SCMS MANAGER™
SECURITY CREDENTIAL MANAGEMENT SYSTEM

ELECTOR POLICY

VERSION 1.0

October 22, 2019

Author(s)

SCMS Manager Board of Directors

TABLE OF CONTENTS

SCMS MANAGER ELECTOR POLICY

1.0 ELECTOR POLICY OVERVIEW

The SCMS Manager is composed of representatives of public and private stakeholders (e.g. Vehicle Manufacturers, SCMS Component Vendors, Federal and State DOTs, etc.) interested in establishing and maintaining both the SCMS trust model and the security of the overall V2X ecosystem for the United States (possibly with association/extension to other North American areas). The SCMS Manager Board of Directors (BOD) manages the operations of the SCMS ecosystem and establishes the security requirements for the V2X ecosystem on behalf of the SCMS Manager members. The SCMS Manager BOD is the policy authority for SCMS operations and for the security elements of the national V2X ecosystem.

One aspect of overseeing the security of the V2X ecosystem is the management of Root CAs – specifically the ability to add and remove them as Trust Anchors of the ecosystem. The SCMS Manager will perform this function through the use of Electors. The Elector concept was originally envisaged by CAMP[1] and USDOT in their original development of the V2X SCMS framework. Electors are essentially offline CAs that implement the Ballots conducted by the SCMS Manager. A Ballot either adds or removes a Root CA or an Elector from the V2X ecosystem. Multiple Electors are used to provide a majority vote system such that any End Entity, upon receiving a Ballot signed by a number of Electors may, by determining majority vote of the Electors, determine if the identified Root CA or Elector should be added or removed from its list of trust anchors. Note that Electors themselves are managed by this same scheme in order to provide resiliency at this level of trust anchor.

In the context of Electors and Root CAs, the SCMS Manager BOD approves their policies and procedures and reviews annual audits of their operations. Should an Elector or Root CA be compromised or fail to pass its annual audit, the SCMS Manager BOD will revoke it. Similarly, the SCMS Manager BOD may add a new Root CA or Elector who has passed the Board's review process (defined elsewhere). To add or revoke an Elector or Root CA, the SCMS Manager BOD will issue the appropriate instruction in the form of a Ballot to the existing Elector group. These Electors will then sign the Ballot (i.e., vote) to confirm the SCMS Manager Board of Director's decision.

This SCMS Manager Elector Policy specifies how the decision to add or remove an Elector or Root CA will be made by the SCMS Manager BOD and it describes the policies and procedures that govern the Electors themselves.

1.1 SCMS MANAGER RESPONSIBILITIES

It is the responsibility of the SCMS Manager BOD 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.

It is the responsibility of the SCMS Manager BOD to authorize the Electors to execute the decisions of the SCMS Manager BOD.

[1] CAMP VSC5 – Collision Avoidance Metrics Partners LLC, Vehicle Safety Communications 5

The SCMS Manager BOD shall:

- Establish the number of Electors at five (5),
- Establish the initial set of Electors by affirmative vote of 75% of SCMS Manager BOD,
- Add or delete Electors or Root CAs by affirmative vote of 75% of the SCMS Manager BOD, based on the recommendations of the SCMS Manager Ecosystem Audit Committee and the SCMS Manager President,
- Notify Electors by email, telephone, and by overnight express delivery of a pending task,
- Document and publish on the SCMS Manager website all decisions and votes requiring action by the Electors,
- Have the authority to audit an Elector, with a minimum advance notice of 48 hours.
- Periodically initiate a test by providing a Ballot identified as a Test Ballot to be signed by all Electors. This test is intended to confirm that all Electors are responsive and functional. The BOD may initiate this test at any time at its discretion. The BOD shall not allow the Elector system to be unused for more than one (1) year.

2.0 ELECTORS

An Elector is a unique entity appointed by the SCMS Manager BOD to help ensure the integrity and security of the V2X ecosystem. The role of an Elector is to perform only those actions ordered by the SCMS Manager BOD. An Elector entity and its functions may be an independent organization or be part of an SCMS Manager member's organization.

In instances of any Elector being part of an SCMS Manager entity, it is recommended that the Board representative be separated from any department or persons managing Elector technology.

2.1 ELECTOR RESPONSIBILITIES

An Elector is responsible for:

2.1.1 Operation of the Elector according to this SCMS Manager Elector Policy
An Elector MUST operate in accordance to the responsibilities and requirements specified in this document. If there is ambiguity or lack of clarity, the Elector MUST contact the SCMS Manager BOD for further guidance.

