Connected Vehicle Deployment Technical Assistance

Procurement Considerations for Security Credential Management System (SCMS) for a Connected Vehicle System Acquisition

www.its.dot.gov/index.htm

Final Report — May 2021
FHWA-JPO-21-862

U.S. Department of Transportation

Produced by Noblis, Inc.
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
ITS Joint Program Office

Notice

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-21-862		

4. Title and Subtitle	5. Report Date
Connected Vehicle Deployment Technical Assistance: Procurement Considerations for Security Credential Management System (SCMS) for a Connected Vehicle System Acquisition	May 2021
	6. Performing Organization Code
7. Author(s)	**8. Performing Organization Report No.**
9. Performing Organization Name And Address Noblis 500 L'Enfant Plaza, SW, Suite 900 Washington, DC 20024	**10. Work Unit No. (TRAIS)** **11. Contract or Grant No.** DTFH61-16-D-00036
12. Sponsoring Agency Name and Address ITS-Joint Program Office 1200 New Jersey Avenue, S.E. Washington, DC 20590	**13. Type of Report and Period Covered** Final Report **14. Sponsoring Agency Code** HOIT-1

15. Supplementary Notes

Michelle Noch (TOCOR)

16. Abstract

This document is intended to assist project managers who are planning deployment of connected vehicle (CV) systems in the procurement of Security Credential Management System (SCMS) services. A SCMS is a critical component of a connected vehicle environment serving as a message security solution for Vehicle-to-Everything (V2X). The content in this resource document is based on other early deployers' experiences with the procurement and use of a SCMS for CV. The objective of this document is to share these experiences to help other projects understand and ask relevant questions. As projects are often oriented toward CV deployment and not SCMS by itself, there can be a gap in understanding how SCMS should be treated within the project, and this resource aims to help fill this gap. It builds upon the SCMS technical primer and presents project managers and their teams with considerations that will help make choices in the early stages of a project relating to procuring SCMS services. This may be in the form of asking informed questions or better understanding the work of supporting consultants - the guide is not intended to provide a definitive technical or official procurement specification.

17. Key Words	18. Distribution Statement
Security Credential Management System (SCMS), Connected Vehicles (CV), V2X, Certificates, Procurement	

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	14	

Table of Contents

List of Tables

List of Figures

Introduction

This document is intended to assist project managers who are planning deployment of connected vehicle (CV) systems in the procurement of Security Credential Management System (SCMS) services. A SCMS is a critical component of a connected vehicle environment serving as a message security solution for Vehicle-to-Everything (V2X). It uses a Public Key Infrastructure (PKI)-based approach that employs specialized methods of encryption and certificate management to facilitate trusted communication while preserving individual privacy. The SCMS also plays a key function in protecting the content of each message by identifying and removing misbehaving devices, while still maintaining privacy for individuals. An introduction to the SCMS function is available in the Security Credential Management System (SCMS) Technical Primer (https://www.pcb.its.dot.gov/documents/SCMS_Primer.pdf) and readers of this document who are not familiar with SCMS should review the technical primer first.

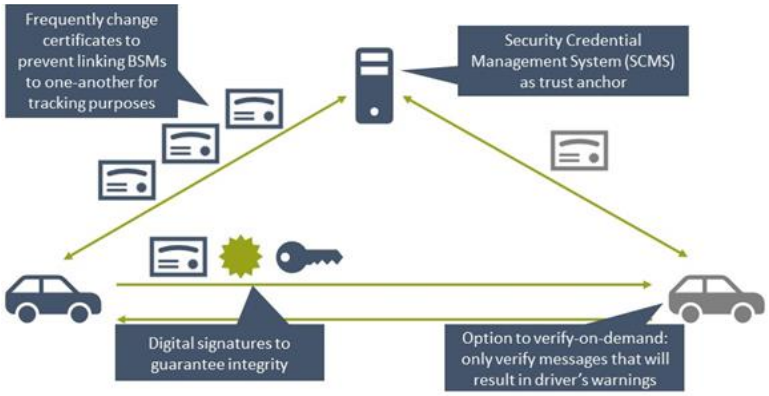
The content in this resource document is based on other early deployers' experiences with the procurement and use of a SCMS for CV. The objective of this document is to share these experiences to help other projects understand and ask relevant questions. As projects are often oriented toward CV deployment and not SCMS by itself, there can be a gap in understanding how SCMS should be treated within the project, and this resource aims to help fill this gap. It builds upon the SCMS technical primer and presents project managers and their teams with considerations that will help make choices in the early stages of a project relating to procuring SCMS services. This may be in the form of asking informed questions or better understanding the work of supporting consultants - the guide is not intended to provide a definitive technical or official procurement specification.

