SCMS MANAGER™
SECURITY CREDENTIAL MANAGEMENT SYSTEM

SCMS MANAGER PROVIDER REQUIREMENTS

DRAFT VERSION 1.0

October 12, 2023

Author

SCMS Manager

© 2019-2023 SCMS Manager LLC - All Rights Reserved

TABLE OF CONTENTS

© 2019-2023 SCMS Manager LLC - All Rights Reserved

© 2019-2023 SCMS Manager LLC - All Rights Reserved

1 OVERVIEW

Organizations operating Root-CAs and subordinate CAs issuing certificates are also referred to as SCMS Providers, or Providers. This document defines the requirements for an SCMS Provider to become part of the SCMS Manager trust environment. These Provider Requirements establish the technical, legal, business, and operational requirements governing the issuance, distribution, revocation and use of certificates and the administration of the Root-CAs and subordinate CAs associated with SCMS Manager.

The requirements of Annex1 (SCMS Manager Provider Operations) form a template which shall be used by the Providers as a basis for their own Certificate Policy (CP) and Certificate Practice Statement (CPS). The CPS shall be in line with this document and shall indicate how the mandatory requirements for the SCMS Manager Provider are met. All requirements from this Provider Requirements document shall be addressed in the Provider' s CPS.

This document is part of a collection of policies and operating requirements that define the SCMS Manager trust environment. In this document, entities such as Electors and the Ecosystem Audit Committee (EAC) are referenced. An overview of these entities is given in this document as necessary. Detailed Information about these entities and their operation can be found in the associated documents:

- Elector requirements (present Elector Policy-version 1.1)
  Reference: Elector-Policy-v1.1.pdf (scmsmanager.org)

Other referenced documents include:

- End-Entity Requirements (Version 1.0)
- Misbehavior Report and Application Specification (Version 1.0)

These documents are available on the SCMS Manager Website:

https://www.scmsmanager.org/publications/

This policy supports implementations of the IEEE 1609.2 Security Services standard defining certificates for use in road vehicles and roadside equipment. The certificate format and operational requirements are defined in the following documents:

- IEEE 1609.2-2022
- IEEE 1609.2.1-2022

SCMS Manager has defined a subset of the IEEE 1609.2.1-2022 operational requirements that are to be required and implemented by SCMS providers. This profile is defined in **IEEE 1609.2.1 Profile (Version 1.0.3).**

Throughout this document, keywords are used to identify requirements. The keywords "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT",and "MAY" are used. These words are a subset of the IETF Request For

© 2019-2023 SCMS Manager LLC - All Rights Reserved

Comments(RFC) 2119 keywords, and have been chosen based on convention in other normative documents [RFC2119].

© 2019-2023 SCMS Manager LLC - All Rights Reserved

2 SCMS MANAGER ENTITIES

This chapter introduces the primary entities and roles of the SCMS Manager. Refer to the current documentation regarding the entities for detailed information about their requirements and operation of them.

2.1 SCMS MANAGER ECOSYSTEM AUDIT COMMITTEE (EAC)

The SCMS Manager Ecosystem Audit Committee (EAC) verifies that entities, such as root-CAs and Electors, are compliant with their obligations to SCMS Manager. It is also the responsibility of the EAC to authorize the addition of new Root-CAs and Electors or the removal of a Root-CA or an Elector if the continued operation of that entity will harm the integrity and trust of the V2X ecosystem.
The SCMS Manager EAC Requirements document specifies how the decision to add or remove an Elector or Root CA shall be made and it describes the policies and procedures that govern the Ecosystem Audit Committee itself.

2.2 ELECTORS

The role of Electors is to endorse a set of trusted Root-CAs and maintain a set of valid Electors. Electors manage the trust of Root-CA certificates and peer Elector Certificates by signing a Certificate Trust List (CTL) containing identifiers for the trusted certificates. Five Electors are active at one time and by a quorum, or more, of trusted electors a CTL is signed. How the quorum and the number of electors is managed and communicated to system participants is outside the scope of this document. The SCMS Manager Elector Requirements document specifies how the decision to add or remove an Elector or Root-CA will be made and it describes the policies and procedures that govern the Electors themselves.