2.1.2 Regular activity reports to SCMS Manager for the overall secure operation of Electors within the SCMS trust model
An Elector MUST provide a quarterly report to the SCMS Manager. This report shall contain a list of all actions performed by the Elector as well as any operational events (such as system updates, security tests and audits, system availability metrics) that occurred in the preceding quarter.

2.1.3 Creation and endorsement of a Root CA or Elector Ballot upon notification by the SCMS BOD
The primary purpose of Electors is to verify the set of valid Electors and Root CAs. As such, this list of valid Electors and Root CAs is managed by the SCMS Manager BOD. It is the responsibility of the Electors to create and endorse Elector and/or Root CA Ballots at the direction of the SCMS Manager BOD.

2.2 ELECTOR REQUIREMENTS

An Elector must adhere to the following requirements:

2.2.1 Document all actions in executing the task ordered by the SCMS Manager BOD
An Elector MUST maintain a permanent log of all task orders received and all actions performed on behalf of the SCMS Manager BOD. Each entry in the log shall have a timestamp and the signature of the person who performed an action. This log must be protected to ensure the integrity and authenticity of the log.

2.2.2 Only perform tasks as authorized and ordered by the SCMS Manager BOD

An Elector MUST only perform task orders requested by the SCMS Manager BOD. Under no circumstances will an Elector take unilateral action or take action at the request of another Elector or any other entity.

2.2.3 Verify all task orders

An Elector MUST validate all task orders to confirm authenticity. An Elector will confirm, via telephone or email, each task order received with at least two members of the SCMS Manager BOD. The validation of task orders MUST be documented in the permanent log.

2.2.4 Perform a "removal task" within 24 hours

A task order to remove an Elector or Root CA MUST be verified and MUST be executed within as little as 48 hours of receipt of the task order. The task order will state the required response time. The removal of a Root CA is a critical, time-sensitive action and MUST receive the highest priority.

2.2.5 Perform an "addition task" within 5 business days

A task order to add an Elector or Root CA MUST be verified and MUST be performed within a maximum of 5 business days of receipt of the task order. The task order will state the required response time.

2.2.6 Submit Elector functional design and hardware specification to the SCMS Manager BOD for approval

The SCMS Manager will publish periodically guidance for the creation and operation of an Elector. A candidate for Elector MUST submit its functional design and hardware specifications showing conformance to this guidance to the SCMS Manager BOD for approval. Any proposed material changes to an established Elector MUST be submitted to the SCMS Manager BOD for approval.

2.2.7 Be designed with disaster recovery

The design of an Elector must allow for recovery from a wide variety of system failures, including physical destruction. The Elector MUST demonstrate to the SCMS Manager BOD a system design that allows for proper system recovery in the event of system or component failure. It is critical that an Elector can return to an operational state after any sort of failure within two calendar weeks from the date of the failure.

2.2.8 Utilize a FIPS 140-2 L3 HSM

It is critical that an Elector protect its cryptographic material in a physical security module. To that end, an Elector MUST utilize a US Government FIPS 140-2 Level 3 certified Hardware Security Module (HSM). This will provide both tamper-evident physical security as well as protection of critical security parameters.

2.2.9 Provide its Certificate to SCMS Manager BOD

Once it generates its Ballot Signature Key Pair, an Elector MUST provide its certificate to the SCMS Manager BOD for SCMS Manager to publish and distribute to End Entity Suppliers for inclusion in their products. SCMS Manager shall confirm by at least telephone and email that it has received the correct certificate from the Elector.

2.2.10 Perform Elector operations in an off-line (no network connections) posture

In order to minimize the possibility of remote security attacks of an Elector, an Elector MUST not have network connectivity at any time. An Elector MUST be powered off and securely stored when not in use and when unattended. Only when it needs to perform a task should the Elector be powered on.

2.2.11 Provide Elector Certificate Policy (CP) and Elector Certification Practices Statement (CPS) to the SCMS Manager BOD

An Elector MUST provide a Certificate Policy and Certification Practices Statement to the SCMS Manager BOD for approval. An Elector MUST cooperate with the SCMS Manager BOD to adjust and update the CP and CPS as necessary.

