Full-Scale Security Credential Management System (SCMS) Deployment

Workshop Read Ahead

U.S. Department of Transportation

Technical Report Documentation Page

1. Report No. **FHWA-JPO-18-690**	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle Full-Scale Security Credential Management System (SCMS) Deployment Workshop Read Ahead		5. Report Date 22 Jun 2018 6. Performing Organization Code
7. Author(s) Joshua Kolleda, Tyler Poling, Scott Andrews, David Fitzpatrick		8. Performing Organization Report No.
9. Performing Organization Name and Address Booz Allen Hamilton 8283 Greensboro Dr McLean, VA 22102		10. Work Unit No. (TRAIS) 11. Contract or Grant No.
12. Sponsoring Agency Name and Address		13. Type of Report and Period Covered Final Report 14. Sponsoring Agency Code
15. Supplementary Notes		

16. Abstract

The Full-Scale Security Credential Management System (SCMS) Deployment Workshop Read Ahead is complimentary material for the Full-Scale SCMS Deployment Support Workshop. This read ahead document is to help ensure the workshop meets these objectives by providing applicable background information to prepare attendees for active participation in workshop activities consisting of seminars, team-based activities, and a scenario-based tabletop exercise. It is imperative that this document be thoroughly reviewed prior to the workshop

17. Key Words	18. Distribution Statement		
Security Credential Management System (SCMS), Proof of Concept, Connected Vehicles, Pilots			
19. Security Classif. (of this report)	**20. Security Classif. (of this page)**	**21. No. of Pages** 40	**22. Price**

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

Trust and protection of individual privacy, facilitated by an SCMS, are critical to ensuring successful messaging among vehicles and other devices. What will it take to establish a full-scale SCMS and governance entity to enable widespread connected vehicle deployment?

Intent of the Full-Scale Security Credential Management System (SCMS) Deployment Project

The purpose of the Full-Scale Security Credential Management System (SCMS) Deployment Support project is to help identify and explore potential strategies for the establishment and governance of a full-scale SCMS ecosystem through thoughtful engagement with stakeholders to seek guidance and determine feasibility of these strategies. Ideally, the outcome will also produce next steps and milestones to implement a full-scale SCMS deployment strategy or strategies for:

- Definition of a governance strategy for the full-scale SCMS – including the functions, roles, and responsibilities of all ecosystem entities, including those of an oversight entity such as an SCMS Manager and a Governance Board or Board of Directors
- Establishment of an overall SCMS Manager (or similar system management entity), along with functions, roles, and responsibilities for managing ongoing operations and executing any functions deemed to be "inherently central" and/or "core"

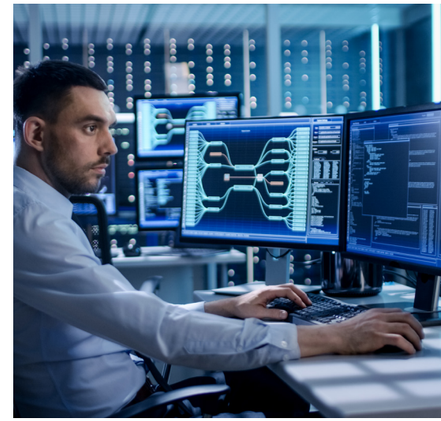
- Establishment of management entities that will be part of the larger SCMS delivery system (and whose authority is directly dependent on and linked to the SCMS Manager)
- Definition of high-level policies and procedures that affect the integrity and efficiency of the system and define and guide interactions among the various entities that make up the SCMS Manager
- Identification of roles and responsibilities of other entities that are not directly part of the SCMS but who may play a supportive, authorization, administrative, or other indirect role (e.g., Federal government, state governments, or industry associations)
- Development of business and financial options for initial deployment and sustainable operations

Purpose of the Workshop and the Read Ahead

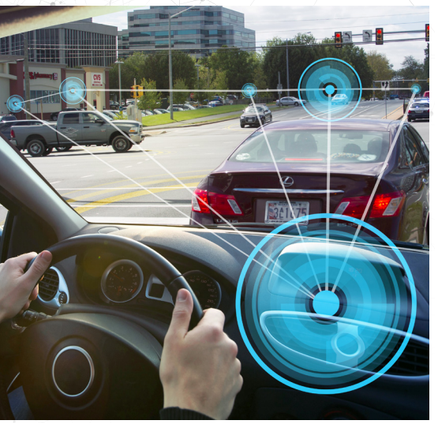
There will be two SCMS Deployment Governance and Ownership Workshops, both being identical in structure. One will be held on September 11th and 12th in Silicon Valley, California, and the second will be held on October 10th and 11th in Mclean, Virginia. The desired outcomes for each workshop are twofold. First, to identify one or more potential full-scale SCMS ownership and governance models, along with the next steps needed for deployment. Second, to develop a foundation for organizations, working groups, and/or consortiums to lead or assist in planning for the full-scale SCMS deployment and certificate policy development, as well as determine the role of the U.S. Department of Transportation (USDOT) in supporting these entities. These outcomes can be achieved by meeting the following objectives:

- Develop potential ownership and governance models, and the qualifying information about these models, such as steps that are needed for successful deployment; determine feasibility of the models
- Refine understanding of stakeholder motivations, interests, concerns, and willingness to dedicate resources to deploy the full-scale SCMS
- Define the SCMS Manager's roles and responsibilities based on models favored by participants
- Identify and describe additional challenges, risks, and opportunities to deploying and operating a functional and sustainable full-scale SCMS

This read ahead document is to help ensure the workshop meets these objectives by providing applicable background information to prepare attendees for active participation in workshop activities consisting of seminars, team-based activities, and a scenario-based tabletop exercise. It is imperative that this document be thoroughly reviewed prior to the workshop.



It is important to note that in December, 2016, the USDOT released a Notice of Proposed Rulemaking (NPRM) requiring all future light vehicles be equipped with dedicated shortrange radio communication (DSRC) to transmit BSMs. However, the recently released Executive Order 13771, "Reducing Regulation and Controlling Regulatory Cost," states that for every one new regulation issued, at least two prior regulations be identified for elimination, and that the cost of planned regulations be prudently managed and controlled through a budgeting process. This creates additional challenges in moving forward with the rulemaking. However, the USDOT still supports the deployment of vehicle-to-everything (V2X) communications.



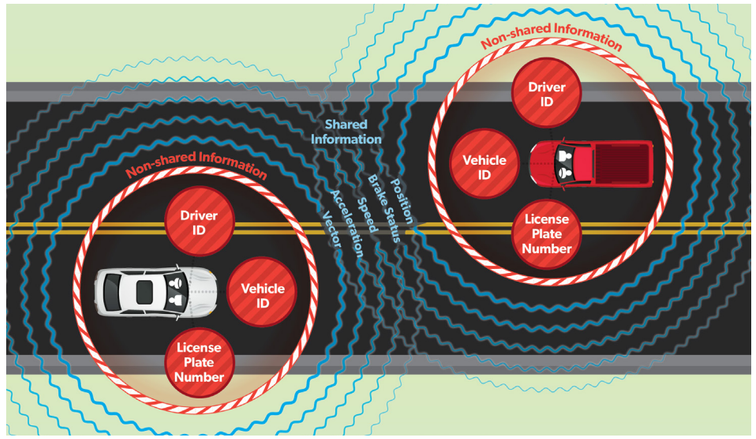
Basic safety messages (BSMs) use low latency communications containing information about vehicle position, heading, speed, and other factors relating to vehicle state and predicted path.

Connected Vehicle Primer

What are Connected Vehicles and How Do They Work?

Connected vehicles (CVs) aim to improve roadway safety and efficiency by providing a mechanism for two-way communication of situational information between vehicles, infrastructure (e.g., traffic signals and warning signs), and non-vehicular users (e.g., pedestrians and cyclists). The communication flows will allow messages to be sent from any equipped roadway entity to other nearby roadway entities to provide additional information about the current situation in that area. This information could then be used by the recipients to improve situational awareness. For example, if a vehicle is braking hard, this information may be useful to vehicles several cars behind the braking vehicle so that the drivers can be prepared for a sudden stop. By providing this advanced warning, drivers can be more aware of what is happening around them, and, as a result, can be more prepared and informed in choosing their driving actions and reactions appropriately.

Figure 1: Connected Vehicle Communications



A Need for Security and Privacy

The basic CV concept does not depend on any particular communications technology. To function safely, the CV system needs to ensure trustworthiness of communication. The source of each message needs to be trusted and message content needs to be protected from outside interference, regardless of the communication technology used. Ensuring authentic communications is critical for vehicle operators to trust the vehicle safety applications that rely on CV messages. Otherwise, if drivers cannot trust the information from CV messages, they will be less likely to take action based on the new CV technology and exchanged CV information. Basically, there is no benefit unless there is trust in the system. Moreover, an unsecure or untrustworthy system could produce a multitude of harmful effects on the transportation system. The CV system assumes that individual users (e.g., vehicles, users of personal devices) will transmit operational status messages, which creates significant privacy concerns. Many of the messages are transmitted regularly and include position and speed data. Ensuring that this information cannot be used to trace a specific user is a key component of the overall cybersecurity solution for the success of the CV system. It's important to note that the SCMS only secures the communication and not the end to end system.

USDOT SCMS Research

The USDOT led the creation and deployment of the SCMS Proof-of-Concept (PoC) to support the CV pilots and other federally-funded V2X related efforts. The SCMS POC used a Public Key Infrastructure (PKI)-based approach that employed highly innovative methods of encryption and certificate management to facilitate trusted communication. Authorized system participants used digital certificates issued by the SCMS PoC to authenticate and validate the safety and mobility messages that form the foundation for CV technologies. To protect the privacy of vehicle owners, these certificates contained no personal or equipment-identifying information but served as system credentials so that other users in the system could trust the source of each message. Each device or user also had a multitude of certificates that the device constantly altered to preserve privacy. Great strides have been made in establishing and operating the SCMS PoC. However, the structure and policies suitable to operate the significantly smaller-scale PoC will not be sufficient to govern the security credential needs of a full-scale nationwide deployment of V2X devices.

Full-Scale SCMS Deployment Overview

Purpose of an Ownership and Governance Model

To deploy and oversee the multifaceted SCMS, there must be an ownership and governance model or models to ensure effective governance and continued operations. Without establishing these models now, the SCMS could organically grow into a non-sustainable system characterized by varying levels of security and enrollment of V2X devices that do not meet standard requirements. For example, without a feasible ownership and funding model, there would likely be a lack of transparent ownership of SCMS technical components, which would also lead to a lack of accountability. There may also be various, possibly inconsistent funding streams that could lead to issues in availability and inconsistent services. Without a governance model and accompanying policies and processes, there could be varying security, privacy, and device standards across components and/or geographical areas. This could result in interoperability concerns and lack of confidence in the system. Of course, a lack of consistent PKI policies could also result in exploitable system vulnerabilities that could cripple the entire CV system. Without considering the worst effects, this would at least render the system useless.