2.3 POLICY AUTHORITY (PA)

The Policy Authority is a working group, consisting of SCMS Manager members, which is responsible for updating this SCMS Manager Provider Requirements document. The PA shall determine the conformance of the Certificate Practice Statement (CPS) to this document for the Providers that issue Certificates and Certificate Trust Lists under this document based on the results and recommendations received from an independent auditor (PKI Auditor). The PA will submit a report to the EAC about the conformance of the CPS. The Providers shall meet all requirements of the approved CPS before commencing operations. The PA is the only body with authority to approve this Provider Requirements document and any amendments to it. Amendments may be made by the PA either by updating and publishing the entire document or by publishing a separate addendum. Subscribers and SCMS Manager members will be notified by email and will have a fifteen (15) day review period to provide any feedback on the amendments before the PA publishes the amended Providers Requirements document. The amendments are effective upon publication. The EAC is to publish a transitional period by which the changed requirements shall be implemented.

© 2019-2023 SCMS Manager LLC - All Rights Reserved

2.4 SUBSCRIBERS

Subscribers are OEM, Tier 1, device manufacturers, governments and road operator organizations who have signed a Subscriber Agreement with a Provider to receive and use V2X end-entity certificates in their RSUs, OBUs or V2X applications. That Subscriber Agreement establishes the rights and responsibilities of the parties regarding the issuance and management of Certificates.

2.5 EXTERNAL PKI AUDITOR

Each provider shall select an accredited PKI auditor to audit it in accordance with this Provider Requirements document. The accredited PKI auditor shall be independent of the audited entity. The PKI Auditor is responsible for performing or organizing audits of Electors, Root-CAs, and Sub-CAs. The PKI Auditor notifies the entity managing the Root-CA of the successful or unsuccessful execution of an initial or periodic audit of the Sub-CAs. The PKI Auditor distributes the audit report result (from an initial or periodic audit) to the Provider. The audit report shall include recommendations from the PKI auditor.

© 2019-2023 SCMS Manager LLC - All Rights Reserved

3 SCMS PROVIDER GENERAL REQUIREMENTS

The sections in this chapter outline core Provider requirements. Additional requirements are defined in Annex 1. These requirements are necessary to maintain the overall SCMS Manager trust environment. SCMS Manager Providers shall agree to meet these minimum requirements.

3.1 PROVIDER (ROOT-CA AND SUB-CA) REQUIREMENTS

Before starting operations, a prospective Root-CA or Sub-CA shall present its Certification Practices Statement (CPS) to an accredited PKI auditor as part of an order for a compliance audit. A CPS states the practices employed by a Provider to provide certification services that include, but are not limited to, issuing, managing, and revoking certificates and certificate trust lists in accordance with the specific requirements of this document. In addition to the minimum requirements in this requirements document, the entities operating the Root-CAs and Sub-CAs may decide on their own additional requirements and set them out in their CPS, provided these additional requirements are not contradicting. A CPS does not have to be released publicly. Providers shall maintain a current TISAX AL2 Certificate. An ISO 27001 certification is an acceptable alternative. The Provider shall forward any audit report issued by a PKI auditor to the SCMS Manager EAC. All SCMS Providers shall utilize an independent accredited auditor to audit according to AICPA/CICA WebTrust for Certification Authorities principles and criteria.

3.2 MISBEHAVIOR AUTHORITY REPORT ACCEPTANCE AND PROCESSING

There is a possibility of inaccurate data in messages due to faults or cyber-attacks. The accuracy of data and the safety of vehicles that rely on these messages is of paramount importance. Thus, SCMS Manager has developed a specification for methods and algorithms to identify erroneous message data, flag them as potential misbehavior, and report them, as needed, to the Misbehavior Authority (MA). SCMS Providers shall agree to enforce established and published SCMS Manager specifications for Misbehavior reports and processing. Providers shall implement a Misbehavior Authority (MA) component and adopt the MA procedures. The Provider shall agree to the cooperative sharing of misbehavior reports with other SCMS Manager Providers. Refer to the SCMS Manager-website for publications regarding the current Misbehavior Report and Application Specification.

