SCMS MANAGER™
SECURITY CREDENTIAL MANAGEMENT SYSTEM

SCMS MANAGER ECOSYSTEM AUDIT COMMITTEE (EAC) REQUIREMENTS

VERSION 1.0

August 9, 2024

Author

SCMS Manager

© SCMS Manager LLC - All Rights Reserved

TABLE OF CONTENTS

© SCMS Manager LLC - All Rights Reserved

1 OVERVIEW

The SCMS Manager Ecosystem Audit Committee (EAC) approves and implements policies on behalf of the SCMS Manager. It accepts guidance for new policies from a collection of workgroups including the Policy Workgroup which reviews and recommends operational requirements for the SCMS Manager and its members.

The EAC verifies that entities, such SCMSes and Electors, are compliant with their obligations to SCMS Manager. It is also the responsibility of the EAC to authorize the addition of new RCAs and Electors or the removal of a RCA or an Elector if the continued operation of that entity will harm the integrity and trust of the V2X ecosystem.

This SCMS Manager EAC Requirements document specifies how the decision to add or remove an Elector or RCA (operated by an SCMS Provider) SHALL be made and it describes the requirements and procedures that govern the EAC. This document is part of a collection of policies and operating requirements that define the SCMS Manager trust environment. Additional details about other entities and their operation can be found in the associated documents listed in section 1.1.

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

1.1 REFERENCES

- SCMS Manager Elector Requirements [in development – to be published in 2024]
- SCMS Manager Provider Requirements (Version 1.0)
- SCMS Manager Elector Technical Specification (Version 1.1)
- SCMS Manager Certified Trust List (CTL) Update Process [in development – to be published in 2024]

Published documents are available on the SCMS Manager Website:

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

1.2 SCMS MANAGER ENTITIES

The following sections introduce the primary entities and roles of SCMS Manager.

1.2.1 SCMS PROVIDER (RCA AND SUB-CA)

A Certificate Authority (CA) is an entity for issuing public key certificates within the V2X ecosystem. The IEEE Std 1609.2.1-2022 document describes a RCA and various subordinate CAs (Sub-CAs). The entities issuing certificates to End-Entities are also referred to as SCMS Providers. Providers SHALL have a

© SCMS Manager LLC - All Rights Reserved

Certificate Policy (CP) and a Certificate Practice Statement (CPS). Before starting operations, a prospective RCA or Sub-CA SHALL present its Certificate Policy (CP) and Certificate Practices Statement (CPS) to an accredited PKI auditor as part of an order for a compliance audit. A CP states the policies governing the PKI and the CPI states the practices employed by a Provider to implement certification services that include, but are not limited to, issuing, managing, and revoking certificates and certificate trust lists. The SCMS Manager Provider Requirements document defines the technical and operational requirements to be fulfilled by the Provider before starting operations.

1.2.2 ELECTORS

The role of Electors is to endorse a list of trusted RCAs and valid Electors. Electors manage the trust of RCA certificates and peer Elector Certificates by signing a Certificate Trust List (CTL) containing identifiers for the trusted certificates. Generally, five Electors are active at any given time. It could be fewer if an Elector has been recently removed and is in the process of being replaced. A minimum of three Electors is required to sign any CTL in order for it to be valid. Each elector SHALL be operated as an offline CA that SHALL sign the proposed Certificate Trust List (tbsCTL per IEEE P1609.2.1/D9) as specified by the EAC.

The Electors form the most basic root of trust of the V2X Ecosystem. The technical security controls for key generation and storage are the same as for SCMS Providers. The role of Electors SHALL be carried out by a trusted entity which has a contracted relation with SCMS Manager. The SCMS Manager Elector Requirements document describes the policies and procedures that govern the Electors and the SCMS Manager Elector Technical Specification provides detailed technical specifications for implementing those policies and procedures.

1.2.3 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.

1.2.4 POLICY WORKGROUP

The Policy Workgroup consists of SCMS Manager members. The Workgroup is responsible for updating this SCMS Manager EAC Requirements document. The Policy Workgroup SHALL also determine the conformance of the Certificate Policy (CP) to the SCMS Manager Provider Requirements document for the Providers that issue Certificates and Certificate Trust Lists based on the results and recommendations received from an independent auditor (PKI Auditor). The Policy Workgroup SHALL submit a report to the EAC about the conformance of the CP. The Providers SHALL meet all requirements of the approved CP before commencing operations. The EAC is the only body with authority to approve any new SCMS Manager Policy or Requirements documents or changes to existing ones. Amendments may be made either by updating and publishing the entire document or by publishing a separate addendum.