SIMPLIFIED SCMS ARCHITECTURE DESIGN

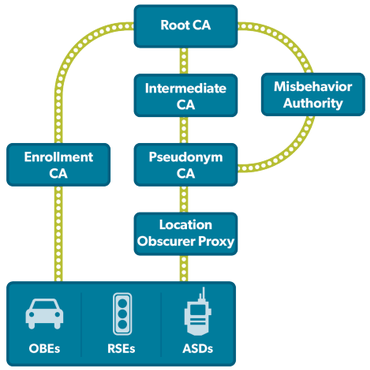


Figure 2: Simplified SCMS Architecture Design

Ownership is a key factor to ensure there is adequate funding for initial deployment, and to support sustainable operations. Essentially, there should be an SCMS Manager, which will serve as the governing body for the SCMS ecosystem. The SCMS Manager would likely coordinate and monitor the operations of SCMS functions. The owner(s) of the SCMS Manager and SCMS technical components will also greatly influence the level and type of industry governance, and stakeholder input to develop governing policies.

Plan for Deployment and Implementation

Along with the development of an ownership and governance model(s), a strategy for deployment and implementation of that model must be developed. The implementation plan is as important as the selected ownership and governance model in making the full-scale SCMS a reality. Depending on the selected model, an implementation plan would contain differing activities and milestones. The strategy would minimally include a transition plan to move from strategy development to model planning to initial deployment. The implementation plan could include the following activities and artifacts:

Establish the full-scale SCMS deployment implementation workgroup. The transition from initial strategy development to detailed planning begins by setting the foundations for an implementation workgroup, consortium, and/or task force committees. Ideally, the working group would be formed in an organic manner by industry and would be comprised of multiple stakeholders across various industries.

Roles and responsibilities framework. To ensure all necessary entities have a role and that relevant skill sets are covered, the transition plan would include a roles and responsibilities framework outlining this information. This document would consider operational factors, such as the organizational separation of certain SCMS components. It would also account for management responsibilities, such as initial and sustainment funding models.

Communications plan. The communications plan would detail key individuals who are responsible for the interactions between the planning and implementation teams to ensure information sharing and transparency.

Project plan and timeline. The project plan and timeline would ensure a seamless transition from planning into deployment, as well as completing tasks in a timely manner.

Evaluation and feedback plan. The implementation team would monitor the progress of standing up the selected ownership and governance model.

The SCMS Architecture

Figure 3 is based on existing research by the Crash Avoidance Metrics Partnership (CAMP) and is not firmly set. However, the full-scale SCMS will likely have similar structure based on the current design.

FIGURE 3 Overall SCMS Architecture

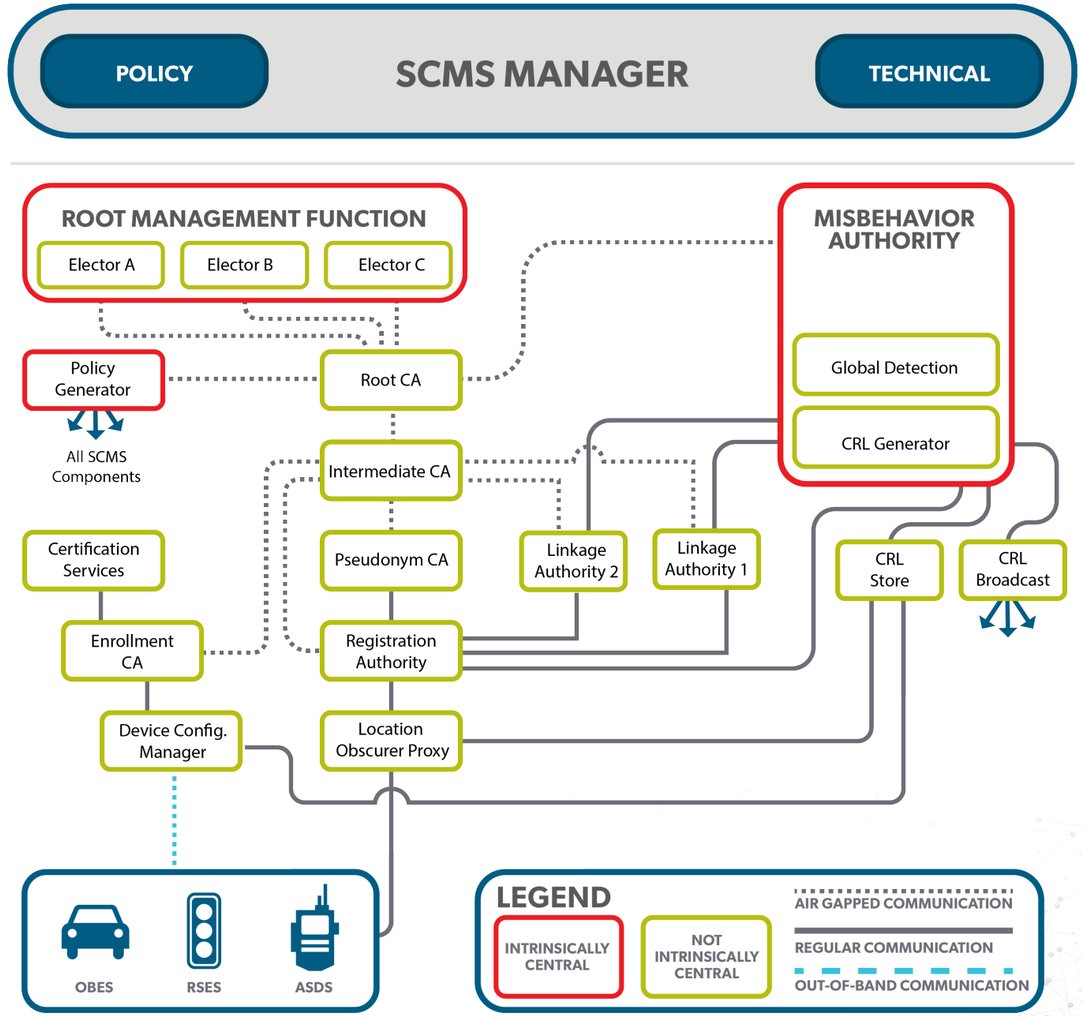


Table 1: SCMS Architecture Technical Components and Activities

Function Name	Activities
End Entities (EE)	An end-entity is a device that sends or receives messages, e.g., an OBE, an after-market safety device (ASD), an RSE, or a Traffic Management Center (TMC) backend.
Misbehavior Authority (MA)	The MA performs multiple functions to manage risk in the SCMS. It receives misbehavior reports from end entities (EEs), a device that sends or receives messages (e.g., on-board units [OBUs], Roadside units [RSUs], traffic management centers), investigates potential misbehavior, and blacklists or revokes other components in the system. The MA sends out an updated certificate revocation list (CRL), a list of certificates that have been revoked, to the devices in the field. In the current design, this is an intrinsically-central function, except for the CRL Generator (CRLG), which is one of the following subcomponents of the MA: • Global Detection (GD) collects the misbehavior reports and decides on revocation of certificates • CRLG compiles and signs the CRL, which contains linkage information that all receiving devices can use to identify the non-trustworthy device.
Root Certificaate Authority (CA)	The root CA (or multiple root CAs) is the root at the top of a certificate chain in the SCMS, making it a traditional PKI trust anchor. The root CA is not an intrinsically-central function. It issues certificates for intermediate certificate authorities (ICAs) as well as SCMS components, like the MA. The root CA has a self-signed certificate, and a ballot with a quorum vote of the electors establishes trust in the root CA. The root CA certificates must be stored in secure storage that is usually referred to as a trust store. An entity verifies any certificate by verifying all certificates along the chain, from the certificate at hand to the trusted root CA. This concept is called chain-validation of certificates and is a fundamental concept of any PKI. If the root CA and its private key are not secure, then the system is potentially compromised. Due to its importance, the root CA is typically offline when not in active use.
Elector	The electors are responsible for managing the Certificate Trust List (CTL). The CTL is a list of root CA certificates that are to be trusted by actors within the system. There are multiple electors to avoid the single point of failure risk that come from single root certificates. The electors manage the CTL by signing trust management messages that instruct the receiver to carry out an action (e.g., add or remove trust) on a certificate (elector or root CA). The recipient does not act on a trust management message until it has received the same instruction from a threshold number, or quorum, of electors. System parameters govern how many electors there are and the value of the quorum.

Function Name	Activities
Pseudonym Certificate Authority (PCA) (i.e., End Entity CA)	The PCA is an intrinsically non-central component of the SCMS. It issues short-term pseudonym, identification, and application certificates to devices. Individual PCAs may be limited to a particular geographic region, a particular manufacturer, or a type of device. Each PCA is associated with a single registration authority (RA) and a pair of linkage authorities (LAs) to perform its core functions. The PCA responds to requests from the MA to investigate potential misbehavior. The full-scale SCMS will also provide enrollment and application certificates to roadside units (RSUs) and other non-vehicular EEs. Application certificates are required for EEs to digitally sign messages, such as traveler information messages (TIMs), signal phase and timing (SPAT) messages, and map data messages (MAPs). These certificates are distinct from the pseudonym certificates issued to vehicles because privacy is not a requirement for roadside units as they are typically owned by a public agency or toll authority.
Registration Authority (RA)	The RA is an entity authorized to validate, process, and forward certificate requests. The RA receives and responds to requests for certificates from EEs via the Location Obscurer Proxy (LOP), which masks the source IP address and route of the EE from the RA. The RA will only accept requests from EEs that have enrollment certificates from enrollment certificate authorities (ECAs) that are authorized to use the RA. The RA can initiate certificate requests to a PCA to generate certificates for a requesting EE. Each PCA is also associated with a pair of LAs (LA1 and LA2) that generate pre-linkage values for pseudonym certificates, and to the MA. The SCMS may include multiple active RAs at any given time. Although multiple RAs may exist, a given device may access only one RA (as seen from the device).
Intermediate Certificate Authority (ICA)	The ICA's certificate is issued by a different root CA or ICA. The ICA shields the root CA from traffic and attacks. It may also allow for greater granularity in permission granting. For example, ICAs and the CAs below them may be limited to a particular geographic region or to a particular manufacturer or type of device to make auditing simpler. ICAs may not be needed for initial deployment. The ICA authorizes all other non-central components including ECAs, PCAs, RAs, LAs, or additional ICAs. Similar to a root CA, an ICA is intended to be an offline component, meaning it should be configured with no direct network access or address. A local ICA Manager operates the ICA manually. The ICA is not an intrinsically-central function.

Function Name	Activities
Enrollment Certificate Authority	The Enrollment Certificate Authority (ECA) is an SCMS back-end component that signs and issues enrollment certificates for EE devices. The ECA receives and responds to requests from one or more device configuration managers (DCMs). This is not an intrinsically-central function. Individual ECAs may, for example, be limited to a particular geographic region or to a particular manufacturer or type of device. The process for obtaining an enrollment certificate is developed in such a way that no single organization has sufficient information to re-identify a device.
Location Obscurer Proxy (LOP)	The LOP obscures the locations of requesting EEs (e.g., OBEs requesting certificates) from SCMS functions, such as the RA. This is intended to mitigate the possibility that the EE's location and/or route could be determined from requests made to the RA. In the simplest sense, one might think of this device as a router performing network address translation. The LOP is not an intrinsically-central function.
Linkage Authority (LA)	The LA generates linkage values for a given EE based on a request from the RA. The certificates for a given device make use of linkage values (LVs) from two LAs, referred to as LA1 and LA2. The splitting is done to make tracking difficult. When necessary, the MA uses the linkage values to determine if multiple misbehavior reports, potentially associated with multiple pseudonym certificates, are actually from the same EE, and allows the revocation of all the EE pseudonym certificates via the CRL. This is not an intrinsically-central function.
CRL Store	The CRL store is a repository that contains the most up-to date-certificate revocation lists generated by the MA. The CRL store is accessible by all CV equipment and SCMS entities so they may obtain the most up-to-date certificate revocation information. This function is not designated as a central or non-central function.
CRL Broadcast	The CRL broadcast is the entity that makes the current CRL available on a broadcast basis (e.g., these may be RSEs or the satellite radio system). This function is not designated as a central or non-central function.