2.2.12 Attain WebTrust certification

An Elector MUST acquire WebTrust certification, specifically WebTrust for CA v2.1 certification (or then current version). WebTrust for Certification Authorities is the de facto certification used throughout the internet for PKI technologies.

2.2.13 Pass annual WebTrust audits

An Elector MUST maintain its WebTrust certification. To that end, it must pass an annual WebTrust audit. The Elector shall authorize its WebTrust auditor to communicate the results of the annual audit directly with the SCMS Manager BOD. Such results shall be communicated to the SCMS Manager BOD within 72 hours of the audit report completion by the auditor.

2.2.14 Allow the SCMS Manager BOD to perform an on-demand audit

An Elector MUST allow the SCMS Manager BOD to perform an on-demand audit of the Elector using a mutually agreed auditor. The auditor shall be agreed upon when the Elector begins service to SCMS Manager. The auditor may be changed annually after the completion of an audit. The Elector will help facilitate and assist in performance of an on-demand audit. The SCMS Manager BOD MUST provide at least 48-hours notice prior to an audit. Each party shall bear their respective costs for such an audit.

2.3 ELECTOR CONFIGURATION

2.3.1 Elector Certificate validity

By default, an Elector certificate shall be valid for 15 years.

The first 5 Electors' validity shall be staggered by 3 years, and these Electors shall be initially valid for 12, 15, 18, 21 and 24 years. All additional Electors should coordinate with the SCMS Manager BOD to ensure proper spacing of validity periods to avoid multiple Elector certificates expiring in the same year.

2.4 ELECTOR OPERATIONS

This section specifies the workflow for Elector operations.

2.4.1 REMOVING AN ELECTOR

- SCMS Manager BOD is made aware of the need to remove *Elector X*.
- Upon an event causing the SCMS Manager BOD to investigate an Elector, if 75% or more members of the SCMS Manager BOD vote for removal, then the SCMS Manager BOD issues a Ballot to all Electors to remove *Elector X*.
- The SCMS Manager BOD will specify a "response time" along with the Ballot. Upon receiving a Ballot, an Elector must complete within this response time the following steps for verifying, signing, and returning a removal Ballot:
    - Elector adds to its audit log, the receipt of Ballot to remove *Elector X*.
    - Elector confirms the directive and Ballot contents to remove *Elector X* by contacting at least two members of the SCMS Manager BOD for verification.
    - Elector adds to its audit log, who, how and when, the directive was verified.
    - Once verified, Elector signs Ballot to revoke *Elector X*.
    - Elector adds to its audit log a copy of the Signed Ballot.
    - Elector returns the Signed Ballot to the SCMS Manager BOD.
    - SCMS Manager BOD sends the Elector a notice of receipt of the Signed Ballot.
    - Elector adds to its audit log, the receipt from the SCMS Manager BOD.
- The BOD collects the Signed Ballots from the Electors.
- When a quorum is reached, the SCMS Manager BOD generates an *Elector Remove* message for *Elector X* that contains the sequence of Elector signatures endorsing the removal of *Elector X*.
- The BOD then furnishes the endorsed *Elector Remove* message to the authorized Root CA Operators and Misbehavior Authority Operator to publish in their respective Global Policy File via the Global Certificate Chain File (GCCF), and the CRL Generator (CRLG).

2.4.2 ADDING AN ELECTOR

- SCMS Manager BOD is made aware of the need to add *Elector X*.
- Within 10 business days, the BOD reviews and, if warranted, votes to add *Elector X*.
- If 75% or more members of the BOD vote to add *Elector X*, then BOD issues a Ballot containing the self-signed certificate from *Elector X* to all currently valid Electors

- Per the task order, an Elector has up to 5 business days to complete the following steps for verifying, signing, and returning an *Elector Add* Ballot:
    - Elector adds to its audit log, the receipt of Ballot to add *Elector X*.
    - Elector confirms the directive to add *Elector X* by contacting at least two members of the BOD for verification.
    - Elector adds to its audit log, who, how and when, the directive was verified.
    - Once verified, Elector signs Ballot to endorse *Elector X*.
    - Elector adds to its audit log, a copy of the Signed Ballot.
    - Elector returns the Signed Ballot to the BOD.
    - The BOD sends the Elector a notice of receipt of the Signed Ballot.
    - Elector adds to its audit log, the receipt from the BOD.
- The BOD collects the Signed Ballots from the Electors.
- When all Electors have returned their Signed Ballots, the BOD generates an *Elector Add* message for new *Elector X* that contains the sequence of Elector signatures that endorse adding *Elector X*.
- The BOD then furnishes the endorsed *Elector Add* message and the self-signed Elector certificate to the authorized Root CA Operators and Misbehavior Authority Operator to publish in their respective Global Policy File via the Global Certificate Chain File (GCCF).

