SCMS Manager Intersection Validation and Certificate Issuance Policy

SCMS Manager

January 13, 2025

Contents

1 Executive Summary

This policy establishes the requirements and procedures for validating connected intersections and issuing digital certificates through the Security Credential Management System (SCMS). It ensures the accuracy and reliability of broadcast messages from connected intersections to support vehicle safety applications through validation procedures and continuous monitoring.

2 Introduction

2.1 Purpose

Successful connected intersection deployment and operation depends on trust among production vehicles and a variety of transportation infrastructure. The SCMS architecture supports trust by providing a collection of trusted root certificates operated by authorized vendors who agree to implement a common set of policies. Security infrastructure alone can only provide assurance for the integrity of broadcast messages as they travel from a sender to a collection of receivers. Assurance that the data content of those messages is consistently accurate and aligned with physical signals and signage requires validation.

2.2 Scope

This document describes the role of the SCMS Manager in the implementation and enforcement of validated intersections. SCMS Providers which are authorized by the SCMS Manager to issue certificates to V2X stations must support the intersection validation procedures defined in this policy if they intend to issue credentials for validated intersections.

2.3 Definitions and Acronyms

- CAMP: Crash Avoidance Metrics Partnership
- CSI: Connected Signalized Intersection
- CIMMS: Connected Intersections Message Monitoring System
- CVPFS: Connected Vehicle Pooled Fund Study
- IOO: Infrastructure Owner Operator
- OSCAL: Open Security Controls Assessment Language
- PSID: Provider Service Identifier
- RSU: Roadside Unit
- RTCM: Radio Technology Commission for Maritime Services
- RLVS: Red Light Violation Warning
- SCMS: Security Credential Management System
- SPaT: Signal, Phase, and Timing
- SSP: Service-Specific Permissions
- V2X: Vehicle-to-Everything

3 Roles and Responsibilities

The following sections define specific roles and responsibilities for SCMS Manager, individual SCMS Providers, IOOs, continuous monitoring, and certification functions. Note that some of these roles may be combined in a single entity. For example, an IOO may be approved to self-certify their own systems or to operate their own continuous monitoring technology. When roles are combined, the implementer must take on the requirements and responsibilities for all combined roles.

3.1 SCMS Manager

The SCMS Manager is responsible for:

- Establishing and maintaining validation and certificate issuance policies
- Authorizing SCMS Providers to issue certificates for validated intersections
- Defining required message formats and validation criteria
- Approving certification requirements for testing tools and labs
- Maintaining a registry of certified testing organizations and tools
- Reviewing and updating policies based on operational experience
- Coordinating with standards organizations on message specifications
- Mediating disputes between stakeholders regarding validation status
- Publishing technical bulletins and policy clarifications as needed

3.2 SCMS Providers

SCMS Providers authorized by the SCMS Manager must:

- Evaluate enrollment requests for RSUs intended for validated operation
- Issue enrollment certificates with appropriate Service-Specific Permissions
- Review and verify validation reports from certified testing organizations
- Issue application certificates with appropriate validation flags
- Monitor continuous operation reports from validated intersections
- Maintain records of validation status for enrolled RSUs
- Notify IOOs of validation issues or missing reports
- Implement certificate blocking or revocation when required
- Report significant validation issues to the SCMS Manager
- Maintain secure systems for certificate management and report storage

3.3 Infrastructure Owner Operators (IOOs)

IOOs operating validated intersections are responsible for:

- Ensuring RSUs are properly enrolled with an authorized SCMS Provider
- Contracting with certified testing organizations or maintaining certified testing capabilities
- Conducting initial validation testing using certified tools
- Implementing continuous monitoring systems
- Maintaining intersection operation within validated parameters
- Submitting required reports according to established schedules
- Responding to validation issues identified by monitoring systems
- Conducting or arranging annual on-site inspections
- Maintaining accurate records of intersection configuration and changes
- Notifying SCMS Provider of any significant operational changes
- Ensuring staff are properly trained on validation requirements

3.4 Testing Organizations

Certified testing organizations must:

- Maintain certification from approved certification bodies
- Use only certified testing tools and procedures
- Conduct validation testing according to established procedures
- Generate complete and accurate validation reports
- Submit reports directly to designated SCMS Providers
- Maintain calibration and verification of testing equipment
- Report any testing irregularities to IOOs and SCMS Providers
- Maintain qualified staff and training programs
- Participate in industry working groups on testing procedures
- Maintain independence from intersection operators

3.5 Continuous Monitoring Service Providers

Organizations providing continuous monitoring services must:

- Maintain certification for monitoring systems and tools
- Implement automated data collection and analysis
- Generate weekly monitoring reports for SCMS Providers
- Implement immediate notification of out-of-specification conditions
- Maintain secure communication with RSUs and SCMS Providers
- Archive monitoring data according to retention requirements
- Support investigation of validation issues
- Maintain system availability according to service level agreements
- Implement data quality checks and validation
- Provide technical support to IOOs for monitoring system operation

3.6 Certification Bodies

Organizations certifying testing tools and organizations must:

- Develop and maintain certification criteria
- Evaluate testing organizations and tools
- Issue and maintain certifications
- Conduct periodic audits of certified entities
- Investigate certification compliance issues
- Report certification status to the SCMS Manager
- Maintain public registry of certified entities
- Coordinate with industry on certification requirements
- Process certification appeals
- Provide technical guidance on certification requirements

4 Connected Intersection Requirements

4.1 System Components

A signalized intersection consists of a collection of equipment and traffic control signals that safely coordinates the flow of traffic through a shared segment of roadway. A connected signalized intersection (CSI) is an infrastructure system that broadcasts:

- Signal, Phase, and Timing (SPaT)
- Lane level location information (MAP)
- Radio Technology Commission for Maritime Services (RTCM) GPS position correction data

4.2 Operational States

An intersection may operate in one of two states:

- **Validated**: A CSI that has passed the required validation tests
- **Unvalidated**: Any CSI that has not been tested or that has failed a validation test

4.3 Message Requirements

A CSI must broadcast SPaT, MAP, and RTCM as defined in SAE J2735, “V2X Communications Message Set Dictionary” to support specific safety applications such as Red Light Violation Warning (RLVW).

Two indicators are used to identify the validation state of an intersection:

1. The RSU that signs and broadcasts the SPaT data associated with the intersection shall include an SSP that identifies the intersection as having `validation_supported`. The specific bit field used to

define this SPaT has not yet been standardized. Details on the chosen SSP value will be included in a security profile published in a future version of the SAE SPaT definition.

2. The SPaT data content shall set a bit in the ASN.1 structure indicating that it is operating in `validated_mode`.

The recommended method for signaling `validated_mode` is to re-purpose a bit that is currently defined in SAE-J2735 as part of the `IntersectionStatusObject`. This object has a bit string that can be used to describe specific features of the signal. Bit 13 is currently defined as `noValidSPATisAvailableAtThisTime` which is described as describing a state where the "SPAT system is not working at this time". It is recommended that this bit be re-defined and interpreted as`inValidatedMode`. This interpretation supports backwards compatibility. Legacy systems operating with this bit set to 0 can continue to operate without causing any confusion. Only systems with this bet enabled (set to a value of 1) will indicate that they are operating in validated mode.

4.4 Message Body Content

The use of two methods of defining intersection validation status requires careful interpretation. The following table defines the potential operating modes for any connected intersection.

