root CA

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

4.1.1.3. ICA

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

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

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

4.1.1.5. CRL Signer

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

4.1.1.6. End Entity

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

(136) Each EE registered at the ECA or X.509 CA shall send enrollment certificate requests according to IEEE 1609.2.1 [1].

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

4.1.2. Enrolment process and responsibilities

(138) Permissions in Root CAs and Subordinate CAs for special (governmental) purposes (i.e. special mobile or fixed EEs) where restricted by law may be used in EE certificates only if the relevant authority having jurisdiction granted by legislation authorizes the requested credentials.

4.1.2.1. Electors

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

(140) The Elector's enrollment process is based on a signed application that shall be securely delivered to the 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 the SCMS Manager. In case of approval, the SCMS Manager generates and sends a certificate of conformity to the corresponding Elector.

(143) The Elector addition to the CTL is an SCMS Manager-defined internal process.

4.1.2.2. Root CAs

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

(145) The Root CA shall provide the following information to the SCMS Manager when applying for CTL insertion:

- Its corresponding CP and CPS,
- The name of the HSM used for key generation and storage and a link to the NIST FIPS 140 [4] certification,

- Evidence of TISAX or ISO 27001 [5] certification (document or appropriate web link),
- Evidence of WebTrust for CAs [6] certification (link to Provider's web page where the WebTrust [6] certification logo provided by the auditor upon completion of the audit, has been displayed).

(146) The enrollment process is based on a signed application that shall be securely delivered to the SCMS Manager.

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

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

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

(150) After being approved by the SCMS Manager, the Root CA shall deliver the technical information as required by IEEE 1609.2.1 [1] (CCF, RCA, etc.)

4.1.2.3. *ICA*

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

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

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

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

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

4.1.2.5. End entity

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

(156) The EE subscriber can use multiple methods of authorization described in Section 1.3.4.3

(157) The EE shall generate enrollment certificate key pairs and enrollment certificate requests in accordance with IEEE 1609.2.1 [1].

(158) During the enrollment of a normal EE (as opposed to a special mobile or fixed EE), the Enrollment CA shall verify that the permissions in the initial request are not for governmental use. Permissions for governmental use are defined by the corresponding governmental entity. The detailed procedure for EE subscriber

registration at the Enrollment CA shall be set out in the corresponding CPS of the ECA.

(159) Regular EEs should be enrolled at a single Enrollment CA and therefore bound to a single RA for all of their certificates with a particular set of permissions. Special-purpose vehicles (e.g., police cars) may be enrolled at an additional Enrollment CA 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 Sub-CAs issuing certificates for such special-purpose EEs shall determine how the enrollment process applies to such EEs.

(160) If the EE is in the process of migrating from one Enrollment CA to another Enrollment CA, the EE may be enrolled at two Enrollment CAs.

4.2. Certificate application processing

4.2.1. Performing identification and authentication functions

(161) The Certificate application process shall provide sufficient information to:

- Establish the applicant's Authorized Individual authorization to obtain a Certificate per the "Identification and Authentication" section of the present document.
- Establish and record the applicant’s Authorized Individual identity as per the "Identification and Authentication" section of the present document.
- Obtain the Subscriber’s public key and verify the Subscriber’s possession of the private key for each Certificate request per the "Method to Prove Possession of Private Key" section of the present document.
- Verify any role or authorization information requested for inclusion in the Certificate as well as any other information in certificate applications.

(162) The above steps shall be completed before certificate issuance.

(163) Only Subscribers’ Authorized Individuals may submit a certificate application.

4.2.1.1. Identification and authentication of Electors / Root CAs

(164) The SCMS Manager is responsible for authenticating the Elector’s /Root CA’s authorized representative and approving its application. The application approval shall be done by the CTL Committee.

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

4.2.1.2. Identification and authentication of the ICA

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

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

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

(168) The corresponding ICA is responsible for authenticating its subordinate CAs' or other SCMS elements' authorized representative and approving its application.

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

4.2.1.4. Identification and authentication of CRL signer

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

(171) 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

(172) 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.

(173) 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

(174) During enrollment certificate requests, in accordance with IEEE 1609.2.1 [1], the ECA shall use at least one of the authentication options mentioned in Section 1.3.4.3

(175) During successor enrollment certificate requests and successor enrollment certificate downloads, in accordance with IEEE 1609.2.1 [1], the RA shall use at least one of the authentication options for both EE and RA mentioned in Section 1.3.4.3

(176) During authorization certificate requests and authorization certificate downloads, in accordance with IEEE 1609.2.1 [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.

(177) During misbehavior report submission, in accordance with IEEE 1609.2.1 [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

(178) Providers shall reject any application for which validation and authentication cannot be completed, or when the Provider has cause to lack confidence in the application or certification process, or if the IEEE 1609.2 or X.509 Certificate fields as profiled by SCMS Manager, are inappropriately configured in the CSR.

4.2.2.1. Approval or rejection of Elector/Root CA certificates

(179) The SCMS Manager 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 compliant with its CP.

4.2.2.2. Approval or rejection of ICA certificates

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

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

(181) The ICA shall verify the Sub CA's, or other SCMS element's certificate request based on their audit results. If this verification leads to a positive result, the ICA may issue a certificate to the requesting entity.

4.2.2.4. Approval or rejection of CRL Signer certificates

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

4.2.2.5. Approval or rejection of enrollment certificate

(183) 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

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

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

(a) A current, valid and relevant CRL and CTL are available at the RA / DC,
(b) The Root CA certificate and ICA certificate of the CA's certificate chain were not revoked,
(c) The Root CA certificate is listed on the current, valid and relevant CTL.