The sections below provide considerations that the project manager and supporting team should understand and use as a resource as procurement documents are developed;. they are not a definitive or all-encompassing set of requirements for the procurement of a SCMS. It is critical for technical staff and procurement staff to work collaboratively at an early stage when determining the appropriate procurement method and mechanism, as well as developing a scope for this type of system. Since the connected vehicle environment, including SCMS, continues to evolve over time, this may include external engagement (such as with public agency CV working groups, subject matter experts, and peers) to ensure an up-to-date understanding of the current connected vehicle environment prior to developing procurement documents. Given the dynamic maturity levels with the CV environment, procurement officers will need supporting expertise for a successful procurement that can adapt to changes in the technology being procured.

1.1 Connected Vehicles and the Role of the Security Credential Management System

In a connected vehicle environment, SCMS provides several key supporting functions to enable sustained field operation (outside of a research or testing environment):

- **Interoperability across Devices and Deployments:** For connected vehicle devices to trust messages received from other devices, there needs to be a mechanism to ensure that messages are from a legitimate source that follows a shared set of criteria and operating assumptions, reflected in key connected vehicle interfaces and standards. In a closed environment, a variety of methods may be possible, but since vehicles can travel to other jurisdictions and deployment areas, a common interoperable solution is needed. The SCMS enables devices to take a received message from an unaffiliated OBU or RSU, and verify that a trusted actor (the SCMS provider) can digitally attest that the source, has followed a set of common policies, guidelines and procedures, as defined by standards and specifications. This trust capability is essential to allow V2V and V2I applications to function, as applications cannot rely upon untrusted data.



Source: USDOT, 2019

Figure 1. The SCMS Ecosystem

- **"Privacy by Design":** At the same time, a key goal of the SCMS is to protect the privacy of end users. To maintain privacy against attackers from outside the SCMS, certificates need to change (e.g., every X minutes). Another key requirement is that attacks should be difficult to mount for SCMS insiders. Thus, the SCMS operations are divided among different components, and those components are required to have organizational separation between them.
- **Misbehavior Detection and Revocation:** Misbehavior Detection is the process for identifying devices that send messages that could cause malicious events within the connected vehicle environment. There is a current minimum viable misbehavior detection capability that exists and utilizes basic algorithms to analyze Basic Safety Messages (BSM) to determine misbehavior. Devices that support misbehavior detection would then send a misbehavior report (e.g., such as described in https://scmsmanager.org/wp-content/uploads/2020/01/Misbehavior-Report-and-Application-Specification-v1.0.pdf) to the SCMS, where SCMS operators can act on those reports and potentially add a misbehaving device's certificates to the certificate revocation list (CRL). The CRL is used by connected vehicle devices to reject certificates from a misbehaving device. A CRL is a list of digital certificates that have been revoked by the issuing Certificate Authority before their scheduled expiration date and should no longer be trusted. A certificate is irreversibly revoked if, for example, it is discovered that the Certificate Authority had improperly issued a certificate, or if a private key is thought to have been compromised. Certificates may also be revoked for failure of the identified entity to adhere to policy requirements, such as publication of false

documents, misrepresentation of software behavior, or violation of any other policy specified by the Certificate Authority operator or its customer.

1.2 Certificates

The SCMS is responsible for issuing certificates to devices through the Registration Authority (RA) to connected vehicle devices. The SCMS makes use of several certificate types depending on whether the connected vehicle application is installed on a vehicle or RSU. There are three types of operational certificates:

- **OBU Pseudonym Certificates:** Pseudonym certificates are short term and used primarily to sign BSMs. They are downloaded in batches, are valid for one week and rotate on a set basis (e.g., distance traveled, time since last certificate change). For privacy reasons, a device is given multiple certificates that are valid simultaneously, so that it can change them frequently. The SCMS generates and keeps 3 years' worth of pseudonym certificates available for devices to download. Some security profiles are configured for downloading a varying number of weeks' worth of these certificates to a vehicle at a time, typically based on how often an OBU is likely to communicate with an RSU that can provide the updated certificates. At this time, batch frequency and size are universal.