© SCMS Manager LLC - All Rights Reserved

Subscribers and SCMS Manager members SHALL be notified by email and SHALL have a fifteen (15) day review period to provide any feedback on the amendments before the amended document is published. The amendments are effective upon publication. The EAC is to publish a transitional period by which the changed requirements SHALL be implemented.

1.2.5 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.

1.2.6 EXTERNAL PKI AUDITOR

Each SCMS Provider SHALL select an accredited PKI auditor to audit it in accordance with the 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, RCAs, and Sub-CAs. The PKI Auditor notifies the entity managing the RCA 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 SCMS Provider. The audit report SHALL include recommendations from the PKI auditor. The PKI auditor SHALL perform the audit in compliance with the AICPA/CICIA WebTrust certification program. More information is available at CPA Canada.

1.3 TERMS

Certificate Policy – a document that describes what a PKI is expected to do

Certificate Practice Statement – a document that describes the how the CP is implemented

Ecosystem Audit Committee – A committee of SCMS Manager that is responsible for the overall security of the V2X system, specifically the management of the CTL.

Elector – One of a set of five signers that is responsible for signing the CTL. It generally functions as and is protected in a similar way to a Root CA but is used for this special purpose. If for any reason one Elector is lost or removed, a new one will be created to take its place. So there may be briefly less than five during such a transition period.

Root Certificate Authority – The foundational key of an SCMS Provider. It is signed by the CTL.

WebTrust – an auditing program for certificate authorities, developed by the AICPA (American Institute of Certified Public Accountants) and CICA (Canadian institute of Chartered Accountants) and managed by the CPAC (Chartered Professional Accountants of Canada). Many auditors are certified to perform audits against this standard. Details at: WebTrust seal program - CPA Canada

1.4 ACRONYMS

CP – Certificate Policy

CPS – Certificate Practice Statement

© SCMS Manager LLC - All Rights Reserved

CTL – Certificate Trust List (see also tbsCTL)

EAS – Ecosystem Audit Committee, a committee of SCMS Manager

OEM – Original Equipment Manufacturer, in this context an automobile company

OBU – On Board Unit

PKI – Public Key Infrastructure

RCA – Root Certificate Authority

RSU – Road Side Unit

SCMS – Secure Certificate Management System

SPOC – Single Point Of Contact

tbsCTL – to be signed Certificate Trust List (see also CTL)

V2X – Vehicle-to-Everything

2 ECOSYSYEM AUDIT COMMITTEE (EAC) REQUIREMENTS

2.1 EAC MEMBERSHIP REQUIREMENTS

Only SCMS Manager Core members can join the SCMS Manager EAC. The types of membership in the SCMS Manager and the requirements for this are not described in this document. Refer to the SCMS Manager membership documentation for information regarding types of membership. The existing SCMS Manager Core members SHALL decide by majority about the membership of new Core members. Core members SHALL appoint an EAC Chair who SHALL act as a single point of contact for the EAC. An organization can only have one representative with decision making authority in the EAC. The organization can swap the representative. The appointment of the representative SHALL be made in written form at core member's organization management level. While rare, EAC members may be needed to respond to an urgent situation in a timely fashion. If the representative is going to be temporarily unavailable, the representative SHALL designate an alternate to serve during the absence.

2.2 EAC INTERACTIONS WITH THE ELECTORS

Any decision by the EAC to make modification to the CTL SHALL require a majority of the members to vote in the affirmative for the changes. The EAC SHALL then inform the Electors of its decision in a manner that provides assurance to the Electors that they are receiving an authentic and authorized request for those changes. The details of this procedure are described in the SCMS Electors Requirements document [under development – to be published in 2024].

© SCMS Manager LLC - All Rights Reserved

2.3 EAC CHAIRPERSON AND VICE CHAIRPERSON

The committee SHALL have a chairperson and a vice chairperson. The election of the chairperson and vice chairperson is to be voted on annually by the EAC, and can be re-elected.

The chairperson has the following responsibilities:

a. Presiding over EAC meetings,
b. Documenting meeting minutes and decisions
c. Providing leadership to the committee and ensuring focus on key tasks and responsibilities,
d. Responsible for the committee conducting audits (and tests of the Electors),
e. Ensuring proper information for the committee needed for decisions,
f. Carrying out elections, achieving committee decisions,
g. Acting as a Single Point of Contact (SPOC) for the EAC regarding communication with entities of the SCMS Manager ecosystem or a Service Provider.