3.3 SCMS MANAGER END-ENTITY REQUIREMENTS

The SCMS Provider shall agree to support the published requirements in the End-Entity Security requirements, design guidance and validation approach document. This document provides requirements for End-Entity devices intended to be provisioned with 1609.2 certificates for connected vehicle operations in North America.. In addition to the requirements in this document, SCMS Manager will define a certification process associated with these requirements such that device manufacturers can establish that their devices are conformant with the requirements and so eligible to receive certificates. The SCMS Manager Provider shall confirm that the End-Entity has met these requirements before any certificate issuance. Refer to the SCMS Manager website for publications regarding the current End-Entity Security requirements.

© 2019-2023 SCMS Manager LLC - All Rights Reserved

3.4 SCMS MANAGER ARCHITECTURE DESIGN GUIDANCE

The SCMS Provider shall implement the SCMS architecture according to chapter 4 (architecture) of the current release of the:

P1609.2.1-2022 for Wireless Access in Vehicular Environments (WAVE) – Certificate Management Interfaces for End Entities and **IEEE1609.2.1 Profile (Version 1.0.3)**

3.5 CYBERSECURITY (CS) MANAGEMENT

The SCMS Provider shall perform threat analysis and risk assessment. SCMS Manager EAC reserves the right to audit this. The SCMS Provider shall perform continuous CS monitoring and incident response. The SCMS Provider shall agree that in case there is a cybersecurity incident detected, SCMS Manager EAC will be notified immediately and provide the SCMS Manager with the information on which devices are impacted and with information about the remediation plan. A Cybersecurity Incident is according to NIST defined as "An occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies."

3.6 VALIDATION REVIEW AND UPDATES

Devices validated under the procedures described above will be subject to re-validation based on requirements to be developed by SCMS Manager.

- Full or partial re-validation will be required when any changes are made to the product that impact the security of the device. Initially, this determination will be made by self-attestation by the vendor. As will other aspects of validation, this may evolve over time to an external review.
- Re-validation may be done periodically to confirm that the devices being delivered are the same as the device originally validated.
- Re-validation may be required when Misbehavior Detection or other analysis indicates a potential security problem with a validated device.

3.7 INTEROPERABILITY CERTIFICATION

The SCMS Manager Providers shall implement the SCMS in such a way that it meets the approved interoperability requirements regarding devices and also regarding interoperability between the SCMS Providers. The device level interoperability shall be certified by an approved test lab. It requires a test plan and successful tests against that plan. Alternatively, the interoperability can be attested by attending "interoperability test events" and successfully proving interoperability there.

3.8 UPDATE OF THIS PROVIDER REQUIREMENTS DOCUMENT

Any member (observer excluded) of the SCMS Manager can submit a Change Request (CR) to this document. The update process is managed by the Policy Authority PA and follows six steps:

© 2019-2023 SCMS Manager LLC - All Rights Reserved

- Submission of change request (CR),
- Change processing,
- Change approval,
- Change publication,
- Change announcement,
- Change implementation

This Provider Requirements document shall be reviewed by the Policy Authority at least every 3 years. Refer to the applicable SCMS Manager documents for publications regarding the update process.

© 2019-2023 SCMS Manager LLC - All Rights Reserved

4 ANNEX 1: SCMS MANAGER PROVIDER OPERATIONS

4.1 CERTIFICATE USAGE

4.1.1 APPROPRIATE CERTIFICATE USES

The SCMS Provider shall be permitted to issue, manage, and revoke Certificates that enable the creation, operation, or discontinuation of Sub-CAs and other entities including, but not limited to, the Policy Generator, Misbehavior Authority, Intermediate CAs, CRL generators, Enrolment Authority, and Authorization Certificate Authority. The providers also shall be permitted to sign CRLs. Each Sub-CA may create, manage, and destroy cryptographic keys and issue, manage, and revoke its Certificates and perform other functions as described in its applicable certification practice statement. Leaf certificates may only be issued for devices that meet the SCMS Manager EE Requirements. Each SCMS Provider is responsible for the proper installation, use, and end of life for all certificates issued by their PKI infrastructure.

4.1.2 PROHIBITED CERTIFICATE USES

Certificates issued by the Providers shall not be used for any purpose other than those permitted in the "Appropriate Certificate Uses" section. Certificates and CTLs not explicitly authorized by SCMS Manager may not be processed or issued by the Electors and any such properly issued Certificates and signed CTLs shall not be used for any purpose other than those permitted in the "Appropriate Certificate and CTL Uses" section. In addition, Certificates and CTLs issued under this Providers Policy may not be used where prohibited by law.