CV and SCMS Ecosystem

The SCMS ecosystem includes the SCMS and the peripheral industry participants that play a role in developing, provisioning, operating, and maintaining the equipment and systems necessary to support the security functions identified for the overall CV enterprise. The SCMS itself encompasses all PKI functions necessary to establish and maintain privacy and security within the V2X ecosystem. It provides the various functional elements that will perform these security management functions over the equipment and/or application lifecycle. Figure 4, below, is a notional depiction of the SCMS ecosystem. It is intended for illustrative purposes only and is subject to change.

The SCMS ecosystem must also accommodate future stakeholders and participants. For instance, the SCMS may need to interface with other governance bodies, such as credential management systems in Canada and Mexico, in some capacity to support interoperability. Furthermore, the SCMS also has the potential to evolve outside of the traditional V2X ecosystem (e.g., machine-to-machine communications) and additional security measures and polices may be needed to support effective operations.

FIGURE 4 Full-Scale SCMS Ecosystem

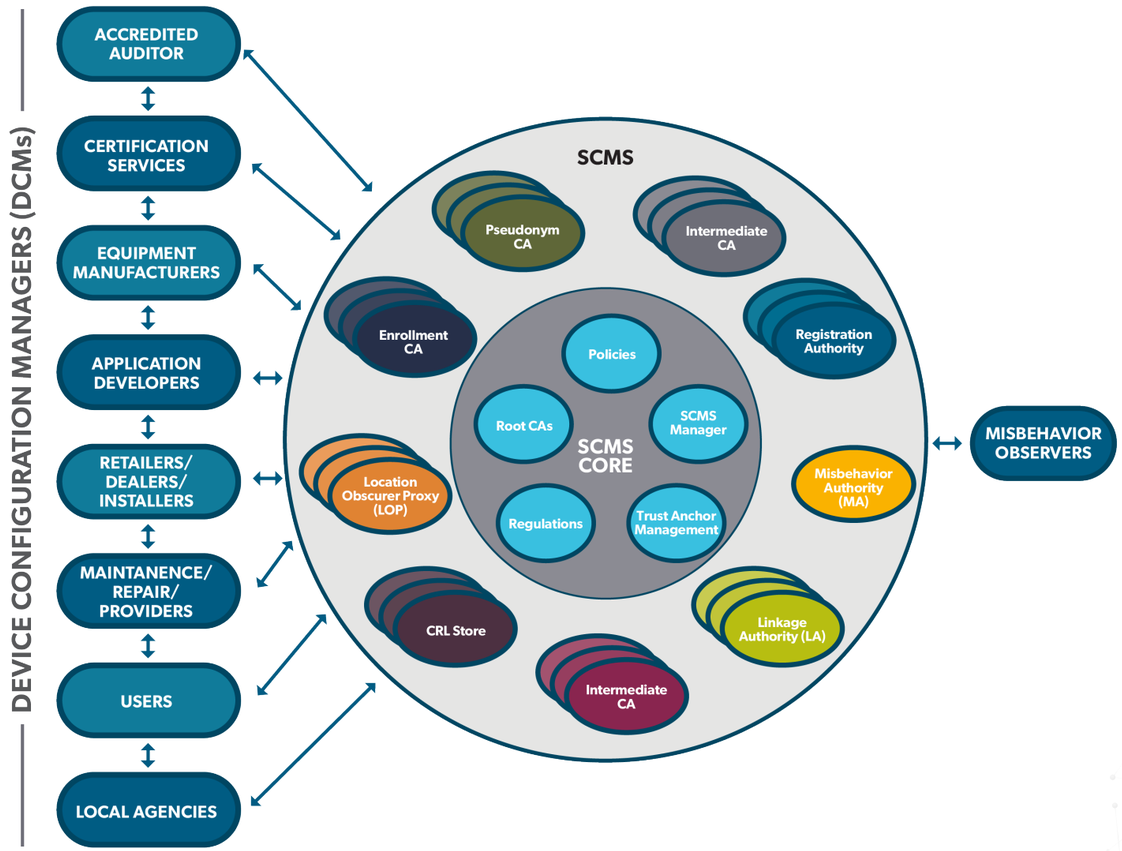


Table 2. SCMS Ecosystem Functions and Activities

Function	Activities
Notional SCMS Core	At the core of the SCMS ecosystem are the root CA(s), the trust anchor management function, the SCMS Manager, and associated policies and regulations. The SCMS Manager provides the core policy and governance foundation for the SCMS ecosystem in general, and the SCMS specific functions in particular. The SCMS Manager's authority, responsibilities, ownership, and organizational structure has yet to be determined, but it is likely that it will serve as the motivating force to establish the SCMS functions through policy and regulation. The SCMS Manager will also likely serve in an ongoing capacity as the core of a governance body, to coordinate and monitor operations among the various SCMS certificate management entities (CMEs) and functions. It is also expected that the SCMS Manager will collaborate with entities and organizations outside of the immediate SCMS, such as certification and testing shops; state and local transportation organizations; vehicle inspection facilities; automotive repair shops; and automotive or device dealerships.
Device Configuration Managers (DCM)	DCMs are entities responsible for provisioning CV equipment (e.g., OBUs, RSUs) so that it can successfully interact with the SCMS and obtain the security credentials appropriate to its operation. While the DCM is external to the majority of the SCMS, it plays a critical part of the enrollment certificate mechanism. DCMs must be subject to the same types of audit and oversight as other technical components. The DCM is used during bootstrap to provide essential information to a bootstrapped device, and to relay information between a device and the ECA. DCMs will coordinate initial trust distribution with CV equipment so that it may then request and successfully receive certificates from the RA. The communication link between a bootstrapped device and DCM is out-of-band (i.e., a non-cryptographically protected communication in a secure environment). The SCMS Manager will need to establish and enforce the minimum level of security required for such out-of-band communications to maintain the integrity of the overall system. The DCM is not an intrinsically-central function; for example, different out-of-band communications methods could be used by various original equipment manufacturers (OEMs). Because these entities are not necessarily constrained to any specific structure or scope of operations, a variety of different industry entities may perform the role of the DCM (e.g., device manufacturers, vehicle manufacturers, systems integrators).
Certification Services	Certification services are responsible for evaluating devices to ensure they perform to specified operational requirements and conform to the security policies specified by the SCMS Manager. The SCMS Manager is likely responsible in this example for accrediting certification labs. In one example, the certification lab could exist in two variations. In one, the OEM performs self-certification and the certification lab acts as a proxy between the OEM's internal lab and the SCMS. Another variation would be to use a test lab which performs intensive tests for a given device type. It is generally assumed that such evaluations and tests will be performed on a "type" basis rather than on every manufactured device. The certification service will then provide verifiable documentation that communicates to the Enrollment CA that units of that particular type are eligible for enrollment certificates.
Communication Carriers	Communications carriers are external to the SCMS, and may or may not operate under policies and regulations associated with the SCMS. For example, cellular carriers may provide an IP link between a device and the SCMS, but the packets carried in that link would be secured independently from the carrier's operations.
Users	Users are vehicle owners and operators, and are responsible for the operation condition and maintenance of the CV equipment (e.g., OBUs or ASDs) associated with their vehicles. Users are expected to have very limited, if any, interaction with the SCMS, unless there is a problem with their vehicle. For example, in cases where a vehicle is misbehaving (either because it has been tampered with, or because it is malfunctioning), the vehicle owner would be compelled to have the vehicle examined and/or repaired by a service technician.
Local Agencies	Local agencies are responsible for public vehicles using CV equipment, and for roadside equipment under their jurisdiction. Local agencies are expected to have somewhat limited interaction with the SCMS. For example, they may need to specify the permissions for certain vehicles operating in their fleet and will be responsible for approving the applications and permissions associated with roadside equipment, which will then be reflected in that equipment's certificates.
Misbehavior Observers	The misbehavior system has not been defined sufficiently to determine exactly what operations it will entail. However, it is reasonable to assume that any form of misbehavior will need to be observed and reported by some entity on the roadway. This could be other CV equipment or roadside equipment operating in a special role to detect and report observed misbehaving CV equipment.

Full-Scale Deployment SCMS Ownership and Governance Model Areas of Interest

This section explores various deployment and operational factors that will need to be considered when selecting ownership and governance models for the SCMS. Refer to the SCMS Baseline Report for additional information on these topics.

Collaboration and Cooperation

A sustained, successful SCMS will depend on new levels of trust and collaboration between industries and entities. Depending on the ownership and governance model, there could be diverse stakeholder participation within the SCMS Manager and ecosystem. Diverse stakeholder participation can present a challenge in that these entities could be competitors (i.e., OEMs competing for market share) within their industry, but will have to work together to ensure the system operates effectively and safely.

The payment card industry is a mature example where this has been successfully executed. Competing payment card organizations (MasterCard, Visa Inc., etc.) worked together to establish the Payment Card Industry Security Standards Council (PCI SSC). The council has worked together to set strict privacy and security standards to ensure protection against malicious use of sensitive data. The PCI SSC sets industry-wide security standards through collaboration and consensus among members. They also develop and operate programs to train, test, and qualify organizations to assess and validate adherence to the various PCI Security Standards and to be re-certified each year.

Single vs. Multiple Root Certificate Authorities

An SCMS design allows for single or multiple roots. The decision of which of these models to deploy will be made based on operational and public interest objectives as well as the chosen ownership and governance model. SCMS deployment could feature a single root, with the intent of expanding to multiple roots to help reduce the short-term governance and oversight costs. However, it's important to consider that operating with a single root may limit future flexibility. If OBUs are designed with the assumption of a single root, it may not be possible to transition to a multiple root architecture. Therefore, EEs must be capable of operating under multiple roots to ensure interoperability regardless the structure.

Considerations for adding root CAs include:

1. At least one root CA is required.

2. If a root CA is compromised, all devices are potentially affected. Therefore, each root CA certificate needs high security standards, defined by the SCMS Manager, regardless of the root CA's size.

3. More root CAs will increase the overall cost of the system and create more opportunities for malicious actors attempting to compromise a root. The security risk is mitigated by applying high security standards for each root CA.

In considering operational models and the number of eventual roots, stakeholders should understand that the number of root certificates presents several potential costs. Considerations include:

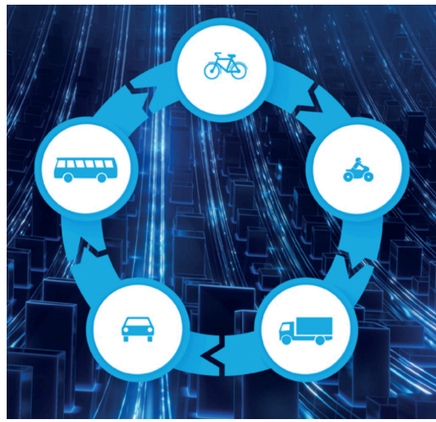
1. OBEs must have all root certificates. More roots would add to the memory requirement, although at very small increments.

2. Each root will have a CRL – hopefully small, but there will be memory cost associated with each.

3. A lot of roots may necessitate more issuing CAs (e.g., every OEM has its own root and issuing CA).

4. Potential processing difference – all certs chain through some issuing CA to a root but root and issuing CA validity only need to be checked once each time CRLs are received – a lot of different chains would mean that there is a need to process each one and cache.

