National Security Credential Management System (SCMS) Deployment Support

Potential SCMS Ownership and Governance Models

U.S. Department of Transportation

Notice

1. Report No. FHWA-JPO-18-686	2. Government Accession No.	3. Recipient's Catalog No.	
4. Title and Subtitle **National Security Credential Management System (SCMS) Deployment Support: Potential SCMS Ownership and Governance Models**		5. Report Date 22 Jun 2018	
		6. Performing Organization Code	
7. Author(s) Joshua Kolleda, Joanne Thornton, Larry Frank, Scott Andrews, Tyler Poling, David Fitzpatrick, Jim Marousek		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 Draft	
		14. Sponsoring Agency Code	
15. Supplementary Notes			

16. Abstract

This report provides an overview of potential Security Credential Management System (SCMS) ownership and governance model options developed within the National SCMS Deployment Support Project. It includes content on high-level deployment model options based on initial ownership and funding, review of ownership and governance public interest objectives and design/deployment attributes with examples, an analysis of the SCMS ecosystem stakeholder groups and their motivations in deploying a full-scale SCMS ecosystem, potential Certificate Management Entity (CME) groupings and owner/operators, as well as considerations for the internal organization and governance of the SCMS Manager. This report helps facilitate stakeholder discussion on potential models and considerations, which will ultimately feed an analysis to develop deployment strategies.

17. Key Words Security Credential Management System (SCMS), Proof of Concept, Connected Vehicles, Pilots		18. Distribution Statement	
19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages 68	22. Price

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

Table of Contents

CHAPTER 5: SCMS MANAGER INTERNAL ORGANIZATIONAL STRUCTURE AND GOVERNANCE 44

ACRONYMS **60**

LIST OF TABLES

LIST OF FIGURES

Executive Summary

This report provides an overview of potential Security Credential Management System (SCMS) ownership and governance model options developed within the National SCMS Deployment Support Project. It includes content on high-level deployment model options based on initial ownership and funding, review of ownership and governance public interest objectives and design/deployment attributes with examples, an analysis of the SCMS ecosystem stakeholder groups and their motivations in deploying a full-scale SCMS ecosystem, potential Certificate Management Entity (CME) groupings and owner/operators, as well as considerations for the internal organization and governance of the SCMS Manager. This report helps facilitate stakeholder discussion on potential models and considerations, which will ultimately feed an analysis to develop deployment strategies.

Initial Ownership and Governance Models

There are three basic, high-level options to deploy a full-scale SCMS from an ownership and funding perspective: public, public-private partnership (P3), and private. However, there are many potential SCMS Manager and broader SCMS ecosystem ownership and governance model variations based on the desired (and potentially necessary) public and private involvement. Chapter 2 briefly describes the National SCMS Ecosystem and high-level potential role and responsibilities of the SCMS Manager to help prepare the reader for a description of five high-level *descriptive example* ownership and governance models for initial deployment. Of course, potential ownership and governance models are not restricted to the ones described in this section. The future model may take some elements from multiple example models, or others not explored within this report, to meet public interest and industry stakeholder objectives. U.S. Department of Transportation (USDOT) does not endorse any specific model. Chapter 2 will also describe public interest objectives that a model should fulfill, as well as design and deployment criteria with examples on how a model may address each criterion.

Models can range from completely public to completely private based on the objectives of the organization, government mandates, market needs, and many other factors. Each model will have its own strengths and weaknesses, along with specific implementation challenges. The deploying entity must balance fulfillment of public interest objectives with considerations such as cost, deployment schedule, risk, and desired government authority (if any). It is also important to understand that the model does not need to be a static selection. Along with the development of 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 SCMS a reality.

The ownership and governance models must consider the entire SCMS ecosystem, which includes the SCMS itself 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 ecosystem includes not only the SCMS technical components (i.e., certificate authorities [CAs]), but also the entities responsible for originating CV equipment and applications (including services provided to the vehicle/user), entities responsible for certifying that this equipment and these applications conform to specified requirements and standards, entities responsible for selling and provisioning

the equipment and/or applications, entities responsible for maintaining and servicing the equipment and/or applications, end users such as vehicle owners/drivers, and state and local agencies that may implement applications using vehicle-based and/or roadside equipment (RSE).

Any model developed should at least consider the following public interest objectives and model design and deployment attributes which could be fulfilled and addressed in many ways.

Public Interest Objectives

Secure Communications. Security is dependent upon technical design and policies, which must ensure security of the system and data regardless of the ownership and governance structure.

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 governmental and private-sector involvement.

Availability (i.e., interoperability, redundancy, flexibility). Valid certificates issued by the SCMS must be available to devices or end entities (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.

Stakeholder Representation. Stakeholder representation during the Full-Scale Deployment SCMS technical component implementation and deployment process, as well as 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.

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 Deployment SCMS must consider initial funding sources, sustainment of funding sources, and how internal organizational and external industry governance affects efficiency.

Performance. Performance can be viewed from an SCMS technical and functional perspective, as well as from 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.