- **OBU Identification Certificates:** These certificates are used in the same way as pseudonym certificates, but for vehicles with special privileges (e.g., police vehicles, ambulances, fire trucks, transit vehicles, etc.). OBUs use identification certificates primarily for authorization in V2I applications, such as signal pre-emption for emergency vehicles. As there are no privacy constraints for identification certificates, an OBU has only one identification certificate valid at a time for a given application.

- **RSU Application Certificates:** Application certificates are used by an RSU to sign any over-the-air messages transmitted, such as signal phase and timing or traveler information message. As there are no privacy constraints for RSUs, an RSU has only one application certificate valid at a time for a given application. These certificates are used to sign the different types of messages an RSU may broadcast including: Signal Phase and Timing (SPAT), MAP and Traveler Information Message (TIM). Devices typically have an active, valid certificate for one week and have another week in reserve. Application Certificates are tied to a Provider Service Identifier (PSID).

For connected vehicle devices to receive and use certificates, each device must have: (i) software associated with signing, authenticating, encrypting and decrypting (governed by IEEE 1609.2); (ii) software to generate public-private key pairs and create the requests for the SCMS to generate enrollment, pseudonym, application and identification certificates to be used by the first software block; and (iii) a *Hardware Security Module (HSM)* to securely store private keys. A HSM is a specialized, physical computing component or device that safeguards and manages digital keys for strong authentication and provides crypto-processing.

In addition to certificates, there are other files associated with the SCMS that devices will use. These files are updated whenever a device communicates with the SCMS Registration Authority (RA). These files serve as administrative/policy files that are defined by the SCMS Manager.

- **Local Certificate Chain File (LCCF):** Provides the chain of trust for certificate authorities to trust. This allows devices to trust certificates generated from other certificate authorities.

- **Local Policy Files (LPF):** This file provides key configuration items associated with the SCMS and include: (i) number of pseudonym certificates granted per week and (ii) certificate validity periods. These are generally negotiable with the SCMS provider.

The SCMS is also responsible for issuing test certificates for all types of certificates described above. The purpose of test certificates is to enable development of applications and supporting functionality that interacts with SCMS functionality within the development environment without affecting other trusted devices, and to test and validate performance and functionality in a SCMS test environment before devices can enroll in the production SCMS. A test certificate can be used only within the domain of a test environment and are generated using the same format and algorithms used for a production certificate. Further considerations are discussed in section 2.2 below.

Procurement Considerations

While agency procurement practices may vary, when getting started it may be beneficial to first issue a Request for Information (RFI) before procuring a SCMS. As the connected vehicle landscape evolves over time, assessing the current state and capabilities in the supplier community can be an informative step to help in developing a Request for Proposal (RFP) that better describes the desired functionality and services and results in a more successful procurement. In addition, an RFI can help an agency to assess the current Technology Readiness Level (TRL) of SCMS and consider the life cycle management responsibilities associated with using a mature production environment with established processes and experience versus an early stage development. Technologies at a lower TRL may enable beneficial applications but are likely to require more significant attention and understanding of responsibilities from both the deploying agency as well as its device vendors (e.g., devices may require firmware or development of patch updates relating to SCMS more frequently). Engaging with collaborative groups such as working groups established by the American Association of State Highway and Transportation Officials (AASHTO) and standards development organizations, and peer agencies with prior experience can be invaluable in assessing the current state of SCMS and connected vehicle interactions.

When developing a procurement document to include in an RFP for a SCMS provider, the following items should be considered:

2.1 Objective

To maximize the ability of the SCMS procurement in satisfying CV project goals, the procurement should reflect well-thought out objectives that are clearly stated, explaining the desired SCMS role in supporting the CV projects and ecosystems that rely upon it. Since the agency project's goals may vary significantly, it is important to align the objectives of the SCMS procurement with project needs, but also considering broader and longer term expectations for the life cycle (such as potential risks of lock-in, making the agency dependent on one vendor). Contract terms should account for these agency needs, while recognizing the uncertainties. There are inherent tradeoffs that should be weighed, as there may not be a single best solution for all scenarios.