Certificate Authority Retirement



TThe longer a public/private key pair is in use, the greater the chances are that the keys can be compromised. All roots have a specific lifespan and will eventually retire and new requirements (e.g., increased key size) may necessitate standing up a new root. There must be an effective method to retire and replace roots without negatively impacting SCMS operations. There are many ways to manage root retirement to limit operational interference. For example, an old root can "sign" a "roll over" certificate (contains the new root's public key) which allows the new root to be trusted with little effort. Depending on the reason for the new root, the two roots can exist simultaneously (e.g., for algorithm updates) or, after the new root is established, it signs new issuing CA certs for the existing CA. The old root is revoked and the new issuing CA certs are distributed – the issuing CA now belongs to the new root.

Root retirement further emphasizes the need for a standard approach to trust anchor management. The SCMS Manager and stakeholders will need to define the actual method to manage root retirement within the PKI policies. To ensure the overall integrity of the SCMS, the minimum and maximum lifetime of each certificate type will be defined and enforced by SCMS Manager policy. Operators will likely have some degree of flexibility in defining the actual certificate lifetimes.

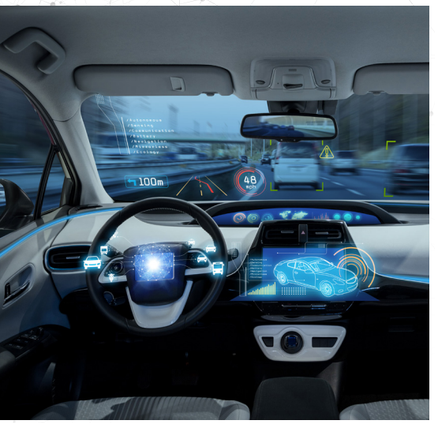
Elector Establishment and Management

The trust anchor management method within the current SCMS design is the elector concept. The advantage of the elector model is that there is no single point of failure. However, each elector is essentially a specialized, stand-alone PKI that has a single certificate. Deploying an elector could cost as much as standing up a root. The SCMS Manager, as the industry governance organization, could possibly bear the cost of deploying and operating the electors or any other trust anchor management method. The SCMS Manager needs to consider the appropriate number of electors that are necessary to make it very unlikely that a quorum cannot be achieved while keeping costs under control.

There are other trust anchor management options that may also be considered. For instance, the European C-ITS is being deployed with multiple roots and using a mechanism called a Trust List to inform end entities of new and revoked roots. The C-ITS model will have a single Trust List Manager – a specialized entity – with a certificate trusted by end entities.

Compliance: Auditing and Certification

Auditing validates that the security measures in the Certificate Policy (CP) are in practice at the organizational level by CMEs. The SCMS Manager may outsource the auditing function to a third-party provider or providers that have specific expertise in ITS and PKI, and that could provide training and assistance to CMEs that do not meet the security standards set in the CP. Usually the auditee pays



for the audit and must account for these costs when developing their funding streams, such as fee structures. Some PKIs base audit frequency on audit performance to reduce costs and prioritize activities. Depending on the level of government involvement within the SCMS ecosystem, the government may also be able to require intermediate inspections of CMEs between full audits. Enforcement of penalties for noncompliance may go beyond the authority of the SCMS Manager, especially regarding criminal activity. General oversight by the SCMS Manager will ensure that CMEs are sharing information in accordance with the CP.

End entities will need to meet certain PKI requirements, and functional and performance requirements, for initial enrollment and to maintain enrollment status with the SCMS regardless of the model. The SCMS Manager's level of control over the certification process will depend on the established policies.

- The SCMS Manager will need to establish the certification requirements to ensure the end entity can adequately protect keys, etc. Device certification ensures that EEs operate as per mandated (V2V) specifications, and possible local safety inspection regulations.
- The SCMS Manager may set and publish its certification lab accreditation policy and process.
- In this situation, a private company or other organization may then set up the required test lab facilities and request accreditation from the SCMS Manager. The test lab completes the published accreditation process and, if it meets the stated criteria, receives accreditation. This grants the test lab the ability to certify devices and to refer to itself as accredited.
- The governance model and associated policies will influence how the certification requirements and processes are funded, enforced, and audited.

Additional polices with respect to the broader SCMS ecosystem that need consideration include:

- The SCMS will likely need to consider whether re-enrollment certification criteria should require electronic proof that the end entity has met state and/or local safety inspection requirements.
- The SCMS Manager should consider policies regarding implications of end entities that are enrolled but subsequently fail state or local inspection requirements.

Misbehavior Management

The MA implements the mechanisms for identifying bad actors in the system and subsequently removing them from the system through certificate revocation. The activities of the MA can be broken into two sub-sets, the operation aspect and misbehavior management. The operational aspect must operate a sophisticated data mining and analysis operation to detect misbehavior and subsequently coordinate with the other SCMS entities to revoke the detected misbehaving vehicles. The management aspect could potentially operate as a law enforcement body or coordinate with such bodies to assure that identified misbehavers are appropriately dispositioned. It is possible that these two roles may be split between multiple operators. For example, a data analytics company might perform the analysis and coordination functions to detect and revoke misbehavers, and then some other physical security administrator might take over the enforcement and compliance end of the process.

Misbehavior management in enforcement of CV policies is not well understood. For example, would the laws and regulations surrounding misbehavior be set by the federal government, or would that responsibility be passed on to the states (e.g., as part of a state's motor vehicle code)? If the regulations are federal, then presumably the MA (or the SCMS Manager acting on behalf of the MA) would need to interact with one or more federal law enforcement agencies to respond to some types of egregious misbehavior. Alternatively, the MA may need to interact with numerous state and/or local law enforcement agencies. By way of another example, if a vehicle is found to be misbehaving and is subsequently revoked, the next step would presumably involve some form of inspection and repair. Many states currently operate various types of inspection systems, often using private, third-party service providers. It is reasonable that similar systems would be put in place to assure that misbehaving vehicles were returned to working order and then re-certified. It is assumed that, while the MA would not be directly involved in these activities, it may need to coordinate with law enforcement and/or state motor vehicle departments to assure that compliance with CV requirements was maintained (in much the same way that compliance with safety and emissions regulations is maintained today).

SCMS Ecosystem Stakeholders

Stakeholder Interview High Level Findings

Throughout the course of the SCMS deployment project, the research team facilitated stakeholder interviews and conducted a stakeholder analysis. The content below highlights common interviewee thoughts, issues, and concerns captured throughout the interview process.

- The stall in momentum of vehicle-to-vehicle (V2V) deployment caused by the Federal Communications Commission (FCC) spectrum-sharing discussion, coupled with the lack of progress on the National Highway Traffic Safety Administration (NHTSA) V2V rulemaking, is causing confusion within the industry and hindering SCMS development and deployment.

SCMS USERS INCLUDE:

- Vehicle Owner/ Operators
- Dealers and Installers
- Service and Parts Facilities
- CV Equipment and Application Suppliers
- OEMs
- State and Local DOTs
- Public Infrastructure System Integrators

- There is desire for United States Department of Transportation (USDOT) leadership, in any form, to unite stakeholders in shared V2V deployment and shape implementation of the National SCMS.
- Some interviewees are concerned that there is a lack of transparency and stakeholder representation within the current SCMS development efforts. There is also concern regarding potentially setting a precedent for certificate policy and technical architecture that cannot or will not be changed.
- Most interviewees supported industry taking the lead in deploying the National SCMS, with the government supporting working group facilitation, policy development, stakeholder representation, and governance processes (i.e., being actively involved in the SCMS Manager).
- Most interviewees believe that high levels of competition and independence within the auto industry will result in them wanting to own and operate their roots to maintain more control over services to their customers. While some stakeholders voiced concern that this mindset could result in a burdensome number of roots within the ecosystem, it's important to note that public key infrastructure (PKI) policy and root operating costs may lead to a smaller number of roots than expected.
- There is uncertainty throughout several stakeholder groups on the device enrollment process. Specifically, interviewees were concerned about where in the supply chain process devices will be enrolled and who will be responsible for device enrollment and provisioning.

Stakeholder Groupings

Stakeholders within the SCMS ecosystem are comprised into three major categories: Implementers, Users, and Other Interested Parties (OIPs). Organizations may fall into more than one of the categories. For example, the USDOT may play some direct role in the SCMS, so they are, to some degree an SCMS Implementer. On the other hand, because they have a large stake in the public benefits of the CV enterprise, they also play a significant role as an OIP. Each stakeholder grouping will have a stake in the SCMS. We define stake as the elements associated with the SCMS that will have a material impact on their organization from either a business, operational, or policy/ public benefits perspective. Please refer to the Potential SCMS Ownership and Governance Models report for more information on stakeholder groupings.

SCMS Implementers: Organizations that will ultimately stand up and operate the various components of the SCMS. They include PKI service providers, and various software, hardware, and administrative operations focused on providing security management services. As a result, the primary stakes for this group are directly business focused. For example, the amount of company investment needed to stand up and operate elements of the SCMS; the company's current capital assets that can support standing up and operating elements of the SCMS; or the company experience to implementing similar elements of the SCMS.

SCMS Implementers include: PKI Security Services, Certification Services, Vehicle Manufacturers (OEMs), USDOT, Communications Service Providers.

SCMS Users: Organizations that will use various elements of the SCMS on an ongoing basis. They include end users, equipment manufacturers, equipment sellers, repair facilities, testing facilities, and other entities that will be required to interact with the SCMS.

As a result, the primary stakes for this group are focused on how these interfaces with the SCMS will impact their business operations. There also may be elements of the SCMS operation that, while not directly related to an SCMS interface, may impact these SCMS Users. For example, if complying with SCMS policies requires a company to include substantial additional hardware or software, then the hardware or software costs represent a stake for that company; or if the SCMS policies require an equipment manufacturer to implement new business process steps—for example, extra steps/costs associated with securing inventory, or extra time associated with provisioning and certifying newly manufactured equipment—the costs of those steps would be reflected in this stake.

SCMS Users include: Vehicle Owner/Operators, Dealers and Installers, Service and Parts Facilities, CV Equipment and Application Suppliers, OEMs, State and Local DOTs, Public Infrastructure System Integrators

Other Interested Parties: These include public entities, such as the USDOT, or organizations with indirect, public, or technical interest in the connected vehicle enterprise, but who may not participate directly in the operation or use of the SCMS. Their concerns and motivations likely consist of policy input, the public good, technical element understanding, and standards development. Examples may include advocacy groups who are concerned about public safety, privacy, consumer rights, etc., or public agencies with the objective to improve public safety or transportation efficiency.

SCMS Other Interested Parties include: USDOT, Academia, Standards Organizations, Advocacy Groups

CME Groupings and Owner/Operators

When assessing SCMS roles against the functions, it's important to note that some SCMS components are mutually exclusive. Some SCMS functions must be performed by implementers who are not associated with other functions. For example, to preserve anonymity and allow for certificate revocation, the LAs must be separate from certain entities. The design of the SCMS assures that each party in the process has some of the information necessary to revoke certificates, but no party has all information. Once the linkage values are determined, it is possible to determine that a given certificate in the field is revoked, but it is not possible to use this information to identify the vehicle or owner.