Design and Deployment Criteria

Ownership. Ownership means the actual, physical ownership of the SCMS technical components and the SCMS Manager organization. Ownership will likely be held by the organization(s) that provides initial funding for full-scale deployment. It is important to understand that ownership models may evolve based on the needs of the system and the appropriate level of government oversight.

Initial Funding. As mentioned in the Affordability objective, the 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. Initial funding usually aligns in some way with ownership. However, the way that funding is generated and used can vary greatly. 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. Deploying entities will need to consider the specific organizations that may be most appropriate, willing, and able to fund initial deployment.

Sustainment Funding. Sustainment funding needs to be considered for the technical components and the SCMS Manager. Funding could be generated by similar methods across various ownership models (e.g., fee automatically included with the purchase of a new vehicle, the original equipment manufacturer [OEM] paying a membership fee, and OEM making a payment to the entity providing certificates); but there could also be different approaches for funding the SCMS Manager and components, depending on the ownership models (i.e., a public-private partnership would likely be funded differently than a completely private model). The way in which the sustainment funding flows to the SCMS Manager and CMEs will depend on the root CA structure and ownership model.

Policy Creation and Approval. Policy creation and approval refers to the need for an entity or group with the necessary expertise and ecosystem understanding to take responsibility for developing the PKI policies, determining what levels of authority must approve those policies, and determining the process to update and refine those processes. For example, 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.

Oversight and Auditing. Depending on the type of ownership, associated legislation or regulation, and involved stakeholders, there will be various needs for oversight of the full-scale SCMS ecosystem. Auditing of the SCMS technical components is necessary no matter the type of ownership model. For example, if there is specific legislation or regulation that provides authority to a SCMS Manager in some way, (such as specifying use of a certain root,) these actions would need to specify the entity providing oversight for the SCMS Manager and larger SCMS ecosystem (e.g., Federal Communications Commission [FCC], NHTSA).

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.

End Entity Certification Method. EEs will need to meet certain PKI requirements, as well as functional and performance requirements, for initial enrollment, and will need to maintain enrollment status with the SCMS regardless of the ownership and governance model. There will also be requirements regarding where and how the EEs are initially enrolled within the SCMS and provisioned with certificates. The requirements themselves, based on various device configurations and sub-components, will likely be determined within the PKI policy development processes. There must be a process to ensure that devices are certified or qualified in some way against the requirements, and that device manufacturing environments and installers are certified.

Legislation and Regulation. Depending on the ownership and governance model, the federal government may need to enact new legislation and regulation, such as granting authority to new government entities and the SCMS Manager, or levying new taxes and fees.

Competition. The ownership and governance model will greatly impact competition within the new SCMS ecosystem. Depending on the final goals and objectives of the 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. The level of competition and number 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.

Adaptability and Resiliency. This is the ability for the SCMS technical components and SCMS Manager to adapt to changes in demand and anticipate, withstand, recover, and evolve based on malicious and non-intentional incidents. Adaptability and resiliency correspond to multiple public interest objectives, including performance and availability.

Overall Risk. Risk within the National 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—what is the impact of a specific governance model and CA structure on the ability of the National SCMS to provide services and meet the public interest objectives?

Ecosystem Stakeholder Group Analysis

Chapter 3 identifies and analyzes the groupings of SCMS ecosystem stakeholders, documenting the team's estimation of the stake that each group holds. This report defines stake as the elements associated with the SCMS, its architecture, and its governance structure that will have a material impact on their organization, from a business perspective, an operational perspective, or a policy/public benefits perspective. Stakeholders comprising the SCMS ecosystem can be grouped into three major categories.

SCMS Implementers: These are the companies and organizations that will ultimately stand up and operate the various technical components of the SCMS. They include public key infrastructure (PKI) service providers, and various software, hardware, and administrative operations focused on providing security management services. Implementers are those companies and organizations who have made a business out of providing security management services, hardware, and software. As a result, the primary stakes for this group are directly business focused.

- **Investment:** How much company investment is likely to be required?
- **Capital Assets:** Does the company already have capital assets that it can deploy?
- **IP Assets:** Does the company have unique intellectual property assets that it can deploy?
- **ROI Expectations:** What is the expected/required return on investment or assets employed?
- **Competitiveness:** What is the competitive landscape?
- **Experience:** How qualified is the company to implement elements of the SCMS?
- **Associated Opportunities:** Are there collateral opportunities to supplement operations?
- **SCMS Internal Structure and Players:** How sensitive is the company to the internal architecture and members?
- **SCMS External Interfaces:** How sensitive is the company to interacting with clients/users?

SCMS Users: These are the companies and 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. SCMS Users are those companies and organizations whose business operations will depend upon interacting with one or more elements of 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. We also understand that there may be elements of the SCMS operation that, while not directly related to an SCMS interface, may impact these SCMS Users.