4.2.3. Time to process the certificate application

4.2.3.1. ELECTOR, ROOT CA certificate application

(186) The time to process the identification and authentication process of an Elector/Root CA certificate application is defined in the SCMS Manager's CP.

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

(187) The time to process the identification and authentication process of a certificate application shall be 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. This maximum timeframe shall be defined in the CPS, though it shall be no longer than 10 business days. Enrollment certificate application

(188) The processing of enrollment certificate applications shall be subject to a maximum time limit laid down in the ECA's CPS. This shall not be - in normal condition - more than 5 days.

4.2.3.3. Authorization certificate application

(189) The processing of authorization certificate applications shall be subject to a maximum time limit laid down in the RA's and ACA's CPS. This shall not be - in normal conditions - more than 15 minutes.

4.3. Certificate issuance

4.3.1. CA actions during certificate issuance

4.3.1.1. Elector certificate issuance

(190) The Elector shall issue its own self-signed Elector certificate in the IEEE 1609.2.1 [1] format and shall send it to the SCMS Manager.

(191) The SCMS Manager shall take care that the Elector certificate is made available as soon as possible via the publication center (PUB).

(192) Electors shall sign the to be signed CTL prepared by the SCMS Manager.

4.3.1.2. Root CA certificate issuance

(193) The Root CA shall issue its own self-signed Root CA certificate in the IEEE 1609.2.1 [1] format and may send it to the SCMS Manager for publication on the CTL.

(194) The SCMS Manager shall check the audit results and the CPS of the Root CA before including the Root CA on the CTL.

(195) The SCMS Manager shall take care that the Root CA certificate is made available as soon as possible via CTL at PUB, cf. Section 2.5.1.

4.3.1.3. ICA certificate issuance

(196) The Root CA shall issue ICA certificates in the IEEE 1609.2.1 [1] format.

(197) The Root CA shall check the audit results of the ICA, before issuing the ICA certificate.

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

4.3.1.4. CRL Signer certificate issuance

(199) The CRACA may issue CRL Signer certificates in the IEEE 1609.2.1 [1] format.

(200) The CRACA shall check the audit results of the CRL Signer, before issuing its certificate.

(201) The CRACA shall take care that the relevant CRL Signer certificates are made available via the RA or DC.

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

(202) The ICA shall issue ECA, RA, ACA, LA, MA, DC certificates in the IEEE 1609.2.1 [1] format.

(203) The ICA shall check the audit results of the ECA, RA, ACA, LA, MA, before issuing their certificate.

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

4.3.1.6. Enrollment certificate issuance

(205) The Enrollment CA shall issue enrollment certificates in the IEEE 1609.2.1 [1] format, or in the X.509 format following RFC 5280 [12] and RFC 5480 [13].

(206) 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, otherwise it shall reject the certificate request.

(207) Enrollment certificate requests and responses shall be encrypted to ensure confidentiality and signed to ensure authenticity and integrity.

4.3.1.7. Authorization certificate issuance

(208) The ACA shall issue authorization certificates in the IEEE 1609.2.1 [1] format.

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

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

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

Not applicable.

4.4. Certificate acceptance

4.4.1. Conducting certificate acceptance

4.4.1.1. Elector

Not applicable.

4.4.1.2. Root CA

Not applicable.

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

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

(212) The Subscriber shall confirm to the Provider that it has received and validated the certificate. Failure by the Subscriber to acknowledge the correctness of the certificate within three (3) business days of issuance may result in the Provider revoking the certificate.

4.4.1.4. End entity

(213) The end entity shall verify the received enrollment certificates and authorization certificates against the original requests, including the signature and the certificate chain. It shall discard all enrollment certificate or authorization certificate 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

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

(215) Sub CA or other SCMS model element certificates shall be published by the respective publication mechanism (i.e., DC or RA).

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

(217) The ICA, ACA, and CRL Signer certificates may be published by the end entity via P2PCD according to IEEE 1609.2.1 [1].

4.4.3. Notification of certificate issuance

(218) The respective provider shall notify the Subscriber within the certificate application processing window of Certificate issuance and may use any reliable mechanism to deliver the Certificate to the Subscriber.

4.5. Key pair and certificate usage

4.5.1. Private key and certificate usage

(219) All Providers shall protect their respective private keys associated with their respective public keys in their Certificates from unauthorized use or disclosure and use reasonable means to prevent any such unauthorized use and disclosure, as specified in this document and the Subscriber Agreement documentation. Should there be a conflict in these referenced documents, the Subscriber Agreement shall prevail.

(220) Relying Party software shall be compliant with IEEE 1609.2 [7] as profiled per SCMS Manager, ICAB, or X.509 and ISO 15118, and/or PA approved documentation and standards. Verifying the validity of issued Certificates is solely the responsibility of the Relying Parties.

4.5.1.1. Private key and certificate usage for Elector

(221) Electors shall use their private keys to sign their own (Elector) certificates and the CTL.

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

4.5.1.2. Private key and certificate usage for Root CA

(223) Root CAs shall use their private keys to sign their own (Root CA) certificates, CRLs, and Sub CA certificates.

(224) The Root CA certificate shall be used by the PKI participants to verify the CRL and the Sub CA certificates.

4.5.1.3. Private key and certificate usage for ICA

(225) ICAs shall use their private keys to sign their own certificate requests and the certificates for ECA, RA, ACA, LA, MA, DC, as well as to sign CRLs.

(226) The ICA certificates shall be used by the PKI participants to verify certificates and CRLs where the ICA is the issuer.

4.5.1.4. Private key and certificate usage for ECA

(227) ECAs shall use their private keys to sign their own certificate requests and enrollment certificates.