Agency CV Objectives could range widely, and may include combinations of multiple objectives over time, for example:

- **Experimental/development use** – SCMS to support research, lab-based development activities, or small-scale pilot

- **Specific CV pilot deployment project** – SCMS to support field applications where devices are within agency control or management

- **Multiple CV deployment projects** – SCMS to support multiple projects including devices that may be under separate control (such as multiple deployments that may potentially interact within a larger region)

- **Future compatibility** – Aiming to enable participation with future participants (such as production vehicles) based on expectations, which may subject to significant uncertainties

Agencies should consider assessing their readiness and the state of the broader CV ecosystem, so the objective does not aim prematurely for a comprehensive solution, which may or may not meet long term needs. It is important to recognize the significant uncertainties now and in the future, and the factors that may be outside the control of the agency and its vendors. In particular, deployments plans for production vehicles have changed substantially in the past, and can change substantially and abruptly at any time. There can be potential lock-in effects associated with making choices, and also may be other options that become available in the future. **Agencies should conduct due diligence to understand the current environment, maturity levels and trends, and risks before initiating a procurement.**

Objectives should also consider the development state and needs of the project. A project including development of CV applications for a pilot will have needs that differ from a deployment of more mature devices and applications that have been deployed in other environments with SCMS interactions. For example, a project solely aiming at experimental/development use is not likely to satisfy requirements associated with a production SCMS environment. Needs for SCMS environments can include the following:

- **Development** - SCMS environments for development are not intended to be interoperable with others, but should give vendors the ability to develop and test device/application software.

- **Test** - A test environment allows testing of interoperability across multiple participating vendors, and could be suitable for a limited scope project. A test environment can also be useful not only to test the technology, but to test the agency's organizational and human capital capabilities. Deployment of new devices into a production environment is also likely to require a test environment to support verification processes.

- **Production** - Finally, a production environment supports processes and protocols that reflect real-world deployment, and therefore imposes requirements on participating devices. For example, end-entity requirements may need to be satisfied before enrollment. See https://wiki.campllc.org/display/SCP for documentation from the CAMP SCMS POC project for examples of end-entity requirements. It is important to note that some requirements may only be satisfied through device implementation in hardware (e.g., https://wiki.campllc.org/display/SCP/Hardware%2C+Software+and+OS+Security+Requirements) and need to be considered prior to device selection. Device certification may also be potentially required for interoperability with certain production-level applications.

As an example, a potential objective description within a Specific CV pilot deployment project may be:

<AGENCY NAME> is seeking a turnkey security credential management system (SCMS) solution as part of its connected vehicle program efforts. As part of its connected vehicle program, <AGENCY NAME> is planning to deploy the following connected vehicle applications (further defined in the procurement document) under agency control:

- *<LIST ALL V2V AND V2I APPLICATIONS>*

<AGENCY NAME> is seeking a <state development environment, test environment, and/or production environment> SCMS solution that must be able to provide device certificates that allow for a full range of connected vehicle applications. The SCMS Provider shall also provide SCMS services for the duration of the period of performance.

2.2 Technical Requirements Considerations

The following are technical requirements that should be considered in the procurement of an SCMS product or service. The list of technical requirements is not intended to be comprehensive. Agencies should review these requirements to determine which requirements are applicable and if additional requirements are necessary. It is important to clearly trace the requirements to the agency or project objectives as established (discussed in section 2.1). This will help avoid unnecessary requirements as well as increase the completeness of the requirements set. Simply copying requirements without connecting to established needs and objectives is unlikely to result in successful application.