- **Material Cost:** What are the costs to meet CV and SCMS requirements?
- **Service/Logistical Cost:** What are the costs to perform required SCMS policy processes?
- **Training/Equipment Cost:** What are the costs to train staff and comply with policies?
- **Customer Experience:** What are the positive/negative experiences that impact operations?
- **Safety Benefits:** What is the customer satisfaction (or lack thereof) with the system?
- **Liability Exposure:** What is the degree of direct or indirect exposure?
- **SCMS Internal Structure:** How sensitive is the company to the internal architecture?
- **SCMS External Interfaces:** Are these interfaces cumbersome or costly?

Other Interested Parties (OIPs): These include public entities, such as the USDOT, or organizations with indirect, public, or technical interest in the connected vehicle (CV) enterprise, but who may not participate directly in the operation or use of the SCMS. There 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.

Potential CME Groupings and Owner/Operators

Chapter 4 assesses the various SCMS functions and technical components and provides a possible first order mapping among stakeholder groups and these functions. It is important to note that some of the SCMS components are mutually exclusive. That is, 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 Linkage Authorities must be separate from other entities.

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.

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.

Based on information gathered from stakeholder engagement activities, the team believes that the following stakeholder types, in addition to PKI service providers, are likely interested in owning and/or operating SCMS components depending on the ultimate ownership and governance model: federal government, non-profit entities, certification services, data analytics, administrative services providers, enforcement and compliance, vehicle manufacturers, and telecommunications services providers.

SCMS Manager Internal Organizational Structure and Governance

The SCMS Manager internal organization and governance is expected to support the development and implementation of operational policies, standards, and technologies, and to facilitate monitoring and potentially enforcing compliance with rules, regulations, and policies. The SCMS Manager will likely support and facilitate consensus-building and a bottom-up approach for continuous improvement and changes in policies, rules, and innovative ideas for optimum operation. Whatever structure or model the SCMS Manager will operate in is expected to best encourage support, cooperation, and collaboration of entities from a broad spectrum of industries with a wide range of expertise.

The internal governance structure may support and facilitate:

- Standards and policy development, promoting a sense of ownership from all participants
- Development of rules and standard operating and maintenance procedures that ensure consistency across jurisdictional boundaries
- Enforcement procedures
- Certification procedures
- User authentication and access procedures, and rules for removing a user from the system
- Processes for solving conflict among stakeholders
- Processes for setting and measuring progress toward performance standards
- Processes for identifying and addressing the evolution of technology
- Technological innovation and intellectual property protection and adaptation
- Risk management and mitigation
- Communication within the SCMS Manager's various functions and divisions as well as with all participants in the SCMS ecosystem
- Financial management and proper use of funds.

Chapter 1: Introduction to the Need for SCMS Ownership and Governance Models

1.1 Project Scope

The National SCMS Deployment Support project is intended to help identify and explore potential strategies for the establishment and governance of a National, or "Full-Scale," SCMS ecosystem. This will be accomplished through thoughtful engagement with stakeholders to seek guidance and potentially gain consensus on these strategies. Ideally, the outcome will also produce next steps and milestones to implement a strategy or strategies. The strategies will include guidance and plans around:

- Establishment of an SCMS Governance Board (or similar oversight entity, such as a Board of Directors), including definitions of functions, roles, and responsibilities
- Establishment of an overall SCMS Manager (or similar system management entity), along with definitions of 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 upon and linked to the SCMS Manager)
- High-level policies and procedures that affect the integrity and efficiency of the system as well as define and guide interactions among the various entities that make up the SCMS Manager
- 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 (such as the federal government, state governments, industry associations, etc.)
- Business and financial options for initial deployment and sustainable operations.

This report is an integral part of this project, exploring the potential SCMS ownership and governance models. It provides content on the deployment models based on initial ownership and funding; an analysis of the SCMS ecosystem stakeholder groups, potential CME groupings and owner/operators; and considerations for the internal organization and governance of the SCMS Manager. This report helps facilitate stakeholder discussion on potential models and considerations, which will ultimately feed an analysis and develop a strategy to deploy a National SCMS.

1.2 SCMS Ownership and Governance Model(s) Development

It is expected that there will be substantial growth in ubiquitous CV communications, and its security and trust must be protected. As these developments draw new suppliers into the market and address new use cases, these suppliers should have clear, consistent guidance from a formalized SCMS Manager and CMEs. These are entities that own and operate one or more SCMS functions as well as explain how devices will be granted certificates to allow them to plan for deployment in volume. Great strides have been made in establishing and operating the technical SCMS Proof of Concept (PoC), and the National SCMS Deployment Support project will address the last missing pieces— ownership, governance, management, policy, and oversight for a national model. 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 national deployment of vehicle-to-everything (V2X) devices. The SCMS may be considered an entirely new public service and, as such, will require ongoing and relevant policies, practices, auditing, oversight, and compliance to ensure efficient and effective operations.

To deploy and oversee the multifaceted SCMS, there must be an ownership and governance model or models to ensure effective oversight and continued operations. The success of these ownership and governance models will be dependent upon the mission, circumstances, and goals of the SCMS ecosystem. Furthermore, the social, political, and cultural environments can create diverse models on a global scale. The SCMS will need to account for these factors, specifically for the interoperability and collaboration with bordering countries' governance and ownership models. 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 functions; this 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 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.