(228) According to IEEE 1609.2.1 [1], the ECA can use an X.509 certificate for authentication in session-based communications.

(229) ECA certificates shall be used by the PKI participants to verify enrollment certificates and signed PDUs from the ECA.

4.5.1.5. Private key and certificate usage for RA

(230) RAs shall use their private keys to sign their own certificate requests and decrypt PDUs. This certificate may be used by the RA to authenticate itself in communication with other SCMS model elements and end entities.

(231) RA certificates shall be used by the PKI participants to encrypt PDUs for the RA.

4.5.1.6. Private key and certificate usage for ACA

(232) ACAs shall use their private keys to sign their own certificate requests, authorization certificates, CRL Signer certificates and CRLs.

(233) ACA certificates shall be used by the PKI participants to verify authorization certificates, CRL Signer certificates and CRLs where the ACA is the issuer.

4.5.1.7. Private key and certificate usage for LA

(234) LAs shall use their private keys to sign their own certificate requests.

(235) LA certificates may be used by PKI participants to authenticate the LA.

4.5.1.8. Private key and certificate usage for MA

(236) MAs shall use their private keys to sign their own certificate requests and decrypt misbehavior reports.

(237) MA certificates may also be used by PKI participants to authenticate the MA in communication.

4.5.1.9. Private key and certificate usage for CRACA and CRL Signer

(238) CRACAs and CRL Signers shall use their private keys to sign their own certificate requests and CRLs.

(239) CRACA and CRL Signer certificates shall be used by PKI participants to verify their CRLs.

4.5.1.10. Private key and certificate usage for End Entity

(240) If direct authorization is used for initial EE enrollment, the EE shall use its canonical private key to sign initial enrollment certificate requests as defined in IEEE 1609.2.1 [1].

(241) End entities shall use their private keys to sign successor enrollment certificate requests and authorization certificate requests.

(242) 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.

(243) 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.

(244) The end entity shall use its authorization certificate's private key to sign messages as defined in IEEE 1609.2 [7] and IEEE 1609.2.1 [1].

4.5.2. Relying party public key and certificate usage

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

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

4.6. Certificate renewal

Not allowed.

4.7. Certificate re-key

4.7.1. Circumstances for certificate re-key

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

(248) Subscribers requesting re-key of Certificates shall identify and authenticate themselves for the purpose of re-keying as described in the "Initial Identity Validation" section of the present Policy, and the re-key request shall include a new CSR containing a new public key.

(249) Entities shall not reuse their previous key pairs.

(250) SCMS Providers shall validate the re-key request information prior to issuing a new Certificate. This validation will include a check with at least one of the Authorized Individuals acting on the Subscriber's behalf. SCMS Providers shall issue a Certificate for a valid re-key request. SCMS Providers shall notify the Authorized Individuals of the Subscriber, and it may use any reliable mechanism to deliver the Certificate to the Subscriber.

(251) After re-keying a client Certificate, SCMS Providers will revoke the old Certificate unless requested by the Subscriber to not revoke the old Certificate for a specific time period in order to accommodate the Subscriber's shift to the new Certificate. In any event, SCMS Providers shall not further re-key, renew, or modify the old Certificate.

4.7.2. Who may request re-key

4.7.2.1. Elector and Root CA

(252) Electors and Root CAs do not request re-key. The re-keying process is an internal process for the Elector and Root CA, because their certificates are self-signed.

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

(253) 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.

(254) The Sub CA's or other SCMS element's certificate re-keying request shall be submitted in due time 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

(255) The end entity shall re-key its enrollment certificate according to IEEE 1609.2.1 [1].

4.7.3. Re-keying process

4.7.3.1. Elector and Root CA

Not applicable.

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

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

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

4.7.3.3. End Entity certificates

(257) The end entity shall re-key its enrollment certificate according to IEEE 1609.2.1 [1].

4.8. Certificate modification

Not allowed.

4.9. Certificate revocation and suspension

(258) SCMS elements shall issue CRLs covering all revoked but unexpired Certificates.

(259) SCMS elements shall make public a description of how to obtain revocation information for the Certificates they publish and an explanation of the consequences of using outdated revocation information. This information shall be given to Subscribers during certificate request or issuance and shall be readily available to any potential relying party.

(260) Certificate suspension is not supported. The SCMS Provider may block the EC of an EE in special cases (i.e., misbehavior, fee debt).

4.9.1. Circumstances for revocation

(261) Certificate revocation may be performed in the following circumstances:

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

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

(c) If the conformance audit described in Section 8 leads to a negative result,

(d) If the Sub CA or end entity is no longer associated with the EE subscriber or the organization managing the Sub CA,

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

(f) If the subscriber agreement has been terminated,

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

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

(262) Whenever a decision is reached to proceed with a revocation, the associated Certificate shall be revoked and placed on the CRL. Revoked Certificates shall be included on all new publications of the certificate status information until the Certificates expire.

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

4.9.2. Who can request revocation

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

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

(266) The Sub CA representative may request the revocation of its own Sub CA certificates.

(267) The issuing CA may trigger the revocation of the certificates issued by itself.

(268) The EE subscriber representative may request the revocation of certificates requested by itself.

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

(270) SCMS Providers shall accept revocation requests from authenticated and authorized parties, such as the Subscriber or an authorized US-DOT representative.

(271) SCMS Providers 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 (3) day notice to Subscriber, unless a shorter time period is necessary due to criticality.

4.9.3. Procedure for revocation request

(272) Entities submitting Certificate revocation requests shall list their identity and explain the reason for requesting revocation.