SSP Content	Message Body	Meaning
`validation_supported` present	`validated_mode` present	message content validated
`validation_supported` present	`validated_mode` absent	message content not validated
`validation_supported` absent	`validated_mode` absent	message content not validated
`validation_supported` absent	`validated_mode` present	misbehavior

5 Validation Process

5.1 Initial Validation

Initial validation measurements must be collected using a Certified test tool or Certified lab with the following requirements:

- Certification to be issued by independent review (OmniAir or other)
- DOT can use a certified tool to collect data on their own intersections (self-validation)
- DOT can contract with a certified lab (third-party validation)
- Reports must be submitted directly from the certified tool or lab to an SCMS Provider
- A validated intersection must use a certified RSU
- Initial validation metrics must include all operational modes
- All validated intersections must be independently tested

5.2 Continuous Monitoring

Requirements for continuous monitoring include:

- Must use a Certified utility to maintain validation
- Continuous monitoring equipment must be type Certified by a lab
- Can trigger an immediate change of state when out of specification
- Response time to switch to standby must be < 10 seconds
- Weekly reports must be submitted to SCMS provider
- Absence of scheduled reports will trigger SCMS provider notification to DOT
- Failure to correct report delivery will cause SCMS provider to block the impacted RSU

5.3 Manual Inspections

Manual inspection requirements include:

- Physical inspection at least once per-year
- Minimally-invasive set of measurements
- Validation of RSU broadcasts
- Visual inspection of signal head operation
- Validation of MAP data through driving tests

IOOs are required to perform a physical inspection of each CSI system at least once per-year. This inspection may be integrated with other annual or routine maintenance operations. If any inconsistencies are observed during the periodic inspection, the IOO must inform the SCMS Provider and initiate corrective action. The intersection shall be switched out of `validated_mode` until the issue has been resolved.

5.4 Report Types

Three types of reports are required:

1. Initial validation report (one-time or as-needed)
   - Validate SPaT accuracy + latency, MAP data accuracy, and RTCM performance
2. Continuous monitoring update (weekly)
   - Capture BSMs from vehicles as they drive through the intersection
   - Analysis shows how human drivers respond to traffic signal changes
3. On-site inspection (annual or as-needed)
   - Confirm system operation
   - Update roadway or signal controller data

6 Certificate Management

6.1 Certificate Issuance Process

Process for installing a new validated RSU:

1. RSU vendor enrolls device with SCMS Provider requesting validated SSP flags
2. SCMS Provider issues enrollment certificate with requested SSP
3. Initial application certificate issued with validation flag set to 0
4. RSU broadcasts signed messages without validation bit set
5. After validation report acceptance, SCMS Provider enables validation flag
6. New application certificate issued with validation bit enabled
7. RSU begins broadcasting with validated flag

7 Operational Requirements

The following sections define operational requirements for critical functions of a CSI system.

7.1 Message Broadcasting

General requirements for message broadcast:

- RSUs must broadcast SPaT, MAP, and RTCM messages continuously during operation
- Message content must accurately reflect current intersection state
- All broadcast messages must be properly signed with valid certificates
- Message format must conform to SAE J2735 standards
- Broadcast frequency must meet minimum requirements for each message type:
  - SPaT: Minimum 10 Hz

  - MAP: Minimum 1 Hz
  - RTCM: Minimum 1 Hz

Validation status requirements:

- RSUs must only broadcast messages with validation flags when authorized
- Validation status must be immediately updated if monitoring detects issues
- Status changes must be logged and reported to the SCMS Provider
- Recovery from unvalidated status requires following the full validation procedure

7.2 Performance Monitoring

Real-time Monitoring:

- Continuous monitoring system must be operational 24/7
- System must verify:
  - Message timing and frequency
  - Signal state accuracy
  - Position accuracy
  - Message integrity
  - Certificate validity
- Performance metrics must be logged at minimum 1-minute intervals
- Out-of-specification conditions must trigger immediate alerts

Response Requirements:

- RSU must transition to standby mode within 10 seconds of detecting critical issues
- IOO must acknowledge system alerts within 1 hour
- IOO must begin investigation of issues within 4 hours
- Resolution plans must be documented within 24 hours
- SCMS Provider must be notified of any unresolved issues within 48 hours

7.3 Status Changes

Planned Changes:

- IOO must notify SCMS Provider 7 days before planned maintenance
- Configuration changes require validation testing before implementation
- Firmware updates must be tested in non-production environment
- Status changes must be coordinated with affected stakeholders
- Return to service requires verification of all operational parameters

Unplanned Changes:

- Emergency maintenance must be logged and reported within 24 hours
- Temporary configurations must be documented and reviewed
- Recovery procedures must be followed before returning to service
- Root cause analysis required for unexpected failures
- Corrective action plans must be developed and implemented

7.4 Incident Response

Security Incidents:

- Suspected security breaches must be reported immediately
- RSU must be placed in standby mode during investigation
- SCMS Provider must be notified within 1 hour
- Incident response team must be activated
- Evidence must be preserved for investigation

Performance Incidents:

- Performance degradation must trigger investigation
- Backup systems must be activated if available
- Users must be notified of reduced capability
- Recovery plans must be documented and followed
- Post-incident review required for systemic issues

7.5 Maintenance and Updates

Scheduled Maintenance:

- Preventive maintenance schedule must be established
- Equipment calibration must be maintained
- Software updates must follow change management procedures
- Testing must be performed after maintenance
- Documentation must be updated to reflect changes

Equipment Requirements:

- Spare parts inventory must be maintained
- Test equipment must be calibrated and certified
- Backup power systems must be tested monthly
- Environmental controls must be maintained
- Physical security must be regularly verified

8 Policy Administration

8.1 Policy Updates

The SCMS Manager maintains this policy as a living document that must evolve to meet the changing needs of the connected vehicle ecosystem. Policy updates follow a structured process designed to ensure all stakeholders have input while maintaining the integrity of the validation system.

Major policy revisions occur annually, with the review process beginning in January of each year. The SCMS Manager will distribute proposed changes to all affected parties and allow a 60-day comment period. During this time, stakeholders may submit feedback, concerns, and suggested modifications through the SCMS Manager's policy portal.

Minor revisions may be implemented throughout the year through technical bulletins. These bulletins provide clarification, interpretation guidance, or temporary modifications to address urgent operational needs. Technical bulletins remain in effect until incorporated into the main policy document during the next major revision cycle.

Emergency changes may be implemented immediately if required to address critical security or safety concerns. In such cases, the SCMS Manager will notify all affected parties within 24 hours and provide detailed justification for the emergency action.

8.2 Transition Procedures

When policy changes affect operational requirements, the SCMS Manager will establish appropriate transition periods to allow stakeholders to achieve compliance. Transition periods are determined based on the complexity of required changes, potential operational impacts, and resource requirements for implementation.

The transition process typically includes three phases. During the preparation phase, stakeholders review new requirements and develop implementation plans. The implementation phase provides time for system modifications, testing, and validation. The verification phase confirms that all changes meet new policy requirements before the transition deadline.

For major changes affecting multiple stakeholders, the SCMS Manager may establish working groups to coordinate transition activities and share implementation experiences. These working groups help identify common challenges and develop consistent solutions across the ecosystem.

8.3 Waivers and Exceptions

The SCMS Manager recognizes that unique operational circumstances may occasionally require policy exceptions. A formal waiver process allows Infrastructure Owner Operators to request temporary relief from specific policy requirements when strict compliance is not immediately achievable.

Waiver requests must include detailed justification, risk assessment, and mitigation plans. The SCMS Manager will evaluate each request based on its technical merit, potential impact on system security and safety, and proposed risk controls. Approved waivers include specific conditions and expiration dates, typically not exceeding six months.

Permanent exceptions are rarely granted and require extensive documentation and ongoing oversight. These exceptions must demonstrate alternative methods for achieving the policy's security and safety objectives while maintaining system integrity.

8.4 Policy Interpretation

Questions regarding policy interpretation should be directed to the SCMS Manager's Policy Office. This office provides authoritative guidance on policy implementation and maintains a database of previous interpretations to ensure consistent application across the ecosystem.

When new situations arise that aren't clearly addressed by existing policy, the Policy Office will issue interpretation guidance. This guidance becomes part of the official policy record and may be incorporated into future policy updates as appropriate.

8.5 Documentation Standards

All policy-related documentation must follow standardized formats and use consistent terminology. The SCMS Manager maintains templates for common documents including waiver requests, implementation plans, and compliance reports. These templates ensure that necessary information is captured consistently and can be processed efficiently.