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 will likely also coordinate and monitor the operations of SCMS functions. The owner or owners of the SCMS Manager and SCMS functions (or components) will also greatly influence the level and type of industry governance, and stakeholder input in the development of governing policies. An important question to answer is how the authority to govern the National SCMS will be bestowed upon the SCMS Manager, which the team begins to explore in Chapter 2.

There are three basic, high-level options to deploy a National SCMS ownership and governance model: public, public-private partnership (P3), and private. However, there are many potential SCMS Manager and broader SCMS ecosystem ownership and governance model variations based on the desired (and potentially necessary) public and private involvement. Models can range from completely public to completely private based on the objectives of the organization, government mandates, market need, and many other factors. Each model will have its own strengths and weaknesses, along with specific implementation challenges. The deploying entity must balance fulfillment of public interest objectives with considerations such as cost, deployment schedule, risk, and desired government authority. It is also important to understand that the model does not have to be a static selection. For example, it could, however unlikely, evolve from an initially completely government-owned and government-operated model to a version where the government still has oversight and authority but is primarily operated by private entities.

1.3 National SCMS 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 to making the National SCMS a reality. Depending on the selected model, an implementation plan would contain different activities and milestones. For example, a variation of a P3

model would likely include facilitation of industry working sessions, development of industry consortia, and establishment of official agreements among key stakeholders.

The strategy would minimally include a transition plan to move from model planning to initial deployment. Implementation may include the following activities and artifacts.

- **Establishment of the National SCMS implementation work group.** Following the structure of the model planning and development process, the transition plan begins by setting the foundations for an implementation work group, industry consortium, and task force committee as necessary. These groups could be comprised of government officials and industry stakeholders needed for the selected governance model and must have a guiding organizational charter.
- **Roles and responsibilities document.** Many entities will be involved in the implementation of a National SCMS. To ensure all necessary entities have a role and that the relevant skill sets are covered, the transition plan should include a 'Roles and Responsibilities' document outlining this information. This document would consider operational factors of the SCMS, 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.** A successful transition requires open and designated lines of communication among participating parties. The communications plan would detail the key individuals who will interact between the planning and implementation teams to ensure the proper levels of information sharing and transparency.
- **Project plan and timeline.** Another crucial element of the transition plan is the project plan and timeline. This will turn the "next steps" for implementation into actionable tasks for the implementation team and will include a schedule for completing each task. The project plan will ensure a seamless transition from planning into deployment. Activities within the project plan could consist of the following high-level examples with sub-tasks and owners.
  - o Establish the SCMS Manager with internal departments, including a technical operations oversight function
  - o Establish PKI policies, including those for all types of certificate authorities (CAs), registration authorities (RAs), and linkage authorities (LAs), as well as the communications between these components
  - o Establish policies for certification labs and authorize at least one certification lab to evaluate and approve components
  - o Establish initial set of electors (or other trust anchor management mechanism) with one logical misbehavior authority (MA) with a certificate revocation list (CRL) store and at least one root CA
- **Evaluation and feedback plan.** The implementation team will monitor the progress of standing up the selected ownership and governance model.

1.4   Model Development Approach

Figure 1 below shows the process used to develop the National SCMS governance models.

Figure 1: Model Development Approach

Develop model skeletons. Developing the model skeletons began with researching SCMS baseline information. The research findings were compiled into a report that provides a shared understanding of the SCMS ecosystem and how it will support trusted and private CV communications. The report provides a background of the SCMS, assumptions, design trade-offs, feasibility considerations, and other issues that may impact the ownership, governance, and operations of the SCMS entities, elements, and functions. Additionally, it includes an explanation of the necessary PKI policies to support a functioning and secure National SCMS. The report also highlights the SCMS PoC and the CV pilots. Research efforts continued with a literature scan of international V2X deployment efforts, other large and distributed PKIs across private and public sectors, and other industry ownership and governance models. The literature scan identified best practices and lessons learned in the design, development, and deployment of policy setting, governance, and accreditation organizations.

The team used the analysis from these research efforts to begin developing model skeletons. The analysis considered the current SCMS baseline, as well as best practices and takeaways from relevant efforts outside of the SCMS ecosystem. It considers potential roles and entities within the ecosystem, as well as how governance and ownership will fulfill public interest objectives. The analysis also defined design and deployment attributes that will be greatly influenced by each model. After these factors were considered, the team developed initial high-level example models.

Refine through working sessions and interviews. The team refined the initial models through several working sessions with the broader research team and USDOT stakeholders. The working sessions further defined the potential roles within the SCMS ecosystem, the public interest objectives' relationship to governance and ownership, and design and deployment attributes for each model. The team conducted interviews with various SCMS stakeholders to gather insights on the public interest objectives and model attributes, the federal government's involvement, initial and sustained funding approaches, and the stakeholders' potential role in the SCMS ecosystem.

Present and gather model feedback during workshops. These models provide a foundation for the two SCMS Deployment Support Workshops, where stakeholders will engage in activities to develop and refine ownership and governance models. Workshop participants will determine the feasibility of models and next steps for deployment. Stakeholder feedback will also help define the SCMS Manager roles and responsibilities as well as their own roles within the ecosystem.