(273) SCMS Providers shall revoke a Certificate if the request is authenticated as originating from the Subscriber for its Certificate or for Certificates under its purview. If the revocation is requested by someone other than an authorized representative of the Subscriber or Affiliated Organization, SCMS Providers shall investigate the alleged basis for the revocation request. SCMS Providers shall maintain a 24/7 support contact mechanism to capture any reporting of a Certificate problem. SCMS Providers shall respond within the time period as specified in their CPS. If appropriate, SCMS Providers may forward complaints to law enforcement. The Providers shall list revoked Certificates in their CRL where the Certificates will remain listed until the end of their validity period.

4.9.3.1. Removal of an Elector

(274) Electors shall be removable from the CTL. In case of an Elector removal, the SCMS Manager shall publish a new CTL as soon as possible, without undue delay.

(275) The removal of Electors from the CTL is the responsibility of the SCMS Manager, as defined by its internal processes. Anyone can request the revocation of a certificate in the event of key compromise if they can prove it. It must be ensured that only requests that are justified and verified by the SCMS Manager result in the removal of the certificate.

(276) Electors shall immediately notify the SCMS Manager of a known or suspected compromise of their private key. It must be assured that only proven requests result in the removal of certificate.

4.9.3.2. Removal of a Root CA

(277) Root CAs shall be removable from the CTL. In case of a removal, the SCMS Manager shall publish a new CTL as soon as possible, without undue delay.

(278) The removal of a Root CA from the CTL is the responsibility of the SCMS Manager, as defined by its internal processes. Anyone can request the revocation of a certificate in the event of key compromise if they can prove it. It must be ensured that only requests that are justified and verified by the SCMS Manager result in the removal of the certificate.

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

4.9.3.3. Revocation of ICA, ECA, RA, ACA, LA, MA, CRL Signer certificates

(280) ICA, ECA, RA, ACA, LA, MA and CRL Signer certificates 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 private key, this revocation shall be done without undue delay. Revoked certificates shall be published on a CRL within 48 hours.

(281) The CRACA or CRL Signer shall update, sign and publish the CRL within 48 hours to the DC.

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

4.9.3.4. Revocation of enrollment certificates

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

(284) 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 blocking/revocation shall be done as soon as possible.

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

4.9.3.5. Revocation of authorization certificates

(286) 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 [1] in the following cases:

(a) In case the EE subscriber requests the revocation,

(b) In case of EE subscriber termination,

(c) In case the MA has requested it,

(d) In case a court decision orders to do so.

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

(287) 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

(288) The MA shall enforce established and published SCMS Manager specifications regarding misbehavior reports and processing.

(289) The 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 that has issued the MA is listed.

4.10. Certificate status services

(290) SCMS Providers shall publish CRLs within one business day of any change (update) and prior to the expiry of the current CRL. Furthermore, each CRL shall be published no later than the time specified in the "nextUpdate" field of the previously issued CRL for same scope.

(291) A new CTL shall only be issued in response to a request received from SCMS Manager EAC to add or remove a Root CA or Elector from the SCMS Manager-approved ecosystem. A new CTL issued to add a Root CA shall be published within three business days.

(292) When using TLS, SCMS Providers should also support validation using the Online Certificate Status Protocol (OCSP).

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.

5. FACILITY, MANAGEMENT AND OPERATIONAL CONTROLS

(293) The SCMS ecosystem is composed of Electors, Root CA, ICA, ECA, RA, ACA, LA, MA, CRL Signer, DC (including their ICT components e.g., networks and servers).

(294) 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 …'.

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

5.1. Physical controls

(296) All SCMS model element operations shall be conducted in a physically protected environment that 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 [5] or TISAX.

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

(298) 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

(299) The location and construction of the facility housing the Elector or Root CA equipment and data (HSM, activation data, backup of key pair, computer, log, etc.) shall be consistent with facilities used to house high-value and sensitive information. Root CAs shall be operated offline and shall be separated from other PKI components.

(300) 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, to guarantee that:

- The environment is isolated from public networks,
- 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.
- 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 mechanisms.

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

- Perimeter alarms, closed-circuit television, reinforced walls and motion detectors,
- 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.

(302) Electors and Root CAs shall use authorized personnel to monitor the facility housing equipment. The personnel of the operational environment shall only be granted access to the secure areas of a Root CA if they are specifically authorized.

5.1.1.2. Sub-CAs and other SCMS model elements

(303) 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, etc.) shall be consistent with facilities used to house high-value and sensitive information. These entities may be hosted in a secure cloud environment based on risk analysis.

(304) 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 mechanisms.

(305) 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.

(306) Sub CAs and other SCMS model elements shall use authorized personnel to monitor the facility housing equipment. The personnel of the operational environment shall only be granted access to the secure areas of a CA if they are specifically authorized.

5.1.2. Physical access

5.1.2.1. Elector, Root CA

(307) Root CA and Elector equipment and data (HSM, activation data, backup of key pair, computer, log, etc.) shall always be protected from unauthorized access. The physical security mechanisms for equipment shall at least:

- Monitor, either manually or electronically for unauthorized intrusion at all times,
- Ensure that no unauthorized access to the hardware and activation data is permitted,
- Ensure that all removable media and paper containing sensitive plain-text information are stored in a secure container,
- 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,
- Ensure that an access log is maintained and inspected periodically,
- Provide at least two layers of progressively increasing security, e.g., at perimeter, building and operational room level,
- Require two trusted-role physical access controls for the HSM and activation data.

(308) 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:

- The equipment is in a state that is appropriate for the current mode of operation,
- For offline components, all equipment is shut down,
- Any security containers (tamper-proof envelope, safe, etc.) are properly secured,
- Physical security systems (e.g. door locks, vent covers, electricity) are functioning properly,
- The area is secured against unauthorized access.