The vice chairperson has the following responsibilities

a. To assist the chairperson as needed,
b. To be available for quick response if the chair is unavailable.

The duty of acting as a SPOC for communication of important information regarding the safe and secure operation of the SCMS Manager ecosystem requires a high availability and may require a short response time. It SHALL be ensured that the chairperson or the vice chairperson can be reached in the event of an urgent matter.

2.4 EAC RESPONSIBILITIES

2.4.1 ADD OR DELETE ELECTORS OR RCAS

The EAC SHALL have the responsibility to add or remove Electors and RCAs from the CTL.

Should an Elector or RCA be compromised, or some other situation or incident occur that has an adverse impact on the security and trustworthiness of the V2X ecosystem, the EAC SHALL have the authority to remove Electors and/or RCAs as it deems appropriate. The EAC also has the option to consider other approaches or measures that it deems appropriate in lieu of removal from the CTL.

To add an RCA to the CTL the EAC SHALL confirm that the requirements in SCMS Manager Provider Requirements have been met. To add an Elector to the CTL the EAC SHALL confirm that requirements in SCMS Manager Elector Requirements have been met.

As part of this confirmation process, the EAC SHALL ask the Policy Workgroup to determine the conformance of the Certificate Policy (CP) to the appropriate SCMS Manager requirements document based on the results and recommendations received from the PKI Auditor. Within one month of the request the Policy Workgroup SHALL submit a report to the EAC about the conformance of the CP. The EAC SHALL review this report as part of its decision about any additions to the CTL.

The EAC decision making process is described in section 2.5 below.

© SCMS Manager LLC - All Rights Reserved

Once the decision to add or remove an Elector or a SCMS Provider is made, the EAC Members SHALL inform the Electors of the decision. The process of informing the Electors, the Elector responses, and the EACs processing of the signed CTL are covered in SCMS Manager Certified Trust List (CTL) Update Process (under development).

2.4.2 COMPLIANCE VERIFICATION

The EAC SHALL verify annually that the Electors and RCAs continue to maintain their WebTrust compliance. If there are problems, the EAC has the responsibility to maintain the security and trustworthiness of the V2X ecosystem. The EAC SHALL determine the appropriate course of action, including the options of remediation or removal from the CTL.

2.4.3 APPROVAL OF SCMS MANAGER DOCUMENTS

The EAC approves requirement and policy documents, or their updates, published by SCMS Manager or used in is operation or governance. Changes may be made either by updating and publishing the entire document or by publishing a separate addendum. Subscribers and SCMS Manager members SHALL be notified by email and SHALL have a fifteen (15) day review period to provide any feedback on the amendments before the amended document is published. The amendments are effective upon publication. Along with the new document, the EAC SHALL publish a transition plan by which the changed requirements SHALL be implemented.

2.4.4 APPROVAL OF SUMMITTED DOCUMENTS

The EAC approves Certificate Policies summited by SCMS Service Providers and Electors. The EAC relies on input from the Policy Working Group to evaluate these Policies. The Policy Working Group also provides recommendations to the EAC regarding any audits performed. The EAC then uses this input to determine eligibility to be added to the CTL (or remain on the CTL).

2.5 EAC DECISION MAKING

All Decisions of the EAC are made by majority vote based on the number of EAC members. Each EAC member has one vote. If the EAC has an even number of members and the vote is split equally then the proposition does not pass.

The EAC chairperson is conducting the voting procedure.

Decisions to be voted on, at a minimum, include:

- To add or remove an Elector,
- To add or remove an RCA,
- To add or remove an EAC member,
- To approve a CP or CPS of a SCMS Provider,
- To approve a CP or CPS of an Elector,
- Approve changes of SCMS Manager Policies and Requirements documents or changes to it.

© SCMS Manager LLC - All Rights Reserved

2.6 EAC OPERATIONAL REQUIREMENTS

EAC members are expected to actively take part in the operations of the SCMS Manager and V2X ecosystem. If any EAC member misses more than three consecutive EAC meetings the EAC members SHALL decide on a removal of this EAC member. If any member is not taking part in a vote to add or remove an RCA or Elector, the EAC members SHALL also decide on a removal of this EAC member. The EAC is not required to remove a member for these reasons. Only to consider the matter and make a decision. For example, if the member is communicating the need for the absence in advance this may be a mitigating factor.

2.7 UPDATE OF THIS EAC REQUIREMENTS DOCUMENT

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

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

This EAC Requirements document SHALL be reviewed by the EAC at least every 3 years.

© SCMS Manager LLC - All Rights Reserved