Finalize models based on workshop outcomes. The output of the workshops will help finalize the ownership and governance models as well as help clarify the government's roles, responsibilities, and possible next steps to support the development and deployment of a full-scale SCMS.

Chapter 2: Initial Ownership and Governance Models

There are many factors that must be considered when selecting an industry ownership and governance model and planning for the subsequent deployment of that model. This chapter briefly describes the National SCMS Ecosystem and high-level potential role and responsibilities of the SCMS Manager. This will help prepare the reader for a description of five high-level _descriptive example_ ownership and governance models for initial deployment of the National SCMS. Of course, potential ownership and governance models are not restricted to the ones described in this section; the USDOT does not endorse any specific model. The reader should use these models to frame their thinking around what they perceive as the optimal model for fulfilling public interest objectives and ensuring a functional, secure, and sustainable system that maintains end-user (e.g., private vehicle owner/operator) privacy. This section will also describe public interest objectives that a model should fulfill, as well as design and deployment criteria with examples of how a model may address each criterion. Remember that these are only examples: the future model could be comprised of any number of example criteria within this document or others that have not yet been considered. Refer to the SCMS Baseline report for additional information on the SCMS functions and components.

2.1 National SCMS Ecosystem and Manager

The SCMS ecosystem includes the SCMS itself 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.

As illustrated in Figure 2 below, the current SCMS ecosystem includes the entities responsible for originating CV equipment and applications (including services provided to the vehicle/user); entities responsible for certifying that this equipment and these applications conform to specified requirements and standards; entities responsible for selling and provisioning the equipment and/or the applications; entities responsible for maintaining and servicing the equipment and/or the applications; end users such as vehicle owners/drivers; and state and local agencies that may implement applications using vehicle based and/or RSE. These entities will likely interact in some way with the SCMS functions over the life cycle of any given application and any given equipment implementation (i.e., on-board equipment [OBE], aftermarket safety device, or RSE). Refer to Chapter 3 for an analysis of the ecosystem of stakeholder groups and their potential interest in the National SCMS, as well as their needs, drivers, and potential offerings within the ecosystem. Understanding each stakeholder group's interests, concerns, and motivations for initial deployment and continued operation is critical to analyzing which entities may play a role in the actual ownership and/or operation of SCMS components and participate within SCMS Manager activities.
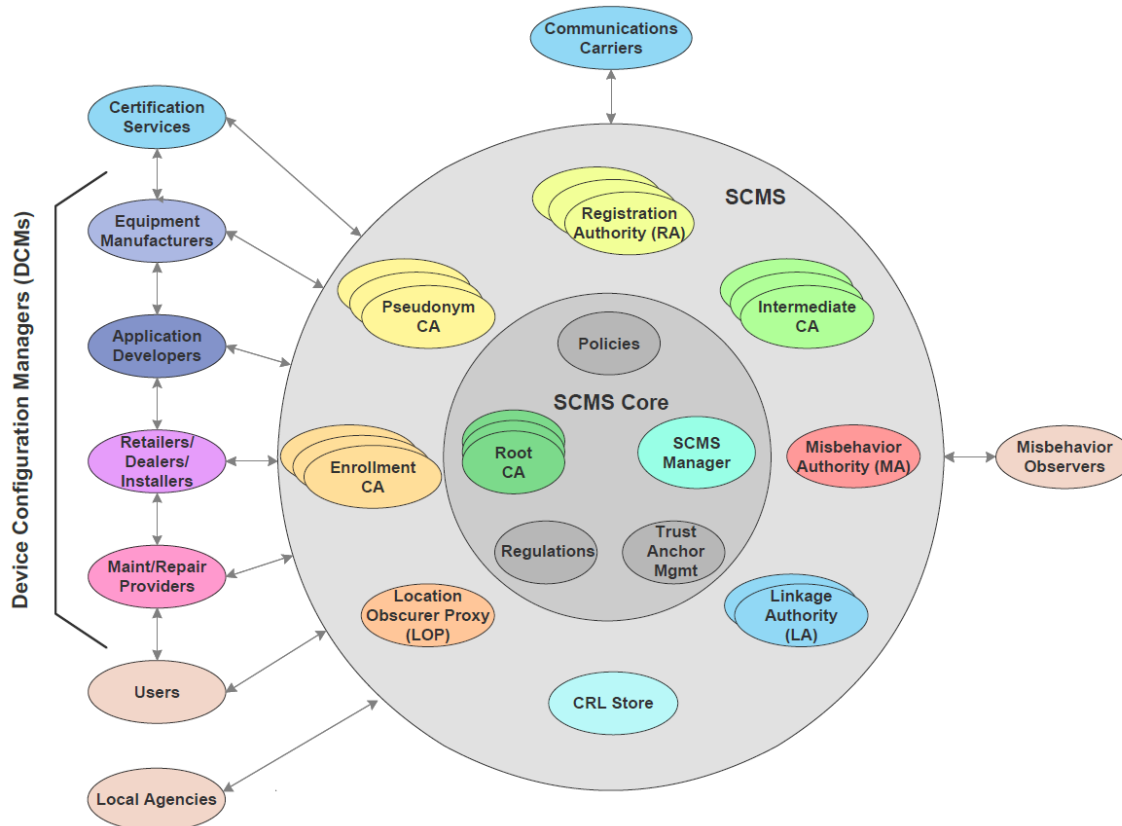
Figure 2: SCMS Ecosystem

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 (described in greater detail within the SCMS Baseline report) that will perform these security management functions over the equipment and/or application lifecycle. This includes various levels of CA; functions to detect, identify, and remove misbehaving devices from the system; and functions to facilitate the operation of the SCMS without compromising the privacy of the system users.