(309) 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, to avoid only one person having access to the private key.

(310) 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 sign 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

(311) Sub CAs and other SCMS model elements may be operated in secure cloud environments based on risk analysis and with certified HSM.

5.1.3. Power and air conditioning

(312) 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 equipment in the event of a lack of power. 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

(313) 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

(314) To prevent damaging exposure to flame or smoke, the secure facilities of 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

(315) 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.

(316) Media used in the SCMS model elements shall be 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 shall be retained.

(317) 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.

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

5.1.7. Waste disposal

(319) 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

(320) Backups of SCMS model elements, sufficient to recover from system failure, shall be made offline after the SCMS model element's 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.

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

(322) The private key material of the 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

5.2.1. Trusted roles

(323) Employees, contractors and consultants (if any) 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.

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

- The validation of information in certificate applications,
- The acceptance, rejection or other processing of certificate applications, revocation requests or renewal requests,
- The issuance or revocation of certificates, including personnel having access to restricted portions of its repository or the handling of subscriber information or requests.

(325) Trusted roles shall include roles that involve the following responsibilities:

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

(b) System Administrators: Authorized to install, configure and maintain the TSP's trustworthy systems for service management.

(c) System Operators: Responsible for operating the TSP'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.

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

5.2.2. Number of persons required per task

(327) 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.

(328) 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.

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

5.2.3. Identification and authentication for each role

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

(331) 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.

(332) The CPS of the trust model element shall describe the mechanisms used to identify and authenticate individuals.

5.2.4. Roles requiring separation of duties

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

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

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

(334) 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.

(335) 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. Each SCMS Provider shall have its own senior executives, senior staff and staff in trusted roles.

(336) The SCMS Provider that serve mobile EEs should separate logically and on the level of trusted roles the ACA from ECA and RA. These entities should not exchange any data which breaks the pseudonymity. Other protocols may be used, provided that IEEE 1609.2.1 [1] is implemented.

5.3. Personnel controls

5.3.1. Qualifications, experience, and clearance requirements

(337) 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

(338) 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.

(339) 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.

(340) 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.

(341) 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

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

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

(344) 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

(345) 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.

(346) 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.

(347) 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

(348) 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

(349) 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

(350) 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.

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

5.3.8. Documentation supplied to personnel

(352) 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

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

(353) As an offline CA, event logging only occurs when a Root-CA is activated. All operator actions are logged and reviewed following each activation by a system auditor. All available logs may be subject to audit by the independent accredited PKI auditor.

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

(355) SCMS model elements shall record the following types of audit events (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 should 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 should 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) Operator registration – an event shall be created when an operator 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).

(356) 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.

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

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

(359) 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 (if applicable).

5.4.2. Frequency of processing log

(360) Audit logs shall be reviewed in response to alerts based on irregularities and incidents within the Elector/SCMS Provider systems and, in addition, periodically every year.

(361) 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 based on audit log reviews shall be documented.

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

(363) Electors shall report their activities quarterly to the SCMS Manager.

5.4.3. Retention period for audit log

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

5.4.4. Protection of audit log

(365) 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.

(366) Where applicable, audit log entries shall be signed with a secure method.

(367) Events shall be 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.

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

5.4.5. Audit log backup procedures

(369) 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.

5.4.6. Audit collection system (internal or external)

(370) 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.

(371) 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.

5.4.7. Notification to event-causing subject

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

5.4.8. Vulnerability assessment

(373) 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.

(374) 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:

- After any system or network changes determined by the SCMS model elements as significant for PKI components; and
- At least annually, 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 as significant by the SCMS model elements,

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

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

5.5. Record archiving

5.5.1. Types of record archiving

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

(a) Any accreditation of the specific Root-CA or sub-CA,

(b) CP and CPS versions,

(c) Contractual obligations and other agreements concerning the operation of the CA,

(d) System and equipment configurations, modifications, and updates,

(e) Certificate and revocation requests,

(f) Identity authentication data,

(g) Any documentation related to the receipt or acceptance of a Certificate or token,

(h) Subscriber Agreements,

(i) Certificate issuance,

(j) A record of Certificate re-keys,

(k) Other signed files such as CRLs and CTLs,

(l) Any data or applications necessary to verify an archive's contents,

(m) Compliance auditor reports,

(n) Any changes to the specific CA audit parameters,

(o) Event and audit logs, including identified attempts to delete or modify the logs,

(p) Key generation actions,

(q) Access to Private Keys for key recovery purposes,

(r) Changes to trusted Public Keys,

(s) Approval or rejection of a Certificate status change request,

(t) Appointment of an individual to a trusted role,

(u) Destruction of a cryptographic module,

(v) Certificate compromise notifications,

(w) Remedial action taken as a result of violations of physical security,

(x) Violations of the respective CP or CPS.

(376) The SCMS model element entity shall retain the above records for at least five years from their dates of origination on a secure offsite location in a manner that only authorized persons may read, modify or delete the archives.

5.5.2. Retention period for archive

(377) 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

(378) 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.

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

(380) 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

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

5.5.5. Requirements for timestamping of records

(382) 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.

(383) 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

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

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

5.6. Key changeover for trust model elements

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

(387) Sub CAs 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. Sub CAs 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

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

(389) If the personnel responsible for the management of the Root CA or Elector detect a potential hacking attempt or other form of compromise, they shall investigate in order to determine the nature and the degree of damage. In the event of the private key being compromised, the affected Root CA certificate or Elector certificate shall be removed from the CTL. The IT security experts of the SCMS Manager shall assess the scope of potential damage 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, the SCMS Manager determines which services are to be maintained and how.