4.2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

4.2.1 PUBLICATION OF CA INFORMATION AND ACCESS CONTROLS

Self-signed Provider Root CA certificates and associated CRLs shall be available in a publicly accessible repository. SCMS Providers only obtain the CTL published by the SCMS Manager EAC. Providers shall make sure that they distribute the latest CTL (and certificate chains as Certificate Chain File) to the Subscribers. The Provider shall implement repository access controls in relation to all PKI participants and external parties for at least two different levels (e.g., public and restricted to CA level) and prevent unauthorized entities from adding, modifying, or deleting repository entries. These access control mechanisms shall be detailed in the entity's corresponding CPS.

4.2.2 PROVIDERS CP CHANGE

If the Provider determines that changes to their Certificate Policy are necessary or desirable, the Provider will provide a fifteen (15) day review period (Review Period) to all then current Subscribers to which Certificates have been issued and which have not expired or been revoked. Such updates become binding upon being published for all Subscribers and for all Certificates and for all Certificate Trust Lists issued or to be issued.

© 2019-2023 SCMS Manager LLC - All Rights Reserved

4.3 IDENTIFICATION AND AUTHENTICATION

4.3.1 NAMING

4.3.1.1 HOSTNAME SPECIFICATION

The Root-CAs and the Electors Certificates are based on IEEE 1609.2. Hostnames (also known as subject names in X.509 parlance) are UTF8String (SIZE (0…255)) and may be selected by the Subscriber so long as part of the selected hostname identifies the host's function. The recommended host function identifiers are: elector for an Elector-CA, rootca for the Root-CA, ica for Intermediate-CA, ma for Misbehavior Authority, pg for Policy Generator, crlg for CRL Generator, aca for Authorization Certificate Authority, and eca for Enrollment Certificate Authority. The hostnames shall be meaningful. SCMS Manager Providers, at their sole discretion, may refuse to issue a Certificate with a hostname not meeting these requirements. The Root-CAs following the X.509 structure should use conventional subject names. Subject names shall be meaningful. SCMS Manager Providers, at their sole discretion, may refuse to issue a Certificate with a subject name not meeting these requirements.

4.3.1.2 UNIQUENESS OF NAMES

The name for Root-CAs shall consist of a single CertificateID attribute. The uniqueness of names is the sole responsibility of the PA. The PA shall maintain the registry of root CA names upon notification of approval, revocation, removal of a Root-CA. Subject namesCertificateIDs in certificates are limited to 32 bytes. Each Root-CA proposes its name to the PA. The PA is responsible for checking name uniqueness. The name in each ECA/ACA certificate may consist of a single CertificateID attribute with a value generated by the issuer of the certificate. The uniqueness of names is the sole responsibility of the issuing Root-CA. Refer to the IEEE1609.2 standard for additional requirements.

4.3.1.3 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

Subscribers may not request Certificates with any content that infringes the intellectual property rights of another entity. It is not required that an Applicant's right to use a trademark be verified, however, providers may reject any application or require revocation of any Certificate that is part of a trademark or intellectual property dispute or if the provider has reason to believe that such application or Certificate infringes a third party's intellectual property.

4.3.2 INITIAL IDENTITY VALIDATION

For a prospective Root-CA subscriber, the SCMS Provider shall use any legal means of communication or investigation to ascertain the identity of an Applicant. The SCMS Provider may refuse to issue a Certificate at its sole discretion.

4.3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

For Certificate Signing Requests ("CSRs"), Subscribers shall submit a properly formed certificate body that is self-signed to establish both authenticity and integrity of the request. Additional CSR requirements are outlined in the Subscriber Agreement "Certification Signing Request" section.

© 2019-2023 SCMS Manager LLC - All Rights Reserved

4.3.2.2 ORGANIZATION IDENTITY AUTHENTICATION

Applicants for certificates shall submit their name, address, and documentation of their status as a legal entity to the Provider as part of the application process. The legal status of all Applicants shall be verified using reliable third-party and government databases or through other direct means of communication with the entity or jurisdiction governing the entity's legal creation, status, or recognition. If such efforts are insufficient to confirm the legal existence and identity of the entity, the Applicant may be required to provide legal documentation. The SCMS Provider shall verify the information submitted by the Applicant in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the Applicant.