2.4.4 REMOVING A ROOT CA

- SCMS Manager BOD is made aware of the need to remove *RCA X*.
- Within 24 hours, the BOD investigates and, if warranted, votes to remove *RCA X*.
- If 75% or more members of the BOD vote for removal, then BOD issues a Ballot to all Electors to remove *RCA X*.
- Pe the task order, an Elector has a minimum of 48 hours to complete the following steps for verifying, signing, and returning a removal Ballot:
    - Elector adds to its audit log, the receipt of Ballot to remove *RCA X*.
    - Elector confirms the directive to remove *RCA X* by contacting at least two members of the BOD for verification.
    - Elector adds to its audit log, who, how and when, the directive was verified.
    - Once verified, Elector signs Ballot to revoke *RCA X*.
    - Elector adds to its audit log, a copy of the Signed Ballot.
    - Elector returns the Signed Ballot to the BOD.
    - BOD sends the Elector a notice of receipt of the Signed Ballot.
    - Elector adds to its audit log, the receipt from the BOD.
- The BOD collects the Signed Ballots from the Electors.
- When a quorum is reached, the BOD generates an *RCA Remove* message for *RCA X* that contains the sequence of Elector signatures endorsing the removal of *RCA X*.
- The BOD then furnishes the endorsed *RCA Remove* message to the authorized Root CA Operators and Misbehavior Authority Operator to publish in their respective Global Policy File via the Global Certificate Chain File (GCCF), and the CRL Generator (CRLG).

2.4.5 ADDING A ROOT CA

- SCMS Manager BOD is made aware of the need to add *RCA X*.
- Within 10 business days, the BOD reviews and, if warranted, votes to add *RCA X*.
- If 75% or more members of the BOD vote to add *RCA X*, then BOD issues a Ballot containing the self-signed certificate from *RCA X* to all currently valid Electors
- Per the task order, an Elector has up to 5 business days to complete the following steps for verifying, signing, and returning an *RCA Add* Ballot:
    - Elector adds to its audit log, the receipt of Ballot to add *RCA X*.
    - Elector confirms the directive to add *RCA X* by contacting at least two members of the BOD for verification.
    - Elector adds to its audit log, who, how and when, the directive was verified.
    - Once verified, Elector signs Ballot to endorse *RCA X*.
    - Elector adds to its audit log, a copy of the Signed Ballot.
    - Elector returns the newly Signed Ballot to the BOD.
    - The BOD sends the Elector a notice of receipt of the Signed Ballot.
    - Elector adds to its audit log, the receipt from the BOD.
- The BOD collects the Signed Ballots from the Electors.
- When all Electors have returned their Signed Ballots, the BOD generates an *RCA Add* message for new *RCA X* that contains the sequence of Elector signatures that endorse adding *RCA X*.
- The BOD then furnishes the endorsed *RCA Add* message and the self-signed Root CA certificate to the Root CA Operators and Misbehavior Authority Operator to publish in their respective Global Policy File via the Global Certificate Chain File (GCCF).

3.0 ACCREDITED PKI AUDITOR

An acceptable PKI Auditor SHALL be accredited to perform WebTrust audits (hereafter "Accredited PKI Auditor")

An Accredited PKI Auditor is responsible for:

- performing audits of an Elector
- assessing compliance of the Elector to this Elector Policy
- providing an audit report (related to either an initial or periodic audit) to the BOD according to the requirements defined in this Elector Policy
- notifying to the entity managing the Elector on the successful or unsuccessful execution of an audit

An Elector Audit shall consist of:

- WebTrust for CAs v2.1 (or then current version)

An Elector Audit Report shall include:

- Compliance with this Elector Policy
- Confirmation of correct logs of all activities/actions undertaken by Elector since last audit
- Compliance to WebTrust for CAs v2.1 (or then current version)

4.0 ELECTOR FEES

The SCMS Manager BOD periodically may establish payments to Electors for their operation. Electors shall not charge fees for their services other than those established by SCMS Manager.