(390) Incident, compromise and business continuity shall be covered in the CPS of the SCMS model element.

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

5.7.2. Corruption of computing resources, software and/or data

(392) If an incident 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.

(393) 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

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

(a) Suspend its operation,

(b) Start the disaster recovery and migration plan,

(c) Investigate the key issue that generated the compromise and notify the SCMS Manager, which will remove the corresponding Elector/Root CA certificate from the CTL,

(d) Alert all affected subscribers with whom it has an agreement

(e) Create a report of the incident with the cause of the compromise or loss and the measures which should be taken to prevent a reoccurrence.

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

(a) Suspend its operation,

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

(c) Alert all affected subscribers with whom it has an agreement.

(396) 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.

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

5.7.4. Business continuity capabilities after a disaster

(398) 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.

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

(400) The SCMS Manager shall have an action plan for the case when a compromised Root CA, Sub CA 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

(401) The Elector may terminate its operation.

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

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

(a) Request the 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 the SCMS Manager.

(404) The SCMS Manager shall remove the corresponding Elector certificate from the CTL.

(405) The SCMS Manager Organization shall invite a new Elector into the ecosystem.

5.8.2. Root CA

(406) The Root CA can only be removed from the CTL by the SCMS Manager. In the event the Root CA is terminated, all Certificates issued by the CA will become invalid and the Root CA will cease to issue Certificates.

(407) If a Provider terminates a Root CA system, the Provider shall provide a minimum of 90days' notice (Notice Period) to all then-current Subscribers to which Certificates have been issued and which have not expired or been revoked. During this Notice Period, the SCMS Manager shall coordinate the transition of the terminating Root CA system to another CA entity established or agreed upon by the Subscribers to continue service. For the Provider to complete this transition, a simple majority of the then-current Subscribers shall agree to the transition to the new entity. Should a simple majority not agree to the transition, then the SCMS Manager will terminate the Root CA at the end of the Notice Period. Upon termination, the records of the CA will be archived and retained for a period of two years.

(408) 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.

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

(a) Notify the SCMS Manager about the termination of services 90 days before the planned termination date and the revocation of its certificate at the end of service,

(b) Request the SCMS Manager to remove the Root CA certificate from the CTL,

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

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

(e) Publish the last revocation status information (CRL signed by the Root CA) to the relying parties, indicating clearly that it is the latest revocation information,

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

(g) Transfer archived records to the SCMS Manager.

(410) Upon receiving termination documentation, the SCMS Manager shall remove the corresponding Root CA certificate from the CTL.

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

(411) In the event of the termination of the service of a Sub CAs or other SCMS model element, the Sub CA or other SCMS model element shall provide notice at least to the superior CA and the related end entities' subscribers. A Sub CA or other SCMS model element shall not terminate its operation without establishing a migration plan that guarantees ongoing operation for all subscribers.

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

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

(b) Destroy the Sub CA or other SCMS model element private key including key backups,

(c) Archive all audit logs and other records prior to termination of Sub CA or other SCMS model element,

(d) Transfer archived records to the superior CA.

(413) Upon receiving termination documentation, the superior CA shall revoke the corresponding Sub CA or other SCMS model element certificate.

6. TECHNICAL SECURITY CONTROLS

6.1. Key-pair generation and installation

(414) The SCMS model elements and end entities shall be able to generate their own key pairs in accordance with subsection 6.1.1 of the present document.

(415) When generating key material, the SCMS model element shall create auditable evidence to show that it enforced role separation and followed its key generation process.

(416) The SCMS model elements shall have an independent third-party auditor validate the execution of the key process by either witnessing the key generation or by examining the signed and documented record of the key generation. The SCMS Manager may verify the audit result documentation.

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

(418) The key pair generation process shall be subject to the requirements of subsection 6.1.2 of the present document.

(419) 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.

(420) The RA, the ACA, and the end entities shall also support the butterfly key mechanism specified in the IEEE 1609.2.1 [1]. and may support the non-butterfly key mechanism.

(421) The end entities shall perform the butterfly private key derivation inside their cryptographic module.

6.1.1. Cryptographic requirements

(422) Table 2 shows the mandatory algorithm implementations for each certificate type and for usages (Specified by NIST FIPS 186-5 [8] and RFC 5639 [9], defined in IEEE 1609.2 and IEEE 1609.2.1 [1])

	ecdsaBrainpoolP256r1WithSha256	***ecdsaBrainpoolP384r1WithSha384***	***ecdsaNistP256 WithSha256***	***ecdsaNistP384WithSha384***
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*

	ecdsaBrainpoolP256r1WithSha256	***ecdsaBrainpoolP384r1WithSha384***	***ecdsaNistP256 WithSha256***	***ecdsaNistP384WithSha384***
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*
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*

Table 2: Mandatory algorithm implementation

6.1.1.1. *Crypto-agility*

(423) Requirements on key lengths and algorithms must be changed over time to maintain an appropriate level of security. The SCMS Manager shall monitor the need for such changes in the light of actual vulnerabilities and state-of-the-art cryptography. It will draft, approve and publish an update of its certificate policy if it decides that the cryptographic algorithms shall be updated. Where a new issue of the CP signals a change of algorithm and/or key length, the SCMS Manager shall adopt a migration strategy, which includes transition periods during which old algorithms and key lengths must be supported. In addition, the SCMS Provider shall also monitor the relevant standards and recommendations so that it can implement cryptographic changes in its own system if necessary - e.g. based on the decision of the SCMS Manager.