4.3.2.3 INDIVIDUAL IDENTITY AUTHENTICATION

Subscribers shall provide the names of two individuals who are authorized ("Authorized Individuals") to act on the Applicant's/Subscriber's behalf for correspondence with the Provider. Authorized Individuals acting on behalf of Applicants and Subscribers shall be authenticated by the Provider as part of the Subscriber Agreement process.

4.3.3 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

All revocation requests shall be authenticated by the SCMS Provider. A Subscriber shall request the revocation of its Certificate in email, carbon copied to all Authorized Individuals and appropriate Subscriber senior executive, with a paper letter requesting the same, signed by both Authorized Individuals or an Authorized Individual and a senior executive of the Subscriber, and sent by overnight courier to the SCMS Provider Administrator. The SCMS Provider contact information shall be listed in the Certificate Practice Statement (CPS). 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.

4.4 CERTIFICATE AND CTL LIFECYCLE OPERATIONAL REQUIREMENTS

4.4.1 CERTIFICATE APPLICATION SIGNING REQUEST

The Certificate application process shall provide sufficient information to:

- Establish the applicant's or SCMS Manager's Authorized Individual authorization to obtain a Certificate per the "Identification and Authentication" section.
- Establish and record applicant or SCMS Manager Authorized Individual identity per the "Identification and Authentication" section.
- For a Certificate request, obtain the Subscribers public key and verify the Subscriber's possession of the private key for each Certificate required per the "Method to Prove Possession of Private Key" section.
- Verify any role or authorization information requested for inclusion in the Certificate.

These steps may be performed in any order that is convenient for the SCMS Provider administrator and applicants/subscribers/SCMS Manager that does not defeat security, but all shall be completed before Certificate issuance.

© 2019-2023 SCMS Manager LLC - All Rights Reserved

4.4.1.1 CERTIFICATE APPLICATION QUALIFICATIONS

Only Subscribers Authorized Individuals may submit a Certificate application.

4.4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

Providers are responsible for verifying the identity of individuals and entities in accordance with the requirements in this document prior to authorizing the issuance of a Certificate. Each Applicant and SCMS Manager member individual shall submit sufficient information and documentation for the provider to perform the required verification of identity prior to issuing a Certificate. All communications during the Certificate application process shall be authenticated and protected from modification.

4.4.2 CERTIFICATE APPLICATION PROCESSING

The Provider shall verify the accuracy of the information in Certificate applications before Certificates are issued.

4.4.2.1 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

Any Certificate application that is received by the Provider, for which the identity and authorization of the Authorized Individual have been validated and authenticated, will be duly processed. However, the Provider shall reject any application for which such 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 their then current successors), or X.509 Certificate fields as profiled by SCMS Manager, are inappropriately configured in the CSR.

4.4.2.2 TIME TO PROCESS CERTIFICATE APPLICATIONS

The time to process a certificate application shall be acted under a maximum time limit defined in the CPS, but no later than within ten (10) business days after a Subscriber Agreement has been signed and all documentation and authorizations relevant to the application have been received by the Provider.
The Provider shall make every reasonable effort to meet its issuance times and to make applicants aware of any factors that may affect issuance times in a timely manner, targeting normal issuance within 2 business days of receiving a fully executed Subscriber agreement and a valid certificate request. Worst case processing time should be no longer than 5 business days from completion of the relevant agreements and receipt of a valid certificate request.

4.4.3 CERTIFICATE ISSUANCE

4.4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

Upon receiving the request, the SCMS Provider will:

- Verify the identity of the requester.
- Verify the authority of the requester and the integrity of the information in the certificate request.
- Build and sign a requestor's TBS if all certificate requirements have been met.

© 2019-2023 SCMS Manager LLC - All Rights Reserved

- Make the Certificate available to the Subscriber after confirming that the Subscriber has formally acknowledged their obligations as described in the "Subscriber Representations and Warranties" section.

This Certificate will not be created until all verifications and modifications, if any, have been completed to the provider's satisfaction.