2.2.1 General Technical Requirements Considerations

- *Provide a security and credential management system (SCMS) platform for the duration of the <PROGRAM NAME & EXPECTED END DATE>, with the option to extend <SPECIFY EXTENSION DURATION/TERMS>.*
- *Compliance with IEEE 1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments—Security Services for Applications and Management Messages*
- NOTE: A production SCMS environment will likely enforce requirements on the participating devices. Agencies should verify both that the requirements are consistent with desired protections, and understand the constraints imposed on the deployment. In particular, device compliance with FIPS 140-2 (may be required by SCMS so that devices can store certificates securely in a production environment, e.g., https://wiki.campllc.org/display/SCP/Hardware%2C+Software+and+OS+Security+Requirements) could result in project requirements such as
    - *Services requiring role-based authentication shall meet the authentication requirements of FIPS 140-2, Section 4.3 Level 2 and any supporting FIPS 140- 2 implementation guidance.*
    - *Services requiring authentication shall meet the single attempt and multiple attempt authentication strength requirements of FIPS 140-2, Section 4.3.*
    - *The validation of signed software shall require use of a verification key that is protected by local hardware to a level equivalent to FIPS 140-2 at the level appropriate for the device.*

- *Provide technical support services to <AGENCY NAME> through the life of the contractual engagement.*
- *As needed, be able to support <AGENCY NAME's> existing IPv4 infrastructure and network (assuming it exists), with an active or migratory path towards IPv6>.*[1]
- *Provide a service that is interoperable with connected vehicles deployed as part of the <INSERT DEPLOYMENTS/PROJECTS YOUR AGENCY WANTS TO BE INTEROPERABLE WITH> and devices in private vehicles, including <INSERT PRIVATE VEHICLE DEPLOYMENTS (E.G., OEM DEPLOYMENTS) YOU WANT TO BE INTEROPERABLE WITH>.*
- *Be able to support full-scale connected vehicle deployment device support, including an estimated <INSERT NUMBER> on-board units (OBUs) and <INSERT NUMBER> roadside units (RSUs).*

  Note: Consider including a graduated deployment curve over the period of performance that conveys the number of years to reach these estimates. It should be noted that the number of certificates is related to the number of devices and duration of the project. However, in some projects it may be difficult to define the number of units over time in a precise manner. Since pricing models may vary, it is important to focus the procurement on the operational and mission needs rather than simply counting certificates, which could lead to unanticipated costs. An RFI could be used to explore the available pricing models and terms. This information may be included in an appendix. An example is provided below:

Table 1. Example Device Certificates and Duration Required

DEVICE	20<XX>	20<XX>	20<XX>	Extension Option
OBUs	<Insert>	<Insert>	<Insert>	<…>
RSUs	<Insert>	<Insert>	<Insert>	<…>

Individual certificate durations shall satisfy the project duration requirements, for example:

  - *OBU Pseudonym Certificates – 1 week duration with <X> certificates usable concurrently, and <Y period into future> available to device*
  - *OBU Identification Certificates - <X> duration with <Y period into future> available to device*
  - *RSU Application Certificates - <X> duration for <application A>, <Y> duration for application B>, …*

- NOTE: Consider potential need to adjust timing or extend duration of SCMS services

[1] Note: Requirement may need to be updated to reflect the agency's existing infrastructure and network.

based on project timeline and potential delays, considering the agency's experience and project maturity level. For example, consider provisions such as:

  - *Retroactively provide certificates to devices already deployed in <AGENCY NAME's> ecosystem at the time this SCMS solution is implemented, estimated at no more than <INSERT NUMBER OF UNITS> RSUs and <INSERT NUMBER OF UNITS> OBUs.*
  - *Prior to enrollment, provide option for reallocation of device certificates to a later validity period, not to exceed <duration>.*

- *Provide managed services inclusive of any on-premise devices as part of this system.*
- *Provide a Service Level Agreement (SLA) that details incident response times, system uptime guarantees, and any additional support offerings.*
- *Accept liability for damages caused by an exposure of the private key for the Certificate Authority, including all certificates impacted by such an event and costs associated with re-bootstrapping all devices.*

The SCMS provider will likely need to make available technical experts available for the duration of the contract. *The providers technical experts shall be available on-site, via phone calls, or video conferences as needed to:*