(424) To enable and facilitate the transfer to new algorithms and/or key lengths, all PKI participants should 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*

(425) SCMS model elements and end entities shall use NIST validated FIPS 140-2 [4] Level 3 physical cryptographic modules (HSMs) in their systems.

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

(a) Generating, handling and administering 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.

(427) 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.

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

(429) At least two authorized persons are required for signing the CTL at Elector.

(430) At least two authorized persons are required for signing the CRL with the Root CA.

(431) The Sub CAs may perform automatic signature creation, after a manual key activation.

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

(433) A cryptographic module for end entities shall be used for:

(a) Generating, handling and administering private keys,

(b) Generating and handling 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

(434) 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.

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

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

6.1.4. Destruction of private keys

(437) 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 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.

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

6.2. Activation data

(439) The term activation data refers to authentication factors required to operate cryptographic modules to prevent unauthorized access. The usage of the activation data of an SCMS model element cryptographic device shall require action by two trusted persons.

6.3. Computer security controls

(440) The Electors' and CAs' computer security controls shall be designed in accordance with the high security level by adhering to the requirements of WebTrust for CAs [6] or ISO 27001 [5] or SOC2 [11].

6.4. Life-cycle technical controls

(441) The Electors' and CA's technical controls shall cover the whole lifecycle of the CA. This includes the requirements of subsection 6.1.1.1 of the present document.

6.5. Network security controls

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

(443) 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 [5] and ISO/IEC 27002 [10].

(444) 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 profile

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

(446) The IEEE 1609.2 [7] certificates shall indicate the permissions for the types of usage.

(447) For X.509 certificates:

(a) The X.509 certificate shall follow the RFC 5280 [12]-defined PKIX profile.

(b) In case of ECDSA keys, the key shall be RFC 5480 [13]-encoded.

(448) The certificate types allowed for SCMS elements (defined in IEEE 1609.2.1 [1]) are summarized in Table 3.

SCMS element (certificate profile)	**X.509 or IEEE 1609.2.1 [1]**	**IEEE 1609.2.1 [1] type (Explicit and/or implicit)**
Elector	IEEE 1609.2.1 [1]	explicit
Root CA	IEEE 1609.2.1 [1]	explicit
ICA	IEEE 1609.2.1 [1]	explicit
ECA	X.509 or IEEE 1609.2.1 [1]	explicit
ACA	IEEE 1609.2.1 [1]	explicit
CRL Signer	IEEE 1609.2.1 [1]	explicit
RA	X.509 or IEEE 1609.2.1 [1]	explicit
LA	X.509 or IEEE 1609.2.1 [1]	explicit
MA	X.509 or IEEE 1609.2.1 [1]	explicit
EC	X.509 or IEEE 1609.2.1 [1]	implicit or explicit
AC	IEEE 1609.2.1 [1]	implicit or explicit

Table 3: *Certificate types allowed for SCMS elements*

7.2. Certificate validity

7.2.1. SCMS model elements

(449) 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.

(450) The SCMS model elements certificates shall have the following time parameters defined in Table 4:

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, key lifetime maximum: 20 years
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

Table 4: *SCMS Model element certificate time parameters*

(451) When an SCMS Provider certificate is about 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 the verification of the end entity.

(452) The end entity certificates shall 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 [1] ACPC not used
AC (RSE)	3 year (-validity)*	1 w + 1 h overlap time	1	2	* when IEEE 1609.2.1 [1] ACPC not used
EC	3 months	3 years	1	1	

Table 5: *End entity certificate time parameters*

7.2.1.1. Time-period parameters

(453) The Time-Period base parameters are described in Table 6:

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	-

Table 6: *Time-period base parameters*

7.3. Certificate revocation list

(454) The format and content of the CRL issued by a CA or CRL Signer shall be as laid down in IEEE 1609.2.1 [1].

(455) The CRL shall be issued at least monthly with 4 days of overlap time.

7.4. Certificate trust list

(456) The format and content of the CTL issued by the SCMS Manager (and signed by Electors) shall be as laid down in in IEEE 1609.2.1 [1].

(457) The CTL is valid until:

(a) A new CTL is issued,

(b) One of the Elector 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

(458) A compliance audit shall be ordered by a SCMS Provider for itself and optionally for its own subordinate CAs against the requirements of WebTrust for Certification Authorities v2.2.2 [6].

(459) A compliance audit shall be ordered by a SCMS Provider for itself and optionally for its own subordinate CAs against the requirements of either TISAX AL2 or ISO 27001 [5].

(460) The SCMS Provider shall present its CPS to the accredited auditor.

(461) The audit result of a Root CA compliance audit shall be forwarded to and approved by the SCMS Manager before adding the Root CA certificate to the SCMS Manager's CTL.

(462) The audit shall cover all requirements of WebTrust for Certification Authorities v2.2.2 [6] as well as the applicable CP(s) to be fulfilled by the SCMS element Provider to be audited. The scope of the audit shall cover all of the processes mentioned in its CPS, the premises and responsible persons.

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

8.1.2. End Entity devices

(464) The device audit shall be based on the requirements of the following documents:

(a) requirements specifications developed by professional organizations, (e.g. C2C-CC BSP 1.6 [2][3] or newer, or C-ROADS Release 2.0 [3][4] or newer) for OBEs and RSEs,

(b) RSEs should be audited against the requirements of ITE RSU Standard 1.0 [14]

(465) The device HSM audit shall be based on the requirements of the following documents:

(a) HSM modules validations defined in Section 6.1.2 (requirement (425))

8.1.3. End entity device operator

(466) A compliance audit shall be ordered by an end entity device operator for itself.