All TBS field information received from a Subscriber shall be verified before inclusion in a Certificate. The responsibility for verifying prospective Subscriber data shall be described in the CPS. The Provider shall verify that the identified and authenticated Subscriber is the source of the Certificate request and that the Subscriber is the entity that will be issued the Certificate. Databases used to confirm Subscriber identity information shall be protected from unauthorized modification or use. Provider actions during the Certificate issuance process shall be performed in a secure manner.

4.4.3.2 NOTIFICATION TO SUBSCRIBERS BY THE CA OF CERTIFICATE ISSUANCE

The SCMS 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.

4.4.4 CERTIFICATE ACCEPTANCE

The SCMS Provider shall confirm with the Subscriber 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. If a certificate or CTL is rejected, the provider and SCMS Manager EAC will identify the reason for rejection, and a new Certificate will be issued by the Provider to SCMS Manager EAC and confirmed that it is correct and accepted by SCMS Manager EAC.

4.4.5 KEY PAIR AND CERTIFICATE USAGE

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. Relying Party software shall be compliant with IEEE 1609.2 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.

4.4.6 CERTIFICATE RENEWAL

Certificate renewal is not supported.

© 2019-2023 SCMS Manager LLC - All Rights Reserved

4.4.7 CERTIFICATE REKEY

Rekeying a Certificate consists of creating a new Certificate with a different subject Public Key while retaining the remaining contents of the old Certificate that describe the subject (e.g., hostname and permissions). The new Certificate may be assigned a different validity period, specify a different CRL, and/or be signed with a different key. Subscribers seeking rekey of Certificates shall identify and authenticate themselves for the purpose of rekeying as described in the "Initial Identity Validation" section, and the rekey request shall include a new CSR containing a new Public Key. Reuse of old previously certified private/public key pairs is not allowed. The Provider 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. The Provider shall issue a Certificate for a valid rekey request. The Provider shall notify the Authorized Individuals of the Subscriber, and it may use any reliable mechanism to deliver the Certificate to the Subscriber. The Provider shall contact the Subscriber to confirm receipt of the issued Certificate. After re-keying a client Certificate, the provider 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, the Provider shall not further re-key, renew, or modify the old Certificate.

4.4.8 CERTIFICATE MODIFICATION

Modifying a Certificate means creating a new Certificate for the same subject with authenticated information that differs slightly from the old Certificate (e.g., changes to permissions) provided that the modification otherwise complies with the requirements in this document. The new Certificate shall have the same subject Public Key. Additional examples of circumstances when Certificate modification may occur include minor name changes and the replacement of the Certificate where a minor error in Certificate information or profile has been discovered. After modifying a Certificate, the Provider shall revoke the old Certificate if it has been distributed by the Subscriber to Relying Parties. If the Subscriber has not used the old Certificate, both parties shall destroy it to prevent its dissemination. The Provider shall not further re-key, renew, or modify the old Certificate. The Provider may modify Certificates at its own discretion or upon the request of a Subscriber. Upon receiving a request for modification, the Provider shall verify any information that will change in the modified Certificate. The Provider may issue the modified Certificate only after completing the verification process, which may include telephonically contacting the Subscriber. The validity period of a modified Certificate shall not extend beyond the authorized duration (see the "Technical Security Controls" section).

4.4.9 CERTIFICATE REVOCATION AND SUSPENSION

This section describes Certificate revocation by the SCMS Manager. Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. The Provider shall issue CRLs covering all revoked but unexpired Certificates issued. The Provider shall make public a description of how to obtain revocation information for the Certificates they publish and an explanation of the consequences of using dated revocation information. This information shall be given to Subscribers during certificate request or issuance and shall be readily available to any potential relying party. Certificate suspension is not supported.

4.4.9.1 CIRCUMSTANCES FOR CERTIFICATE REVOCATION

© 2019-2023 SCMS Manager LLC - All Rights Reserved

Certificate revocation may be performed for the following circumstances:

- If the CA has reason to believe that the private key associated with a certificate has been compromised (revealed, lost, stolen)
- If the IEEE 1609.2 equivalent subject or identifier in the certificate is no longer associated with the Subscriber
- If there is incorrect information included in the certificate which may cause it to be used or relied upon inappropriately
- If the Subscriber agreement has been terminated
- If the Subscriber has violated its license or certificate usage agreements
- If the entity subject to suspension or revocation has materially failed and is unable to mitigate security or processing integrity concerns of a relevant audit
- If ordered by a court or entity with contractual or legal jurisdiction

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.