SCMS IMPLEMENTERS INCLUDE:

- PKI Security Services
- Certification Services
- OEMs
- USDOT
- Communications Service Providers

SCMS OTHER INTERESTED PARTIES INCLUDE:

- USDOT
- Academia
- Standards Organizations
- Advocacy Groups

However, this means that some SCMS functions may represent a relatively limited commercial opportunity because they cannot be combined with other operations to form a larger enterprise. It is possible that these may represent sufficient opportunity to be attractive to an implementer, but to the extent that this is not the case, these elements may need to be subsidized in some way. Table 3 summarizes the SCMS component grouping restrictions and potential conflicts of interest based on the current design. Refer to the Potential SCMS Ownership and Governance Models report for more information on the potential component groupings and conflicts of interest.

Table 3: SCMS Component Grouping Restrictions and Potential Conflicts of Interest

SCMS Technical Components	SCMS Manager	Elector 1	Elector 2	Elector N	Root CA	Int CA	ECA	PCA	RA	LA1	LA2	LOP	MA	CRL Store
SCMS Manager		Y	P	P	P	P	P	P	P	P	P	P	P	P
Elector 1			P	P	P	Y	Y	Y	Y	Y	Y	Y	Y	Y
Elector 2				P	P	Y	Y	Y	Y	Y	Y	Y	Y	Y
Elector N					P	Y	Y	Y	Y	Y	Y	Y	Y	Y
Root CA						Y	Y	Y	Y	Y	Y	Y	Y	Y
Int CA							Y	Y	Y	Y	Y	Y	Y	Y
ECA								Y	Y	Y	Y	Y	Y	Y
PCA									N	N	N	Y	Y	Y
RA										N	N	N	N	Y
LA1											N	Y	N	Y
LA2												Y	N	Y
LOP													N	Y
MA														Y
CRL Store														

N	Prohibited from being in the same organization
P	There is no technical prohibition but presents a potential conflict of interest (See notes below)
Y	No issue with being in the same organization

Other than requiring different internal processes and certificate content unique to the CV security design, the functions of the Root Certificate Authority (CA), Intermediate CAs, Enrollment CAs, Pseudonym CAs, and Registration Authorities are not substantively different from those associated with other PKI systems. Thus, these functions should all be technically feasible for most PKI service providers. A key element that is different is the scale: because there will ultimately be over 500 million vehicles provided with certificates and certificate updates, the implementation of these functions must be done in a scalable manner, requiring implementers with the necessary experience and resources.

The LAs, Location Obscurer Proxy (LOP), Misbehavior Authority (MA), and Device Configuration Manager (DCM) are all new functions that will require substantial development. For example, because the DCM will reside near the consumer end of the product chain, it will be widely distributed. Training, equipping, and certifying the practitioners will represent a significant undertaking, and will likely involve a substantial software development effort to assure that the configuration process is followed exactly and is easily controlled and audited. The LAs have never been implemented before

and, while not particularly challenging from a technical perspective, the need for data security and system integrity will require special efforts to assure that the processes and information remain secret. The LOP is relatively simple in technical implementation, but because of the volume of vehicles and the distributed geographic nature of the CV enterprise, the implementation and management of the LOP will present a moderately challenging throughput (i.e., bandwidth and system availability) challenge. Lastly, the MA in this context has never been implemented. There are no existing models on which to base such a system, and the mechanisms for validating reports and identifying misbehaving vehicles are, as yet, undefined. It is also unclear how the MA will interface with law enforcement and various vehicle documentation entities (i.e., DMVs), so that enforcement activities beyond simple certificate revocation may be implemented within existing law enforcement processes.

Table 4: SCMS Implementer Types and Potential Roles

Types of Entities	SCMS Manager	Elector 1	Elector N	Root CA	Int CA	ECA	PCA	RA	LA1	LA2	LOP	MA	CRL Store
Federal Government	P	L		P									
Non-Profit Entities	P	P	P										
PKI Service Providers	P		L	L	L	L	L	P	P	P			
Certification Services								P				P	
Data Analytics												L	
Administrative Services Providers	P							P	P	P	L	P	L
Enforcement and Compliance												L	
Vehicle Manufacturers			P	L	L								

P	Possible to own or operate, depending on the SCMS deployment Model
L	Likely to own or operate

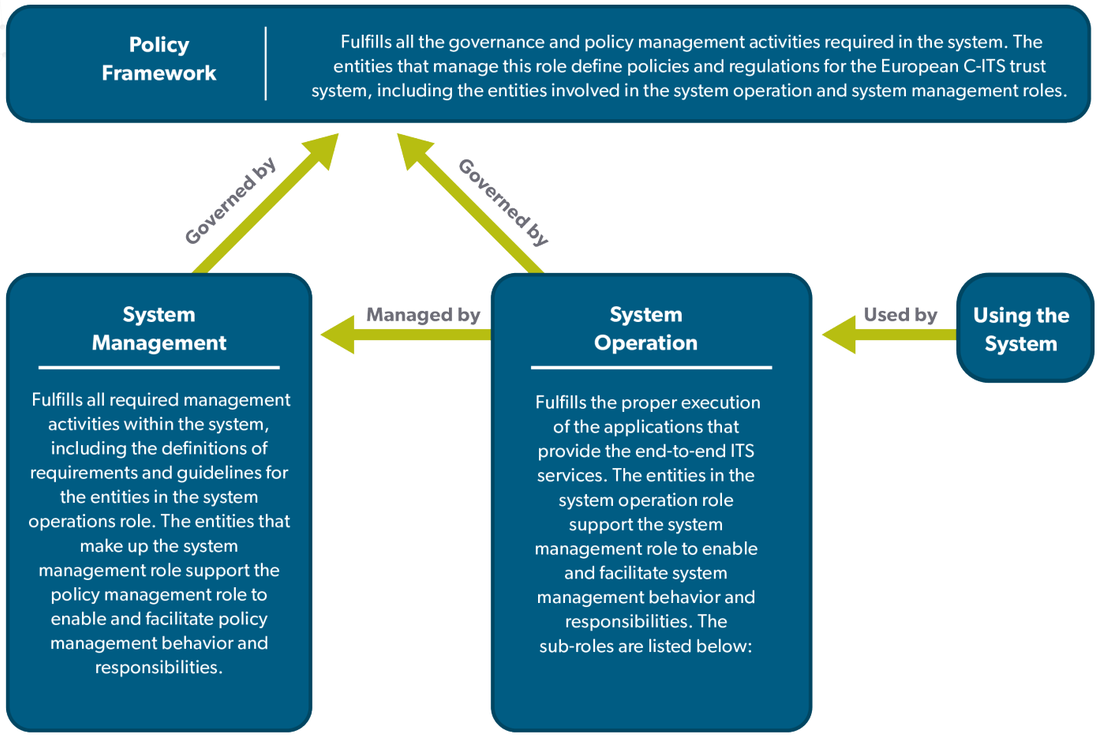
It's important note that the research team established the stakes identified for the stakeholder groupings and the SCMS implementer types and potential roles. Therefore, these are notional and are subject to change.

It's important note that the research team established the stakes identified for the stakeholder groupings and the SCMS implementer types and potential roles. Therefore, these are notional and are subject to change.

European Commission V2X Trust Model

The European Commission's Cooperative Intelligent Transportation System (C-ITS) trust model concept is based on multiple roots, which provide additional redundancy and interoperability, allowing for more flexibility in expanding and decentralizing operations. The European Commission's initial research and development of the trust model is led by a working group comprised of various stakeholders (e.g., OEMs, tier 1 suppliers, RSU/OBU manufacturers, state governments). The working group has developed initial versions of two key policies for the trust model. The first is a Certificate Policy, which defines the roles and processes for how security certificates are issued for a common level of trust in C-ITS messages. The second document is the Security Policy & Governance Framework, which defines additional cybersecurity requirements and specifies who is responsible for all roles in the overall C-ITS ecosystem. These polices facilitate a governance framework, which is depicted at a high level in Figure 5.

Figure 5: European C-ITS Trust System Organizational Roles



Policy framework development sub-roles:

- **C-ITS Governing Body** – Defines rules for the resolution of issues detected by the C-ITS Supervision Body and is the main contact to policy makers (e.g., European council, European parliament) as well as to international counterparts responsible for the C-ITS infrastructures
- **C-ITS Supervision Body** – Detects deployment and operational phase issues. It identifies, assesses, and monitors new security vulnerabilities, and ambiguous, or 'impractical' statements in requirements, regulation, or standards defining the system
- **C-ITS Certificate Policy Authority** – Approves and maintains the Certificate Policy. It manages change requests, and defines the Certificate Practice Statement (CPS) approval and audit procedures. It authorizes the C-ITS Point of Contact and the Trust List Manager to operate and report regularly and oversees root CA's CPS approval. It also oversees audit reports
- **Privacy Policy Authority** – Defines and manages the data protection rules and is responsible for being the central point of contact for the Data Protection Authorities
- **Security Policy Authority** – Defines, manages, and maintains the Security Policy
- **Compliance Assessment Body** – Operates the Device Registry Database as a central service

System management sub-role:

- **Operations Governing Body** – Defines and maintains operational requirements derived from the C-ITS Supervision Body. It coordinates and manages incidents reporting from the Operations Manager and to the C-ITS Supervision Body, as well as ensures compliance of the operation managers with the requirements. It defines the minimum de/commissioning requirements for operational performance, and implements necessary security changes

System operations sub-role:

- **Operations Manager** – Implements the operational requirements published by the Operations Governing Body. It manages and reports incidents to the upper layers of the Operations Governing Body and the C-ITS Supervision Body when it is not capable
- **Trust List Manager (TLM)** – Generates and updates the European Certificate Trust List (ECTL) according to the CP and regular activity reporting to the Policy Authority for secure operations
- **C-ITS Point of Contact (CPOC)** – Handles all communication with individual root CA managers, publishing the common trust anchor and the ECTL
- **Accredited PKI Auditor** – Assesses the compliance of a PKI entity to the European certificate policy by carrying out an audit procedure

[1] To view the Certificate Policy for Deployment and Operation of European C-ITS, visit: https://ec.europa.eu/transport/sites/transport/files/c-its_certificate_policy_release_1.pdf.

[2] To view the Security Policy & Governance Framework for Deployment and Operation of European C-ITS, visit: https://ec.europa.eu/transport/sites/transport/files/c-its_security_policy_release_1.pdf.

Overview of Analogous Ownership and Governance Models

This section provides high-level information on ownership and governance models across multiple industries and domains to gain perspective on deployment and governance approaches. Refer to the Literature Scan Report for additional examples of analogous ownership and governance models.

CA/Browser (CA/B) Forum

Overview: The CA/B Forum was organized as a voluntary group of commercial CAs, vendors of Internet browser software, and suppliers of other applications that use digital certificates for SSL/TLS and code signing. Forum members worked closely in defining the guidelines on how to implement best practices as a way of providing heightened security for Internet transactions and creating a more intuitive method of displaying secure sites to internet users. PKIs that meet the criteria of one or more product vendors are called "publicly trusted." The forum has a charter detailing its purpose, membership requirements, and policy change and voting process. The US Government is an associate member (non-voting status) but is developing a publicly trusted PKI and, when approved, could apply for voting membership.

The CA/B Forum derives its Policy Authority from independent decisions by product vendors to enforce policies for inclusion of PKI roots in public trust stores in the vendor's product. PKI providers adhere to the policies because it allows their customers to obtain certificates for their web servers or code signing operations, which will be trusted in products. Without that trust, users see warnings and are advised not to trust web sites or code that does not chain up to a root trusted by the product.