Document retention requirements vary by type but generally align with intersection lifecycle phases. Policy versions, technical bulletins, and interpretation guidance must be maintained for the operational life of affected intersections plus three years.

A Day 1 Deployment

This validation policy was developed with an understanding that there will be a two-phase deployment process. A "Day 1" deployment will be possible without requiring changes to message types or existing devices software. A future "Day 2" scenario will enable higher confidence in validated intersection data, but will require more time for deployment.

The key difference is the presence of a fast feedback loop from continuous monitoring to the RSU that signs and broadcasts SPaT data for a validated intersection. Under a "Day 1" scenario, it is assumed that an existing RSU was developed with no knowledge of a requirement for continuous monitoring or the need to switch the proposed bit to indicate `validation_enabled`. In this scenario, the selected bit will need to be manually configured to be forced into the set state (value of 1). Once this is done, there will be no automatic or rapid way to clear this big. Under this scenario, the only effective way to switch an intersection out of the validated mode is to issue new application certificates with the required SSP bit removed. This is a slow process as each RSU typically pre-loads certificates for 1 week into the future. Therefore, the switch out of validated mode may take up to 2 weeks in the worst case.

This “Day 1” scenario represents a temporary situation. Once the relevant standards are updated and RSU vendors make the required software changes, it will be possible for continuous monitoring systems such as CIMMS to be able to communicate directly with the RSU responsible for each connected intersection. In this future or “Day 2” scenario, it will be possible for intersections to rapidly switch out of validated mode. See the supplemental document “SCMS Manager Intersection Validation Misbehavior Management” for additional details on how an RSU may switch out of validated mode and be brought back to validation status.

B CIMMS for Continuous Monitoring

The current recommended method of performing continuous monitoring is to use the Connected Intersections Message Monitoring System (CIMMS) tool, developed as part of the Connected Vehicle Pooled Fund Study (CVPFS). This monitoring system collects Basic Safety Message (BSM) data from vehicles as they drive through a connected intersection. It also monitors the SPaT, MAP, and RTCM data broadcast by the intersection RSU. Statistical analysis is used to detect potential discrepancies between actual driver behavior and the reported signal state or lane marking information in the broadcast messages.

Refer to the report titled “SCMS Manager Intersection Validation Misbehavior Management” for more details on how CIMMS can be used for monitoring. This report describes the operating modes of a CI system and evaluates the impact of the 8 alert types that can be produced by the current version of CIMMS. It also introduces a basic model for estimating the number of events that can be expected at a connected intersection.

C CTI4501 Security Policy Profile

The “Connected Intersections Implementation Guide”, published by ITE as CTI4501, provides technical guidance for IOOs who operate CSI systems. This document includes fairly extensive recommendations for configuring and maintaining the integrity and security of the complete CSI System. All of these recommendations are valuable and relevant for the safe operation of a CSI System.

The supplementary document titled “CTI4501 Security Policy Profile” provides specific guidance on how to prioritize specific sections of the CTI4501 security recommendations when establishing a new CSI system. It specifically identifies the new security and operational requirements needed to safely operate a CSI system that includes at least one RSU and a conventional traffic controller. This document adopts the view that many IOOs have well established method of protecting their traditional traffic control infrastructure. As they add RSUs to these traffic cabinets to create CSI systems, they take on new risks that may not be addressed by their existing policies and procedures. The “CTI4501 Security Policy Profile” document identifies these specific changes and provides guidance for new deployments of validated intersections with an RSU.

D CI Test Results Report Format

A consistent and well structured machine readable report format can make the process of submitting test results to an SCMS provider much more efficient. This is critical if validated intersections will be deployed at scale. The supplementary document “CI Test Results Report Format, Version 0.8” defines a technical report format based on OSCAL, the Open Security Controls Assessment Language. This document defines a specific workflow for generating and submitting a validation report to an SCMS provider. A sample report that delivers SPaT validation metrics is included as an example. Additional details on MAP validation results as well as results from future test procedures to validation RTCM message content will be added in a future version of this document.