4.4.9.2 WHO CAN REQUEST REVOCATION?

SCMS Providers shall accept revocation requests from authenticated and authorized parties, such as the Subscriber or an authorized US-DOT representative. A Provider 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 and SCMS Manager EAC, unless a shorter time period is necessary due to criticality.

4.4.9.3 PROCEDURE FOR REVOCATION REQUEST

Entities submitting Certificate revocation requests shall list their identity and explain the reason for requesting revocation.
A Provider 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, the Provider shall investigate the alleged basis for the revocation request. The Provider shall maintain a 24/7 support contact mechanism to capture any reporting of a Certificate problem. The Provider shall respond within the time period as specified in the CPS. If appropriate, Providers may forward complaints to law enforcement. The Providers shall list revoked Certificates in their CRL where they will remain until the end of their validity period.

4.4.10 CRL ISSUANCE FREQUENCY AND LATENCY

The Provider shall publish CRLs within one (1) 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.

© 2019-2023 SCMS Manager LLC - All Rights Reserved

4.4.11 CTL ISSUANCE FREQUENCY AND LATENCY

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 by the Provider within three (3) business days.

4.4.12 OCSP SUPPORT

Root-CA certificates shall also support validation using the Online Certificate Status Protocol (OCSP). Each Root-CA certificate will include a network address where the corresponding OCSP service handler can be contacted.

4.4.13 KEY ESCROW AND RECOVERY

Root-CA private keys are never escrowed.

4.5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

This section describes the non-technical security controls used by the CA system to perform the functions of key generation, subject authentication, Certificate issuance, Certificate revocation, CTL issuance, audit, and archival.

4.5.1 PROVIDER SECURITY CONTROLS

Critical Provider operations take place within secure facilities to which access is limited to authorized personnel. Cryptographic hardware is physically segregated from the organization's other systems. Access to such systems is controlled by multiple layers of physical security controls, providing reasonable assurance that access is only granted to individuals who require such access to fulfill their job responsibilities. Details of the Provider's security controls are documented in internal documents. These policies are not publicly disclosed but are reviewed within the scope of WebTrust for Certification Authorities.
These policies document controls related to the following:

- Physical site construction
- Physical access controls,
- Environmental controls,
- Operational controls, and
- Personnel security controls.

In order to minimize the possibility of remote security attacks on a Root-CA, a Root-CA shall not have network connectivity at any time.

4.5.2 AUDIT LOGGING PROCEDURES

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 an internal auditor. The administrator is a different person

© 2019-2023 SCMS Manager LLC - All Rights Reserved

from those who control the signing key. The auditor will report any unusual events to the PA for analysis and resolution. All available logs may be subject to audit by the independent auditor.

4.5.3 RECORDS ARCHIVAL

An SCMS Provider shall include enough detail in its archived records to show that a Certificate was issued in accordance with the mandatory requirements. The Provider shall retain the following information in its archives regarding its operation:

1. Any accreditation of the specific Root-CA or sub-CA
2. CP and CPS versions
3. Contractual obligations and other agreements concerning the operation of the CA
4. System and equipment configurations, modifications, and updates
5. Certificate and revocation requests
6. Identity authentication data
7. Any documentation related to the receipt or acceptance of a Certificate or token
8. Subscriber Agreements
9. Issued Certificates
10. A record of Certificate re-keys
11. Other signed files such as CRLs and CTLs
12. Any data or applications necessary to verify an archive's contents
13. Compliance auditor reports
14. Any changes to the specific CA audit parameters
15. Event and audit logs, including identified attempts to delete or modify the logs
16. Key generation actions
17. Access to Private Keys for key recovery purposes
18. Changes to trusted Public Keys
19. Approval or rejection of a Certificate status change request
20. Appointment of an individual to a trusted role
21. Destruction of a cryptographic module
22. Certificate compromise notifications
23. Remedial action taken as a result of violations of physical security
24. Violations of the respective CP or CPS

All records shall be archived in a secure offsite location and retained for a period of five (5) years from their dates of origination. No unauthorized person may read, modify, or delete the archives.