Comparison to the SCMS: The CA/B Forum performs the policy development portion of the SCMS Manager function. It does not operate or provide oversight and governance of the PKIs which adhere to the policies developed by the Forum. It also does not have any role in the certification of the products consuming the certificates or the implementation of misbehavior and revocation processes beyond specifying the requirements for them as part of the policy.

> **Best Practices and Takeaways:** The policy development process provides an appropriate level of transparency to ensure that the policies properly balance security and cost. While the distributed oversight and governance model simplifies roles and responsibilities, it also presents the potential for certificates from compliant PKIs to fail because they did not meet a specific vendor requirement that may not be a requirement of other product vendors.

Internet Corporation for Assigned Names and Numbers (ICANN)

Overview: ICANN was a result of the global internet expansion and is responsible for coordinating the maintenance and procedures of several databases related to the namespaces of the Internet, ensuring the network's stable and secure operation. National Telecommunications and Information Administration (NTIA) issued a proposed rulemaking requesting comments around certain actions to privatize the management of Internet names and addresses allowing for competition and to facilitate global participation in internet management. It proposed issues relating to Domain Name System (DNS) management, including private sector creation of a new nonprofit corporation managed by a globally and functionally-representative board of directors. ICANN was formed in response to this policy. ICANN managed the Internet Assigned Numbers Authority (IANA) under contract to the Department of Commerce, and pursuant to an agreement with the Internet Engineering Task Force. NTIA reached an agreement with ICANN to complete the transition of the technical coordination of the DNS to a private-sector led model, and contains provisions to ensure accountability and transparency in ICANN's decision-making with the goal of protecting the interests of global internet users, as well as mechanisms to address the security, stability, and resiliency of the Internet DNS.

Comparison to the SCMS: ICANN was initially established by the federal government, and transitioned to a private-sector led model. The SCMS could have a is similar transition. The SCMS PoC was initially established by the USDOT and CAMP to support government funded research efforts; however, the USDOT has pivoted to using a commercially available root to support research and pilot projects. While the full-scale SCMS model is still to be determined, the model could build upon the USDOT's past efforts, similar to the deployment and maturation of ICANN. Both the ICANN and the SCMS have a diverse stakeholder group. ICANN relies on their diverse stakeholders to help develop policies. Similar to the ICANN, the diverse SCMS stakeholders could help shape the development and implementation of future policies.

> **Best Practices and Takeaways:** ICANN's transition from public to private is a unique example. NTIA issued a proposed rulemaking to privatize the management of Internet names and addresses that allows for the development of competition and facilitates global participation in Internet management as well as addresses a variety of issues relating to DNS management. The proposed rulemaking allowed stakeholders to provide feedback on the development of the ICANN, like the organizational structure.
>
> ICANN's policy-making process uses a multi-stakeholder model that places citizens, industry, and government on an equal level. Unlike traditional top-down governance models, where governments make policy decisions, the multi-stakeholder approach allows for bottom-up, consensus-driven policy-making. Policy recommendations are developed and refined by the ICANN community through its supporting organizations and influenced by advisory committees composed of volunteers globally

Vehicle Information and Communications System (VICS)

Overview: VICS was originally sponsored by the Japanese National Police Association, Ministry of Construction, and the Ministry of Posts and Telecommunication to develop a national system for the provision of traffic information (including road work, accidents, congestion, and travel times) to vehicle-based terminals. It developed the early guiding policies for the VICS system through a collaboration between the sponsoring ministries and the participating organizations (e.g., car makers, equipment manufacturers, academia, and other public and private organizations and institutes).

VICS is governed by a combination of ministry policies, usually jointly developed by the ministries associated with or responsible for a given technical area and the industries who are responsible for implementing the system. These policies guide the establishment of P3s such as the VICS Center. The companies that provide staff for the center also sit on the management board and provide the overall governance implemented jointly between the government ministries who have established the operation and the private companies, institutes, and universities that operate it. The cooperative nature of Japanese society, and the general level of trust between the various parties facilitates the effectiveness of this approach.

Comparison to the SCMS: VICS is not a security management system, and thus there is very little functional similarity between the VICS center and the SCMS. There is, however, substantial similarity between these two operations in terms of participation and the constraints under which the participants carry out their work. For example:

- Like the SCMS, in order to provide services to all users, VICS equipment must be interoperable and must be tested for compliance with communications and data specifications.
- Like CVs in general and the SCMS in particular, the value of VICS lies in its widespread adoption and use and, as a result, it is difficult to assign a value to use of the system by any single user. As a result, the costs of the system need to be borne widely, and it is also seen as infeasible to assess and collect user fees individually

> **Best Practices and Takeaways:** Trust and cooperation between the government and the industry companies, and among the private business entities, are essential for the VICS governance model to work. The success of VICS has been based on the cooperation of private industry in the development, marketing, and sale of VICS-compliant terminal equipment. Japan is a small country with a homogenous culture and deeply subscribed beliefs to collectively contribute and even sacrifice for the benefit of the society. These factors may have played a role in the success of this governance model

Ownership and Governance Models Considerations and Factors

Range of Governance Models

Figure 6: The Full-Scale Deployment SCMS Ownership and Governance Models Range from Increasingly Public to Increasingly Private

The SCMS technical components and SCMS Manager ownership and governance models can range from completely public to completely private. There are many potential SCMS Manager and broader SCMS ecosystem ownership and governance models based on the desired – and potentially necessary – public and private involvement. Workshop participants will work together in diverse groups to identify feasible models that serve the public's best interest relative to cost, security, and privacy, all while still recognizing the realties and needs of a fair and competitive marketplace. Each model will have its own strengths and weaknesses, along with specific implementation challenges. It is also important to understand that the model does not have to be a static. For example, it could evolve from an initially completely government owned and operated model to a version where the government still has oversight and authority but the SCMS is primarily operated by private entities. There can also be various levels of public and private involvement throughout the various SCMS technical components and through the SCMS Manager based on the necessary resources for implementation. During the workshop, we will use public interest objectives and design/deployment attributes and criteria to frame discussions and activities around model development and implementation.

Purely as examples, we developed a few high-level deployment models to help participants start thinking about what ownership and governance may entail. When reviewing these examples, please keep in mind these five models can have many variations and combinations of ownership and governance approaches across the ecosystem, as well as within the SCMS Manager role. Participants are in no way restricted to these models when developing recommendations during workshops.

Completely Public: The Federal government maintains complete ownership of the SCMS Manager and ecosystem, and could establish a new office to manage the SCMS, or build upon existing agencies. The government is responsible for funding the SCMS, which would need a large up-front appropriation for initial deployment as well as legislation for a new tax or fee to ensure sustained funding for management and operations. Operational aspects (e.g., deploying roots, standing up electors) of the SCMS could be established by the government or be contracted to an external entity. The government could also contract with an entity or multiple entities to build and deploy the SCMS technical components to ensure a functional and secure system that maintains vehicle owner/operator privacy. The government would also need to lead the development of an overarching PKI policy, which enables implementation of additional roots that can conform to the overarching policy. This could be accomplished by contracting out the development of the Certificate Policy (CP) or partnering with a separate government agency.

Government-led Public-Private Partnership (P3): The Federal government could lead the initial deployment of the SCMS Manager and larger ecosystem, and potentially facilitate the development of an industry consortium. The consortium would assist in developing the SCMS Manager charter and initial organizational structure skeleton for implementation. The government could also stand up a single root for initial implementation and other functions/components with contractor support. The government-led consortium could develop an overarching PKI policy, enabling the implementation of additional roots. The government could also lead coordination efforts with companies offering commercial certificate services to bring their root CAs and component infrastructure into compliance with the CP. Eventually, the government could transfer oversight and responsibility to a newly developed industry-led SCMS Manager through a memorandum of understanding (MOU).

P3 Concession: The Federal government could lead the initial deployment of the full-scale SCMS and define governance policies through stakeholder engagement, resulting in a government-defined CP. The government could also establish its own root CA(s) along with policies and requirements that everyone chains back to this particular root (or one of multiple valid roots). The government would also need to grant concessions to own and operate SCMS components. If the SCMS Manager is government-led, there would need to be a capability to develop requests for proposals or cooperative agreements, as well as evaluate responses to determine compliance with the CP and the best interest of the government and public. The government could also provide loans or a percentage of the initial deployment cost to accelerate deployment. If the government determines that there is a high-level of competition to provide SCMS component services, they could require a fee for private entities to be granted various levels of concessions. This fee could be used to support the SCMS Manager policy development, oversight, and enforcement activities, along with any components that the government owns and operates.

Industry-led P3: The Federal government serves in an oversight role in the SCMS ecosystem and as the facilitating agent in establishing the SCMS Manager. The government could also facilitate the development of the SCMS Manager charter, organization of initial consortium/consortia, and planning sessions for industry stakeholders. The government could also issue MOUs to the industry consortium to lead the SCMS Manager as a non-profit (or potentially for-profit with restrictions). The industry-led SCMS Manager would be responsible for working with private industry in establishing electors, standing up a root (or roots) for initial operations, and evaluating proposals to establish and operate additional roots and other functions. Depending on the system structure, the industry-led SCMS Manager could then develop initial policies, such as an overarching PKI policy, to enable implementation of additional roots that conform to the overarching policy.

Completely Private: Industry leaders would be responsible for establishing a consortium, which could be facilitated by the Federal government. The government may become a potential member (e.g., seat on an executive/governance board and/or advisory board) of the completely private SCMS ecosystem; however, without funding or an MOU, the government would likely not be guaranteed a seat. The SCMS Manager will be industry-led and will develop all policies and coordinate with private industry to stand up root(s), CMEs, and other SCMS functions. The SCMS Manager would determine the strategy to deploy additional roots and trust anchor management method as well as determine criteria for new CME owner/operators.

Public Interest Objectives

The public interest objectives, below, should be addressed and fulfilled by the selected ownership and governance model(s). Current public interest objectives consist of secure communications, privacy, availability (e.g., interoperability, redundancy, flexibility), stakeholder representation, affordability, and performance. Please feel free to introduce additional objectives for discussion during the workshop..