At the core of the SCMS ecosystem are the root CA(s), the trust anchor management function, the SCMS Manager, and the SCMS Manager's associated policies and regulations. The SCMS Manager will likely provide 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 may also serve in an ongoing capacity as the core of a governance body to coordinate and monitor operations among the various SCMS CMEs and functions. It is also expected that the SCMS Manager will likely collaborate with entities and organizations outside of the immediate SCMS, such as certification and testing shops; state and local transportation organizations (e.g., state departments of transportation and divisions of motor vehicles); vehicle inspection facilities; automotive repair shops; and automotive or device dealerships. The SCMS Manager and its governance board may also interface with other governance bodies, such as those overseeing credential management systems in Canada and Mexico, in some capacity.

The actual roles and responsibilities of the SCMS Manager can differ based on the deployed ownership and governance model or models. For example, a completely public, government-led P3 (which is an unlikely

option), or P3 Concession model, may have relatively limited participation from industry within the everyday management and operations of the SCMS Manager. An existing government office, or new entity, may completely manage policy development and oversight. However, in an industry-led P3 or completely private model, the government would likely have a limited role within the SCMS Manager, such as a seat on the Board of Directors or advisory board without the full scope of responsibilities and authority of all decisions as they would have in the other models. Refer to a detailed analysis of the potential roles, responsibilities, and organizational structure of the SCMS Manager in Chapter 5 for more information.

2.2   Summary of Example High-level Deployment Models

Within early discussion of potential ownership and governance models for this project, the team identified high-level models ranging from completely publicly owned, governed, and operated to completely private (see Table 1). These initial models have been socialized with USDOT personnel and discussed within collaboration and coordination meetings with international partners, specifically European Commission DG MOVE and Transport Canada. These models were discussed in the context of examples, realizing that government and/or industry could end up implementing any number of variations or combinations of these models depending on future government regulations (or lack thereof), as well as on how quickly the United States government and the industry as a whole progress towards large-scale CV deployments.

Each model has advantages and disadvantages, but the team believes that some variation of a P3 option may be the best option for initial deployment. However, the team continues to explore the completely public and completely private models. It is also important to consider that ownership and governance could potentially be two sets of models, one for the SCMS Manager and one for technical component operations and functions. These statements are based on the following assumptions and constraints.

- In December 2016, the USDOT released a Notice of Proposed Rulemaking requiring all future light vehicles be equipped with dedicated short-range radio communication (DSRC) to transmit BSMs. However, the recently released Executive Order 13771, "Reducing Regulation and Controlling Regulatory Cost," states that, for every 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. The USDOT still supports the deployment of V2X communications and will assist any way possible. The government may be best suited to support technical assistance and policy development efforts
- While the team reviews single- and multiple-root PKI options within this analysis, the industry already seems to be moving to a multiple root environment with multiple providers. For example, multiple PKI service providers are developing their own root CAs for V2V credential management. The models explored within this chapter default to a multiple-root PKI for this reason and to fulfill the objectives of availability, interoperability, and redundancy. Inevitably, no matter whether the structure is built around a single- or multiple-root solution, all end entities (EEs) will need to have multiple-root capability because roots will eventually retire and be replaced
- One entity or organization cannot operate every aspect within the SCMS. For this reason, there is likely a conflict of interest for the government to completely own and operate the entirety of the National SCMS. Refer to the Task 2: SCMS Baseline Summary report for additional information.
  - There must be separation of SCMS components among CMEs to maintain security and privacy of the overall system.
  - There are also inherently central components, namely the MA of the system, which should operate (and potentially be owned) completely separately from all other components within the SCMS.

While the reader reviews these models, it is important to understand that a future model may be entirely different from the high-level example models described below. Section 2.3 describes the public interest objectives and design/deployment attributes and criteria that the team used to create and evaluate potential models. Each objective and attribute contains examples of how a model may fulfill or address the objective or attribute in question. The reader will see that there is the potential for a vast number of model variations.