- *Review <INSERT AGENCY> project documentation and contribute content to technical and systems engineering documents.* ***Note:*** *Include a list of all technical and systems engineering documents the vendor will need to review and contribute content to. Be specific of what will be required by the vendor.*
- *Appropriately scope and plan for an SCMS implementation. Consider requiring the vendor to deliver a SCMS Implementation Plan that defines the scope and plan for delivering the SCMS solution.*
- *Document system requirements in a format that can be incorporated into existing technical documentation and requirements.*
- *Advise on system requirements, hardware requirements, and other preparatory actions needed for an SCMS implementation.*
- *Design and develop alternative solutions if technical barriers to implementation are identified.*
  - *Outline potential implications on SCMS design and privacy protection associated with the current communications protocols and regulations.* While the SCMS should generally be agnostic, there may be requirements that relate to devices' need for communications access to the SCMS, for example to replenish certificates. Agencies should assess the current environment prior to initiating the procurement.
- *Advise on Provider Service Identifiers (PSID) selection, technical details of implementing connected vehicle concept and ensuring application/message/device interoperability with <INSERT DEPLOYMENTS/PROJECTS YOUR AGENCY WANTS TO BE INTEROPERABLE WITH>.*
- *Document compliance with <INSERT AGENCY's> privacy and security policies.*

There will also be a need for the SCMS provider to make available technical experts, and test certificates, associated with a development and/or test environment, necessary for application development, device bench testing, including testing connected vehicle application scenarios,

multiple roadside and on-board unit providers' hardware, and integration testing by the agency and its vendors. A test environment may be used for end-to-end testing including the OBU, RSU, and backend devices (e.g., devices located at the TMC) that have Hardware Security Modules (HSM) prior to a production environment. **Note:** Your agency should understand the relationship with certification services (see SCMS structure described in https://www.pcb.its.dot.gov/documents/SCMS_Primer.pdf) and assess if/when it needs to require hardware vendors (e.g., OBU and RSU vendors) to either have achieved certification or to be working toward the certification in the required timeframe, depending on the requirements for end entities, intended applications (PSID) and interoperability that need to be satisfied. *Services shall include:*

SCMS provider requirements to support Test Certificates and Device Verification within a development and/or test SCMS environment, may include (but are not limited to):

- *Providing OBU test certificates for bench testing, initial enrollment certificate testing.*
- *Providing RSU test certificates for bench testing, initial enrollment certificate testing.*
- *Collaborating with <INSERT AGENCY's> selected hardware providers for initial enrollment and bootstrapping certificates for OBUs and RSUs.*
- *Providing Test application certificates for validation of PSID selection and mapping to applications.*
- *Supporting integration testing with TMC on-site proxy server, or direct connection to provider service.*
- *Supporting prototyping and levels of support during testing activities*

For projects that have an objective to operate in a production SCMS environment, the SCMS provider will also need to provide ongoing production-level SCMS system support for connected vehicle deployments, including for an estimated <INSERT NUMBER> OBUs and <INSERT NUMBER> RSUs. Considerations for services the SCMS provider may need to provide include, but are not limited to:

- *Providing a trusted certificate authority (CA) and making available certifications and validations of the secure nature of the facilities providing these services (agency should identify which certifications/validations, and verification methods, are required based on objectives).*
- *Support for enrollment certificates, pseudonym certificates, application certificates, and identification certificates.*
- *Collaborating with selected device providers (e.g., OBU and RSU providers) for initial enrollment and bootstrapping certificates for OBUs and RSUs.*
- *Providing interoperability with non-<INSERT AGENCY> equipped vehicles, including <INSERT VEHICLES THAT YOU WANT TO BE INTEROPERABLE WITH>.*
- *Ongoing top-off certificate support for OBUs traveling in network, including non-<INSERT AGENCY> equipped vehicles.*
- *Providing an on-site proxy server if determined necessary, or access to provider servers for interfacing with the SCMS.*
- *Providing tunneling or proxy services for IP traffic (e.g., IPv6 tunneling support) if*

determined necessary by <INSERT AGENCY> and the provider.

- *Providing message signing capabilities at point of origin in the TMC (e.g., traveler information messages [TIMs] issued from the TMC to RSU to vehicles).*
- *Providing service plan for installing, testing, maintaining, and patching the purchased services.*
- *Providing software development support for SCMS applications*

Additionally, depending on project objectives, if interoperability of multiple CV deployment projects is a required objective, agencies should identify the relevant requirements including engagement with the other projects. Engagement with automotive industry groups may help to understand the expectations and underlying technical and policy requirements that must be satisfied for interoperability under a future compatibility objective.