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

(a) The present CP,

[3] https://www.car-2-car.org/documents/basic-system-profile

[4] https://www.c-roads.eu/platform/about/news/News/entry/show/release-20-of-c-roads-harmonised-c-its-specifications.html

(b) ISO/IEC 27001 [5] or equivalent.

8.2. Frequency of the audits

8.2.1. SCSMS Providers and Electors

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

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

(b) At every substantial change of the CP, if the SCMS Manager requires it,

(c) Regularly at least every three years during their operation.

8.2.2. End Entity devices

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

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

(471) If a device or HSM was recertified, the lifetimes in (469) and (470) shall be recalculated.

8.2.3. End entity device operator

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

(a) before the start of their operation,

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

8.3. Identity/qualifications of auditor

8.3.1. SCSMS Providers and Electors

(473) Electors and SCMS Providers shall select an accredited PKI auditor to perform the audits described in Section 8.1.

(474) The auditing body performing the WebTrust [6] audit shall be accredited for carrying out WebTrust [6] audits.

(475) The auditing body performing the ISO 27001 [5] or TISAX audit shall be accredited for carrying out ISO 27001 [5] or TISAX AL2 audits.

8.3.2. End Entity devices

(476) The manufacturers of the devices shall select an accredited auditor to audit their products.

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

(a) ISO/IEC 15408 [15], or

(b) ISO/IEC 19790 [16].

8.3.3. End Entity device operator

(478) 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 [5].

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

(a) ISO/IEC 27001 [5]

8.4. Auditor's relationship to audited entity

(480) The accredited PKI auditor shall be independent from the audited entity.

8.5. Action taken as a result of deficiency

8.5.1. SCSMS Providers and Electors

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

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

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

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

(485) In case of a Sub CA (ICA, ECA, ACA) audit, the SCMS Provider of the issuing CA shall decide whether to accept the audit report. Depending on the audit results, the SCMS Provider of the issuing CA shall decide whether to suspend the operation of the Sub CA or revoke the Sub CA's certificate in accordance with rules in the issuing CA's CPS. The Root CA shall always ensure the Sub CA's (ICA, ECA, ACA) compliance with this CP.

8.5.2. End Entity devices

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

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

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

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

8.5.3. End Entity device operator

(488) 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.

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

8.6. Communication of results

8.6.1. SCMS Providers and Electors

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

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

8.6.2. End Entity devices

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

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

8.6.3. End Entity device operator

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

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

9. OTHER PROVISIONS

9.1. Fees

(496) The members of the SCMS Manager together finance the regular recurrent **costs** of operation of the SCMS Manager relating to the activities set out in this CP.

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

9.2. Financial responsibility

(498) 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

(499) The following information shall be kept confidential and private:

(a) Root CA, ICA, ACA, ECA, RA, MA, LA, DC, CRL Signer 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

(500) 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 (e.g. national) frameworks.

REFERENCES

[1] IEEE 1609.2.1-2022; IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Certificate Management Interfaces for End Entities; 2022; URL: https://standards.ieee.org/ieee/1609.2.1/10728/

[2] CAR 2 CAR Communication Consortium Basic System Profile; Release 1.6.7; URL: https://www.car-2-car.org/documents/basic-system-profile

[3] C-Roads harmonised C-ITS specifications; Release 2.0; URL: https://www.c-roads.eu/platform/about/news/News/entry/show/release-20-of-c-roads-harmonised-c-its-specifications.html

[4] FIPS 140-2; Security Requirements for Cryptographic Modules; URL: https://csrc.nist.gov/pubs/fips/140-2/upd2/final

[5] ISO/IEC 27001:2022; Information security, cybersecurity and privacy protection — Information security management systems — Requirements; URL: https://www.iso.org/standard/27001

[6] Webtrust® for Certification Authorities; WEBTRUST PRINCIPLES AND CRITERIA FOR CERTIFICATION AUTHORITIES; Version 2.2.2; URL: https://www.cpacanada.ca/en/business-and-accounting-resources/audit-and-assurance/overview-of-webtrust-services/principles-and-criteria

[7] 1609.2-2022 - IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Application and Management Messages; March 2023; URL: https://ieeexplore.ieee.org/document/10075082

[8] FIPS 186-5; Digital Signature Standard (DSS); February 2023; URL: https://csrc.nist.gov/pubs/fips/186-5/final

[9] RFC 5639; Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation; March 2010; URL: https://datatracker.ietf.org/doc/html/rfc5639

[10] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls; URL: https://www.iso.org/standard/75652.html

[11] SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy; URL: https://www.aicpa-cima.com/cpe-learning/publication/soc-2-reporting-on-an-examination-of-controls-at-a-service-organization-relevant-to-security-availability-processing-integrity-confidentiality-or-privacy

[12] RFC 5280; Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile; May 2008; URL: https://datatracker.ietf.org/doc/html/rfc5280

[13] RFC 5480; Elliptic Curve Cryptography Subject Public Key Information; March 2009; URL: https://datatracker.ietf.org/doc/html/rfc5480

[14] Roadside Unit (RSU) Standard; A connected intersection-ready Standard of AASHTO, ITE, NEMA and SAE International; September 2021; URL: https://www.ite.org/technical-resources/standards/rsu-standardization/

[15] ISO/IEC 15408-1:2022; Information security, cybersecurity and privacy protection — Evaluation criteria for IT security; URL: https://www.iso.org/standard/72891.html

[16] ISO/IEC 19790:2025; Information security, cybersecurity and privacy protection — Security requirements for cryptographic modules; URL: https://www.iso.org/standard/82423.html

[17] RFC 3647 - Public Key Infrastructure Certificate Policy and Certification Practices Framework