It is also necessary to understand that the ownership and governance structures employed in the initial deployment model will likely evolve based on the advances in technology, changes in regulation, process improvement initiatives, ability to self-sustain, and many other factors as the ecosystem matures and the number of connected (and potentially automated) vehicles increase. Advancements in technology may also impact the selected model or elements of the model, such as the PKI policy. We should consider advancement of technology and the ownership and governance models separately. However, an advancement in technology may trigger a change in ownership and/or governance. Advancements may not impact the high-level model, but are more likely to impact policies or the technical management of the full-scale SCMS as well as, potentially, the governance mechanisms of the model. We cannot predict exactly how models and technology will evolve and we do not have a baseline from which to conduct an assessment. For information on how other ownership and governance models have changed and evolved, refer to the Literature Search report.

Table 1: High-Level Example SCMS Manager and CME Deployment Models Based on Ownership and Initial Funding

Model A: Completely Public	Model B: Government-led P3	Model C: P3 Concession	Model D: Industry-led P3	Model E: Completely Private
• Stand-up new government office to serve as the SCMS Manager • Develops all policies with input from key stakeholders • Stands up electors, root, and other SCMS technical components • There must be separation of CMEs (per requirements specified in the SCMS Baseline report) so the government cannot operate all functions • May contract out operations but government maintains overall control • Initial funding for National SCMS stand-up comes from department budget • Sustainment funding through department budget. Need legislation for on-board unit (OBU) fees or other funding mechanism	• Stand-up new government office or team to provide oversight • Team develops all initial policies with input from key stakeholders and potential technical component owner/operators • Team stands up electors, root, and other SCMS functions to then be auctioned off through RFP and run based on MOU from government • Team develops new marketplace for additional CMEs to work through the SCMS Manager for validation to own/operate • Initial funding for National SCMS stand-up comes from department budget • Sustainment funding is the responsibility of the new owner/operators	• Government team to serve as the facilitating agent and governor • Team develops initial policies with input from stakeholders and potential technical component owner/operators • SCMS Manager is run as a concession (government oversees policies and operations, but concessionaire performs operations for a fee from technical components) • Government releases Cooperative Agreement RFP for implementation and operation with a federal and performer funding split • Awardee takes lead on standing up electors, root, and other SCMS functions under oversight by government • USDOT chairs the governance board to ensure public interest objectives are met • Government funding assists with deployment and operates governance/oversight office	• Government team to serve as the facilitating agent • Government to facilitate charter development, organization of initial consortium/-ia, planning sessions • Team develops initial policies with input from key stakeholders and potential technical component owner/operators • Industry takes lead on standing up electors, root, and other SCMS functions • USDOT remains on the SCMS Manager governance board to ensure public interest objectives are met • Only government funding is to assist with initial facilitation	• Industry leaders form their own consortia • Industry-led SCMS Manager develops all policies • Industry funds governance and PKI implementation • USDOT becomes a stakeholder and potential member (e.g., seat on the Board of Directors and/or advisory board) of the completely private SCMS ecosystem

2.3   Analysis of Factors and Interest Areas Influencing Ownership, Governance, and Deployment Strategies for a National SCMS

The team has identified several factors that will influence the development and deployment of ownership and governance models. Throughout the early stages of the National SCMS Deployment Support project, the team identified public interest objectives that should be addressed and fulfilled by the selected ownership and governance model. The team also identified design and deployment attributes or criteria that the selected model will greatly influence and, at the very least, should be thoroughly discussed during model development. Many of these objectives and attributes overlap or influence each other. Tables 2 and 3 list these objectives and attributes with brief descriptions and examples.

2.3.1   Public Interest Objectives

These public interest objectives were originally outlined by the USDOT and its CV and SCMS research and development efforts. The team has analyzed these objectives in the context of various ownership and governance methods and models to deploy the National SCMS. Table 2 below, provides a summary of how these objectives may be fulfilled as well as the trade-offs among potential models.

Table 2: Public Interest Objectives

Description	High-level Examples
Secure Communications. Security is dependent upon 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 tasked with providing 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, or technological advances.	• The governing entity must pay special attention to policy development and apply the appropriate controls for trust anchors (e.g., electors and root CAs). • Regardless of the ownership and deployment model, the PKI policy must detail the certificate policy to ensure security within the Full-Scale Deployment SCMS itself and across the Full-Scale Deployment 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.

Description	High-level Examples
Availability (i.e., 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 Deployment SCMS technical component implementation and deployment process, as well as 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 (SMEs) 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 Deployment 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
Performance. Performance can be viewed from an SCMS technical and functional perspective, as well as from an organizational and governance perspective. The final SCMS technical design and PKI policies will determine the technical and functional performance of everyday Full-Scale Deployment 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,

Description	High-level Examples
	and also grants concessions for entities to own/operate other SCMS technical components

2.3.2 Design and Deployment Attributes

The design and deployment criteria and attributes described in Table 3 are considerations that any ownership and governance model will greatly influence and, at the very least, should be thoroughly discussed during model development. The team has developed and analyzed these attributes in the context of various ownership and governance methods and models to deploy the Full-Scale SCMS. The table provides a summary of how these attributes may be addressed as well as the trade-offs among potential models. Please note that the high-level examples and trade-offs are only examples to help the reader start thinking about these attributes. Of course, there are multiple ways to address each criteria and attribute.