Table 3: Public Interest Objectives

Public Interest Objective	High-level Examples (to ignite additional thinking and ideas)
Secure Communications — Security is dependent on technical design and policies, which must ensure security of the system and data regardless of the ownership and governance structure. The USDOT would likely be challenged to provide any oversight in a completely private model. A completely public model may not be appropriate to rapidly respond and evolve based on identified vulnerabilities, threats, and technology advances.	• The governing entity must pay special attention to policy development and apply the appropriate controls for trust anchors (e.g., electors and root certificate authorities) • Regardless of the ownership and deployment model, the PKI policy must detail the certificate policy to ensure security within the SCMS itself and across the SCMS ecosystem. This policy must be enforced through audits and accredited device certification labs
Privacy — Privacy is dependent on technical design and policies, which must ensure an appropriate level of vehicle and operator data privacy regardless of the ownership and governance structure. Based upon SCMS Manager and CME ownership, there may be increased privacy levels (or perceived differences) depending on government and private sector involvement. The government could focus its involvement on maintaining security, privacy, and adequate stakeholder representation.	• Depending on the perspective, users may perceive heavy government involvement in ownership and governance as a potential violation of privacy. Users may perceive a model with no government involvement as lacking in proper controls for protecting user data • The technical SCMS architecture preserves "privacy-by-design" and the SCMS Manager ensures separation of SCMS technical components to maintain privacy based on the final ownership and governance model
Availability (e.g., interoperability, redundancy, flexibility) — Valid certificates issued by the SCMS must be available to EEs to ensure a functioning V2X communication system that provides safety benefits. The root structure and trust anchor management method, as well as the technical deployment of other CAs, will greatly impact system availability, interoperability, redundancy, and flexibility. These factors will also determine the specific information required within PKI policies. Based on the technical design structure, the SCMS Manager will need to develop the appropriate, detailed policies to ensure that the system, no matter the root and trust anchor structure, is readily available to enable trust among EEs.	• A public model may have less redundancy and flexibility than models with more private involvement and competition, provided that the P3 and completely private models enforce policies for efficient trust anchor management • Models that enable private sector competition to provide services may have the ability to provide better levels of redundancy and flexibility to respond to market needs
Stakeholder Representation — Stakeholder representation during the full-scale SCMS technical component implementation and deployment process, and in the SCMS Manager governance and operational oversight activities, will help ensure transparency and trust in the system by the government, the private sector, and the general public. The SCMS Manager must balance stakeholder input with the need for timely development of technically feasible and responsible policies.	• Certificate policy drafts could be released for public comment • The SCMS Manager could have a tiered membership model where various stakeholder groups have access to information and knowledge of manager activities • The SCMS Manager could have an advisory board to ensure subject matter experts can provide input in developing policy and governance approaches
Affordability — The technical design (e.g., initial single root with plan to introduce other roots); ownership (e.g., P3 non-profit SCMS Manager); and policies that enable competition will greatly impact the system's affordability. Deployment and implementation plans for the full-scale SCMS must consider initial funding sources, sustainment of funding sources, and how internal organizational and external industry governance affects efficiency.	• Create a competitive marketplace where private entities are authorized to provide services with the approval of the SCMS Manager • Arbitrarily limit the number of service providers to reduce the cost of overhead and governance activities

Public Interest Objective	High-level Examples (to ignite additional thinking and ideas)
Performance —Performance can be viewed from an SCMS technical and functional perspective, as well as an organizational and governance perspective. The final SCMS technical design and PKI policies will determine the technical and functional performance of everyday SCMS operations. Ownership and whether the SCMS ecosystem is based on profit, non-profit, or potentially a combination of features will influence organizational and governance performance within the industry.	• A not-for-profit, industry consortium-led SCMS Manager with Federal government representation that develops policy and performs governance activities for an SCMS ecosystem with multiple private, for-profit owner-operators of SCMS technical components • A Federal government office with industry advisors that serves as the SCMS Manager and owns/operates a root CA or multiple root CAs, and grants concessions for entities to own/operate other SCMS technical components

Design and Deployment Criteria and Attributes

The design and deployment criteria and attributes described in Table 4 are considerations that the selected model will greatly influence and, at the very least, must be thoroughly discussed during model development. Current design and deployment criteria consist of ownership, funding, policy creation and approval, oversight and auditing, trust anchor management, Misbehavior Authority management, EE certification method, legislation and regulation, competition, and overall risk. Please feel free to introduce additional criteria and attributes for discussion during the workshop. Please note that the high-level examples and tradeoffs in Table 4 are only examples to help participants start thinking about these attributes. Of course, there are multiple ways to address each criteria and attribute. Participants should not feel constrained by the examples provided.

Table 4: Design and Deployment Criteria and Attributes

Design and Deployment Criteria and Attributes	High-level Examples
Ownership — It is important to understand that ownership models may evolve based on the needs of the system and the appropriate level of government oversight. There could be different ownership models to various components within the SCMS ecosystem. For example, the SCMS Manager could be an entity owned and operated by the Federal government, while select CMEs could be owned and operated by private entities.	• Ownership by the Federal government • Ownership by the government with potential sale or transfer to industry. The government could maintain "ownership" and authorize vendors to operate or grant concessions • Ownership of the SCMS Manager by an industry consortium with various private entities owning and operating the SCMS components
Initial Funding — The full-scale SCMS deployment and implementation plan will need to address initial stand-up funding and sustainment funding. Initial stand-up funding will be largely determined by ownership. For example, a completely private model may fund the initial deployment of the SCMS Manager through an implementation fund provided by consortium members, while private entities completely fund technical components.	• Solely funded by the Federal government through general appropriations or reallocation of state department of transportation appropriations • Cost share between the Federal government and industry consortium • Solely industry funded
Sustainment Funding — Sustainment funding could be generated by similar methods across various ownership models (e.g., fee automatically included within the purchase of a new vehicle); but, there could also be different approaches for funding the SCMS Manager and various technical components. The way in which the sustainment funding flows to the SCMS Manager and CMEs will depend on the root CA structure and ownership model.	• Automatic fee for each device included within the vehicle price. The revenue from this fee is used to pay for certificate services and membership dues to the SCMS Manager • Operational costs funded by the Federal government • Annual fee paid through taxes (pay-as-you-go) • Accreditation and services fees • Auditing fees
Policy Creation and Approval — The entities that take the lead on the initial SCMS Manager stand-up would likely lead the initial PKI policy development. The SCMS Manager should develop policies with a set approval process and determined level of approval. Chartering the SCMS Manager with initial policies already developed may help accelerate the stand-up of CMEs. These policies could follow the structure outlined in Request for Comments (RFC) 3647, which is the PKI industry standard. The personnel make-up and structure of the SCMS Manager and the approval level entity will depend on SCMS Manager and CME ownership.	• Government developed policies released for public comment • Industry consortium (e.g., industry-led SCMS Manager) creates a task force to develop and update policies with the help of an advisory board and with the approval of a board of directors, in which the Federal government may or may not have a seat
Oversight and Auditing — The type of ownership will determine the type and level of SCMS oversight. If there is specific legislation or regulation that provides authority to a SCMS Manager in some way, or specifies use of a specific root for example, these actions would need to specify the entity providing oversight for the SCMS Manager and larger SCMS ecosystem (e.g., Federal Communications Commission, National Highway Traffic Safety Administration).	• Congressional-directed oversight and auditing, if the SCMS technical component and SCMS Manager functions are federally owned and operated • Contract out third parties to conduct audits of technical SCMS components, potentially with intermediate inspections based on the level of oversight

Design and Deployment Criteria and Attributes	High-level Examples
Trust Anchor Management — The full-scale SCMS must have an effective method to manage trust anchors no matter the technical design, ownership model, or governance model. The current default trust anchor management method is the elector concept. The SCMS Manager must develop policies and procedures for trust anchor management to ensure security within the selected root structure and technical design. It is important to consider that the trust anchor management function is a core function and ownership/operation would ideally be separate from the SCMS Manager. The more important question is how many electors are necessary without becoming cost prohibitive.	• Electors managed by the Federal government • Electors ownership and operation split among industry and the government • Elector ownership and operation split among the SCMS Manager, industry, and the government
EE Certification Method — EEs will need to meet certain PKI requirements, as well as functional and performance requirements, for initial enrollment and to maintain enrollment status with the SCMS regardless of the ownership and governance model. However, the level of control of the SCMS Manager over the certification process will depend on the established policies.	• Certification labs are accredited by the SCMS Manager. After accreditation, labs can provide services to suppliers for type certification. The device owner (e.g., OEM, auto dealer) must provide proof of type certification to the Device Configuration Manager to enroll and provision the device • OEMs and other device manufacturers/product integrators self-certify devices with support from suppliers and report compliance to the SCMS Manager. The SCMS Manager has the authority to "spot-check" EEs to ensure compliance
Misbehavior Authority Management — The Misbehavior Authority (MA) is a critical element of the current design that fulfills two roles: implement the mechanisms for identifying bad actors and subsequently removing them from the system through certificate revocation. On the one hand, it must operate a sophisticated data mining and analysis operation to detect misbehavior and coordinate with SCMS entities to revoke the detected misbehaving vehicles. On the other hand, it may also operate as an enforcement body or coordinate with such bodies to assure that identified misbehavers are appropriately dispositioned. The MA is likely a central, stand-alone technical component of the SCMS ecosystem; however, it is possible that the two roles may be split between multiple operators.	• The SCMS Manager stands-up, owns, and operates the Misbehavior Authority internally • The SCMS Manager stands-up the initial MA capability and auctions it off to a single service provider • The SCMS Manager contracts with a single (or multiple) private service provider to stand-up and operate the MA • The SCMS Manager sets the minimum MA policies within the SCMS PKI policy and allows the first service provider (or group of service providers) to fulfill the necessary policies to stand-up and operate the MA

Design and Deployment Criteria and Attributes	High-level Examples
Legislation and Regulation — Depending on the ownership and governance model, the Federal government may need to enact new legislation and/or regulation, such as granting authority to new government entities and/or the SCMS Manager, or levying new taxes and fees.	• Possibly bestowing the appropriate authority to stand up a SCMS Manager, which may or may not also provide oversight for the entire ecosystem • Regulation may also be necessary to create a technical mechanism to ensure early deployments are carefully managed and vetted until the system is mature (e.g., a single specific root is considered valid for initial deployment)
Competition — The ownership and governance model will greatly impact competition within the new SCMS ecosystem. Depending on the final goals and objectives of the full-scale SCMS and its stakeholders, for example, the industry and government may not initially want competition to ensure that the nascent system is under tight oversight and control. In this case, the SCMS Manager and governance board could gradually introduce the ability for external entities to offer CME services if these entities conform to the SCMS PKI policies and requirements. The level of competition and amount of available services will complicate governance, oversight, and auditing, which will increase the workload for the SCMS Manager and the aligned oversight entity, if one exists.	• All competition is established through federal contracting practices to potentially operate SCMS functions over a specific period • Competition to provide all SCMS services is completely open. The owner-operator of the component would only need to be approved to provide services by the SCMS Manager
Adaptability and Resiliency — Adaptability and resiliency correspond to multiple public interest objectives, including performance and availability. The SCMS Manager should have the capability to address coordination and cooperation among technical component operators and address incidents.	• The SCMS Manager has an operational oversight capability that has some level of insight into technical component operations • The SCMS Manager has open lines of communication with all technical component owner-operators to ensure the ability to coordinate incident response • Multiple root CAs to ensure no single point of failure

Design and Deployment Criteria and Attributes	High-level Examples
Overall Risk. Risk within the Full-Scale Deployment SCMS ownership, governance, and operational models will take many forms. For example, there will be financial risk for the entities that stand-up and own the SCMS Manager or CMEs. There is also operational risk. For example, what is the impact of a specific governance model and certificate authority structure on the ability of the full-scale SCMS to provide services and meet the public interest objectives?	• All financial and operational risk falls on the government in a completely public model and vice versa in a completely private model. Both high-level models could have high operational risk, which may not be feasible given the critical nature of ensuring a secure and available vehicle-to-vehicle communications system • A lower risk model may include the Federal government in some capacity, even if it is only in a minor oversight or advisory role, to ensure efficient operations while maintaining the necessary levels of security and privacy

SCMS Ownership and Governance Attributes Options

As mentioned in the beginning of the read ahead, the workshop will include team-based activities, and scenario-based tabletop exercises. This section is specific to one workshop activity where diverse stakeholder teams will be asked to construct their ideal models. We ask that you please familiarize yourself with the SCMS ownership and governance attributes options as they will be used as a basis for building a model. Also, please do not feel restricted by the options listed below. There will be an opportunity to modify, as well as create new attribute options. Reviewing this information prior to the workshop will allow more time for thoughtful discussions around a full-scale SCMS ownership and governance model.