2.2.2 Considerations for Early Deployment Challenges

The SCMS provider plays a critical role that the deploying agency will rely upon for deployment of vehicle and infrastructure devices, even in early deployments where changes in the environment may be expected. Although there may not be a clear solution, agencies will benefit from asking relevant questions and incorporating suitable language into procurements based on factors such as the agency's project objectives and risk management practices. Considerations for understanding potential impacts and defining responsibilities under early deployments include, but are not limited to:

- **Interoperability** – Achieving nationwide CV interoperability is a well-understood goal, yet the supporting processes and policies for a CV environment are not yet solidified. The agency should consider what expected interoperability is to be achieved during the project and consider what steps would be taken if there is a lack of, or partial interoperability with other connected vehicle devices in the targeted population.
- **Lifespan** – While SCMS services may be procured for a defined period of time, a successful ongoing deployment will encounter a need to sustain devices over time. Careful consideration of the expected transition at the end of a project, and if and how devices would be upgraded and supported, should also include SCMS certificates and services.
- **Responsibilities between SCMS and device vendors** – While a procurement may be focused on SCMS services, the interdependence between device vendors and the SCMS can naturally result in situations where actions (e.g., development of patches/updates) may be necessary on either or both parties. Engagement with device vendors can help to understand the capabilities for supporting these actions. Responsibilities should be taken into account when procuring devices as well.
- **Understanding and addressing uncertainties** – Considerable efforts have been made to develop the underlying security design and architecture for SCMS supporting a connected vehicle environment. However, as with any new technology, there are fundamentally risks from potential unknown factors, which could affect the ability for SCMS services to support the planned CV deployment. For example, both the CV devices and the SCMS services rely upon cryptographic processes, and potential flaws in the design or implementation, or independent technological discoveries, could result in the need for significant changes, updates, or other modifications. While it may be

impossible to anticipate all potential uncertainties, agencies may benefit from the use of scenario-based planning to better define and understand impacts and roles, responsibilities and mitigations across a representative set of impactful events.

Additional Information

Readers can find additional related resources on the USDOT Connected Vehicle Deployer Resources web site at https://www.pcb.its.dot.gov/CV_deployer_resources.aspx. The USDOT developed an SCMS Technical Primer that includes an overview of the SCMS as well as best practices and lessons learned from early deployers of connected vehicle technologies. The technical primer is available at: https://www.pcb.its.dot.gov/documents/SCMS_Primer.pdf and lessons learned from the CV Pilots' experiences with SCMS are available at: https://www.its.dot.gov/pilots/cvp_scms.htm For additional SCMS technical details, the CAMP SCMS wiki (developed with USDOT support) should be consulted: https://wiki.campllc.org/display/SCP/SCMS+CV+Pilots+Documentation.

References

1. U.S. Department of Transportation. *Security Credential Management System (SCMS) Technical Primer*. Report FHWA-JPO-19-776. 2019. https://www.pcb.its.dot.gov/documents/SCMS_Primer.pdf
2. SCMS Manager Board of Directors. *Misbehavior Report and Application Specification for Connected Vehicle Pilot Deployment*. Last modified February 14, 2019. https://scmsmanager.org/wp-content/uploads/2020/01/Misbehavior-Report-and-Application-Specification-v1.0.pdf
3. Crash Avoidance Metrics Partners. “SCMS CV Pilots Documentation,” last modified February 20, 2018. https://wiki.campllc.org/display/SCP
4. Crash Avoidance Metrics Partners. “Hardware, Software and OS Security Requirements," last modified February 24, 2017. https://wiki.campllc.org/display/SCP/Hardware%2C+Software+and+OS+Security+Requirements
5. U.S. Department of Transportation. “Connected Vehicle Deployer Resources,” accessed December 3, 2020. https://www.pcb.its.dot.gov/CV_deployer_resources.aspx
6. U.S. Department of Transportation. “Lessons Learned From Recent Secure Credential Management Systems (SCMS) Operation with the CV Pilots," accessed December 3, 2020. https://www.its.dot.gov/pilots/cvp_scms.htm
7. IEEE. *IEEE 1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments--Security Services for Applications and Management Messages*. https://standards.ieee.org/standard/1609_2-2016.html

U.S. Department of Transportation
ITS Joint Program Office-HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487
www.its.dot.gov

FHWA-JPO-21-862

U.S. Department of Transportation