4.5.4 KEY CHANGEOVER

Providers will change Provider Key Pairs periodically. After key change, the provider shall sign Certificates using only the new Private Key. The Provider shall destroy its old CA Private Key and shall make the old CA Certificate available to verify signatures until all Certificates signed using the old Private Key have expired.

© 2019-2023 SCMS Manager LLC - All Rights Reserved

4.5.5 PROVIDER PRIVATE KEY COMPROMISE AND DISASTER RECOVERY

4.5.5.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

If a Provider suspects that a CA Private Key is compromised or lost then the Provider shall immediately assess the situation, determine the degree and scope of the incident, and notify its current Subscribers and the SCMS Manager EAC. The results of the investigation shall be reported to its current Subscribers and the SCMS Manager EAC. The report shall detail the cause of the compromise or loss and the measures which should be taken to prevent a reoccurrence.

4.5.5.2 BUSINESS CONTINUITY AND DISASTER RECOVERY

The entities operating secure facilities for CA operations shall develop, implement, and maintain a disaster recovery plan designed to mitigate the effects of any kind of natural or man-made disaster. Disaster recovery plans address the restoration of information systems services and key business functions.

4.5.6 CA TERMINATION

The Root-CA system can only be terminated by the Electors voting to revoke the CA or by SCMS Manager EAC. In the event the CA is terminated, all Certificates issued by the CA will become invalid and the CA will cease to issue Certificates. If a Provider terminates a Root-CA system, the Provider will provide a minimum of 365 days' 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, SCMS Manager EAC will coordinate the transition of the terminating Root-CA system to another CA entity established or agreed upon by the Subscribers in order 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 EAC 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 (2) years.

4.6 TECHNICAL SECURITY CONTROLS

4.6.1 KEY PAIR GENERATION

All Key Pair generation shall be achieved using a Hardware Security Module ("HSM"), which has been NIST validated as meeting Federal Information Processing Standards ("FIPS") 140-2 Level 3 or higher.
The key pairs generated shall be NIST- or Brainpool- approved key types according to IEEE 1609.2.1-2022.
When generating keying material, the Provider (Root-CAs and all Sub-CAs) shall create auditable evidence to show that they enforced role separation and followed its key generation process. SCMS Manager EAC 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.
Subscribers shall generate their Elliptic Curve Cryptography (ECC) key pairs for Certificate signing using an HSM that has been NIST validated as meeting FIPS 140-2 Level 3 at a minimum.

© 2019-2023 SCMS Manager LLC - All Rights Reserved

4.6.2 PRIVATE KEY PROTECTION

The HSM for generating and storing a Provider's Private Key shall be minimally certified to FIPS 140-2 Level 3 or higher. This shall apply to Root-CAs and to all Sub-CAs. There shall be a separation of physical and logical access to the Provider's Private Key to this extent:

- A minimum of two individuals are required for physical access to the hardware.
- If a Root-CA's Private Key requires disaster recovery, a secret splitting method consisting of individuals, passphrases, and m of n removable tokens is required for logical reconstruction. When a Root-CA signing pair is changed, the old m of n key shares shall be physically destroyed.
- A Root-CA Private Key shall never be exported from the HSM as plaintext.

4.6.3 PUBLIC KEY DELIVERY TO THE PROVIDER

Subscribers shall use a self-signed certificate of the appropriate IEEE 1609.2 structure for the entity the certificate is being requested to deliver their Public Key to the provider and the appropriate Root-CA system. This message format provides proof-of-possession of the Private Key associated with the Public Key. The Provider shall confirm that it has correctly received the Public Key from the Subscriber prior to issuing a Certificate for the Public Key.

4.6.4 ROOT CERTIFICATE OPERATIONAL PERIOD AND KEY PAIR USAGE PERIOD

The SCMS Provider shall follow the recommended Certificate operational periods and private key cryptoperiods as specified by the PA or SCMS Manager EAC. The Root-CA Private Key shall have a Cryptoperiod of 20 years and its Root Certificate shall have a 70-year lifetime. At the end of its Cryptoperiod, the private key will be destroyed.

© 2019-2023 SCMS Manager LLC - All Rights Reserved