Ownership and Governance Attributes for SCMS Structure Options

Ownership Options

Option 1 - **Majority of the SCMS components and the SCMS Manager are initially owned by the Federal Government with potential sale or transfer to industry after operations are stable.** The USDOT could maintain "ownership" and authorize vendors to operate. However, there will likely need to be established separation of operations and organizational firewalls to ensure privacy by design and security is maintained. Otherwise, there could be public backlash based on a perceived invasion of privacy.

Option 2 - **Governed by the Federal Government with root certificate authority and SCMS Manager ownership, with the remaining technical components funded and operated by private industry.** The government establishes its own Root CA(s) along with a set of policies and requirements within a Certificate Policy that everyone chains back to a particular root (or one of multiple valid roots). In this case, the root would be government owned and operated.

Option 3 - **Governed by the Federal Government, but private industry funds the SCMS technical components.** The government owns and manages the Certificate Policy and SCMS Manager. In this case, the government would essentially control entry to the SCMS ecosystem and grant concessions to private enterprises to own and operate SCMS components. In this model the government would control the SCMS, but it would not actually own and operate the technical SCMS infrastructure.

Option 4 - **Industry consortium ownership, with a charter established by the Federal Government.** The government facilitates the full-scale SCMS deployment effort through the development of a charter, organization of initial consortium/consortia, and planning activities. Government establishes a Memorandum of Understanding with an industry consortium to lead the SCMS Manager as a nonprofit entity (or potentially for-profit with restrictions). Industry leads the stand up of electors, root, and other SCMS functions and develops overarching PKI policies.

Option 5 - **Industry consortium ownership, with no Federal Government involvement.** Industry organizations and consortia own the entirety of the SCMS technical components and SCMS Manager. The government plays a minimal role, as requested by industry.

Initial Funding Options

Option 1 – **Federal Government plays a major role in funding the stand-up of the SCMS Manager, Root CA, and CMEs (i.e., various technical component groupings) through a departmental budget**

Option 2 – **Federal Government plays a major role in funding the stand-up of the SCMS Manager, Root CA, and CMEs through a reduction in state allocations and using that funding to provide seed funding**

Option 3 – **20/80 cost share (or other ratio), with the Federal Government funding 20 percent of startup operations and granting a concession for an organization(s) to run the SCMS Manager and other technical components**

Option 4 – **Industry consortium funding for the SCMS Manager with individual organizations responsible for technical component implementation costs**, with minimal funding support from the Federal Government to facilitate working group, consortium, and policy development. Potential sub-options:

- Implementation fund provided by consortium members
- Root CA(s) and/or other CME standup fees to fund SCMS Manager
- Tiered membership structure with required initial funding commitment
- Selling of stock

Option 5 – I**ndustry consortium funding for the SCMS Manager with individual organizations responsible for technical component implementation costs.** Industry solely funds the stand-up and implementation of the SCMS Manager, policy development activities, Root CA(s), and other technical components Potential sub-options:

- Implementation fund provided by consortium members
- Root CA(s) and/or other CME standup fees to fund SCMS Manager
- Tiered membership structure with required initial funding commitment
- Selling of stock

SCMS Manager Sustainment Funding

SCMS Manager Sustainment Funding (allow multiple options to be selected)

Option 1 – **A fee built into the price of the vehicle or other end entity.** A portion of this fee is automatically allocated to the SCMS Manager.

Option 2 – **A fee is collected as part of the state vehicle registration process and automatically allocated to the SCMS Manager.**

Option 3 – **The SCMS Manager creates a tiered membership structure with annual dues (e.g., tiered fees for technical component operators).**

Option 4 – **The SCMS Manager charges accreditation, auditing, and/or other services fees.**

Option 5 – **A miniscule fee is attached to each certificate distributed to an end entity within the ecosystem, which is paid to the SCMS Manager.**

Technical Component Sustainment Funding

Option 1 – **The Federal Government funds sustainment operations for technical components that are inherently central and not viewed as a viable business opportunity, such as potentially the Misbehavior Authority, while the owner-operators of all other technical components are responsible for funding their own operations (e.g., selling services, funded by an additional charge on each vehicle).**

Option 2 – **SCMS Manager charges a "franchise fee" for all self-supporting (i.e., non-central) technical functions, and a portion of this fee is used to support inherently central technical functions.**

Option 3 – **Federal Government underwrites the operations of the inherently central technical components of the system**, and those components charge all user functions for their services to offset the operational costs with the objective of a net zero operating cost to the Federal Government.

Option 4 – **Misbehavior management functions are distributed to the state motor vehicle management authorities (e.g., DMVs) who contract for some of the technical services.** Costs to support this operation are added to state vehicle registration fees.

Option 5 – **All technical components are responsible for funding their own operations** (e.g., an additional charge on each vehicle, selling services, sale of collateral services offered on a subscriber basis, such as technical providers gaining access to vehicle owners and selling additional services in addition to free or subsidized security services).

Competition Options

Option 1 - **The Federal Government deploys the SCMS technical components and auctions (or sells the right to manage and operate) the components, while maintaining control of the SCMS Manager.** The Federal Government continues to maintain overall control of the system for policy development and granting new service provider entrants.

Option 2 – **The Federal Government grants concessions, and the concessionaires implement and operate components and the "SCMS Manager" functions.** The government would continue to play a major role in allowing new entrants into the system based on their positions within the Board of Directors and involvement within SCMS policy development.

Option 3 - **Competition to provide all SCMS services is completely open.** The owner-operator of each component would only need to be approved to provide services by the SCMS Manager by meeting the required PKI policies, which may restrict the number of various components based on demand.

Legislation/Regulation

Option 1 - **New legislation and regulation is required to authorize and fund an existing (or new) government office to set and enforce SCMS policy.** Legislation is also necessary to grant authority to auction off components of the SCMS after it is established.

Option 2 - **New legislation and budget allocation is required to authorize and fund an existing (or new) government office to set and enforce SCMS policy.** Legislation is also necessary to grant authority to award concessions.

Option 3- **Policy is required to authorize a government entity (e.g., FCC, USDOT) to participate in and provide input to policies for SCMS.**

Option 4 – **Potentially some regulation may be required to assure that overall public interest objectives are met.**

Option 5 – **No legislation or regulation is necessary.**

Ownership and Governance Attributes for SCMS Manager Roles and Responsibilities Options

Initial Policy Development

Option 1 – **A Federal Government agency develops policies with input from public comment.** The Federal Government leads the development of creating and updating policies and releases policies for public comment unless releasing policies would negatively impact security or privacy.

Option 2 – **A Federal Government agency develops policies as a collaborative effort with standards organizations and industry working groups of stakeholders and PKI experts.**

Option 3 – **A standards organization or industry-led working group or consortium develops policies with input from function-specific industry SMEs and Federal Government funding support.**

Option 4 - **A standards organization or industry-led working group or consortium develops policies with input from function-specific industry SMEs. The Federal Government could provide input to policy development but would not provide funding.**

Recurring Policy Development and Approval

Option 1 – **The SCMS Manager has a policy review and approval process based on a set schedule, where a task force or working group is convened for the specific purpose of policy review and updates, but a federal government agency is the approval authority.** The task force or working group consists of stakeholders and PKI experts from an SCMS Manager advisory board and SCMS Manager member organizations. A variation of this could have a SCMS Manager with a full-time policy development shop responsible for managing this process.

Option 2 – T**he SCMS Manager has a policy review and approval process based on a set schedule, where a task force or working group is convened for the specific purpose of policy review and updates, and a board of directors (with a seat or seats designated for the Federal Government) is the approval authority.** The task force or working group consists of stakeholders and PKI experts from an SCMS Manager advisory board and SCMS Manager member organizations. Any member organization can submit a policy update with justification for review at any time. A variation of this could require a set percentage of approval from member organizations rather than the board of directors holding all approval authority.

Option 3 – T**he SCMS Manager has a policy review and approval process based on a set schedule, where a task force or working group is convened for the specific purpose of policy review and updates, and a board of directors (with no seat for the Federal Government) is the approval authority.** The task force or working group consists of stakeholders and PKI experts from an SCMS Manager advisory board and SCMS Manager member organizations.

Oversight and Auditing

Option 1 - **The Federal Government would provide oversight in some capacity (e.g., FCC, USDOT) in a public-private partnership, such as having a seat on the SCMS Manager Board of Directors.** The government may contract out a third party to conduct audits and could require intermediate or random inspections. Once a component is operated by industry, that entity would be responsible for contracting for audits with third parties based on the established PKI policies.

Option 2 – **Industry polices themselves through the SCMS Manager and internal industry pressure.** Entities within the ecosystem are responsible for contracting with third parties for audits based on the established PKI policies.

Trust Anchor Management

Option 1 - **Elector ownership and operation is split among industry entities (e.g., PKI services companies) and Federal government to ensure checks and balances in adding and removing electors and roots. In this case, the SCMS Manager does not own or operate any electors.** However, PKI policies set by the SCMS Manager govern the requirements to own and operate an elector, as well as the processes to add and remove electors and roots.

Option 2 - **Elector ownership and operation is split amongst the SCMS Manager, industry entities, and the government.** PKI policies set by the SCMS Manager govern the requirements to own and operate an elector, as well as the processes to add and remove electors and roots.

Option 3 – **Elector ownership is split among industry entities and the SCMS Manager, with no ownership or operation by the Federal government.** PKI policies set by the SCMS Manager govern the requirements to own and operate an elector, as well as the processes to add and remove electors and roots.

Option 4 - **Elector ownership and operation is split among industry entities. In this case, the SCMS Manager does not own or operate any electors.** PKI policies set by the SCMS Manager govern the requirements to own and operate an elector, as well as the processes to add and remove electors and roots.

Option 5 – **An industry-led model implements a trust anchor management method other than the elector model…**

Misbehavior Authority Management

Option 1 – **The Federal Government stands-up, owns, and operates the MA**, including strategies for misbehavior detection and enforcement

Option 2 – **The SCMS Manager stands-up, owns, and operates the MA internally.** The SCMS Manager sets up all misbehavior detection and enforcement strategies

Option 3 – **The SCMS Manager stands-up the initial MA capability and auctions it off to a single service provider**

Option 4 – **The SCMS Manager contracts with a single private service provider to stand-up and operate the MA**, based on set approaches for misbehavior detection and enforcement developed by the SCMS Manager

Option 5 – **The SCMS Manager contracts with multiple private service providers (e.g., data analytics firm, automotive industry group) to stand-up and operate the MA**, based on set approaches for misbehavior detection and enforcement developed by the SCMS Manager

Option 6 – **The SCMS Manager sets the minimum MA policies within the SCMS PKI policy and allows the first service provider (or group of service providers) to fulfill the necessary policies to stand-up and operate the MA**

Option 7 – **The SCMS Manager sets the minimum MA policies within the SCMS PKI policy and works with state DOTs who provide enforcement functions within their current motor vehicle management authorities, and who contract with service providers to perform data mining functions for misbehavior identification**

End Entity Certification

Option 1 – **An industry-led SCMS Manager accredits certification test labs.** After accreditation, labs can provide services to suppliers for device type, manufacturing environment, and installer certification. The device owner (e.g., OEM, auto dealer) must provide proof of type certification to the Device Configuration Manager to enroll and provision the device.

Option 2 – **An industry-led SCMS Manager stands up its own capability for device certification to maintain control of the certification processes.**

Option 3 - **OEMs and other device manufacturers/product integrators self-certify devices with support from suppliers and report compliance to the SCMS Manager.** The SCMS Manager has the authority to “spot-check” EEs, manufacturers, and installers to ensure compliance.