Table 3: Design and Deployment Attributes

Description	High-level Examples
Ownership. Sections 1.3 and 2.2 briefly discuss ownership models. Ownership means the actual, physical ownership of the SCMS technical components and the SCMS Manager organization. Ownership will likely be held by the organization(s) that provides initial funding for full-scale deployment. 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 also be different ownership models for various functions within the SCMS ecosystem: for example, the SCMS Manager could be an entity owned and operated by the federal government, while select CMEs are owned and operated by private entities.	• The SCMS and SCMS Manager are owned by the federal government • 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 become stable • Governed by the federal government with root CA ownership, with the remaining technical components funded and operated by private industry • Governed by the federal government, but funded and operated by private industry; the government owns and manages the Certificate Policy • 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/-ia, and planning activities • Industry consortium ownership with no federal government involvement
Initial Funding. As mentioned in the Affordability objective, the National 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. Initial funding usually aligns in some way with ownership. However, the way that funding is generated and used can vary greatly. For	• Federal government is completely responsible for funding the stand-up of the SCMS Manager, Root CA, and CMEs through a departmental budget • Federal government plays a major role in funding the stand-up of the SCMS Manager, Root CA, and CMEs, but is not solely responsible • Federal government plays a major role in funding the stand-up of the SCMS Manager, Root CA, and CMEs

Description	High-level Examples

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. Deploying entities will need to consider the specific organizations that may be most appropriate, willing, and able to fund initial deployment.	through a reduction in state allocations and using that funding to provide seed funding
	• 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
	• 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:
	   o Implementation fund provided by consortium members
	   o Root CA(s) and/or other CME stand-up fees to fund SCMS Manager
	   o Tiered membership structure with required initial funding commitment
	   o Selling of stock
	• Industry consortium funding with no federal government support

Sustainment Funding. Sustainment funding needs to be considered for both the technical SCMS components and the SCMS Manager. Funding could be generated by similar methods across various ownership models (e.g., fee automatically included with the purchase of a new vehicle, the original equipment manufacturer [OEM] paying a membership fee to the SCMS Manager, and OEM making a payment to the entity providing certificates); but there could also be different approaches for funding the SCMS Manager and various technical components, depending on the ownership models (i.e., a public-private partnership would likely be funded differently than a completely private model). The way in which the sustainment funding flows to the SCMS Manager and CMEs will depend on the root CA structure and ownership model.	• The federal government pays for sustainment operations through an agency's annual budget. This would require the government to completely own the SCMS Manager and/or technical components. • A fee is built into the price of the vehicle or other EE. A portion of this fee is automatically allocated to the SCMS Manager. • A fee is collected as part of the state vehicle registration process and automatically allocated to the SCMS Manager. • The SCMS Manager creates a tiered membership structure with annual dues (e.g., tiered fees for technical component operators). • The SCMS Manager charges accreditation, auditing, and/or other services fees. • A miniscule fee is attached to each certificate distributed to an EE within the ecosystem, which is paid to the SCMS Manager. • The federal government funds sustainment operations for technical components that are inherently central and not viewed as a viable business opportunity, such as the MA, 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).

Description	High-level Examples
	• All technical components are responsible for funding their own operations (e.g., selling services funded by an additional charge on each vehicle)
Policy Creation and Approval. Policy creation and approval refers to the need for an entity or group with the necessary expertise and ecosystem understanding to take responsibility for developing the PKI policies, determining what levels of authority must approve those policies, and determining the process to update and refine those processes. For example, 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.	**Initial Policy Development** • A federal government agency develops policies with input from public comment. • A federal government agency develops policies as a collaborative effort with standards organizations and industry working groups of stakeholders and PKI experts. • A standards organization or industry-led working group or consortium develops policies with input from function-specific industry SMEs and federal government funding support. • 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** • A federal government agency reviews certain policies and makes updates based on a set schedule. • 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 an SCMS Manager with a full-time policy development shop responsible for managing this process. • The SCMS Manager has a policy review-and-approval process based on a set schedule, and a board of directors (with a seat or seats designated for the federal government) is the approval authority. A variation of this could require a set percentage of approval from member organizations, rather than the board of directors holding all approval authority. • The SCMS Manager has a policy review and approval process based on a set schedule, and a board of directors (with no seat for the federal government) is the approval authority.
Oversight and Auditing. Depending on the type of ownership, associated legislation or	• Congressional-directed oversight and auditing for any model owned and operated by the federal government:

Description	High-level Examples
regulation, and involved stakeholders, there will be various needs for oversight of the full-scale SCMS ecosystem. Auditing of the SCMS technical components is necessary no matter the type of ownership model. For example, if there is specific legislation or regulation that provides authority to a SCMS Manager in some way, (such as specifying use of a certain root,) these actions would need to specify the entity providing oversight for the SCMS Manager and larger SCMS ecosystem (e.g., Federal Communications Commission [FCC], NHTSA).	the government hires 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. • 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. • Industry polices themselves through the SCMS Manager and internal industry pressure: entities within the ecosystem are responsible for contracting third parties for audits based on the established PKI policies.
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. Another question is how many electors are necessary without becoming cost prohibitive. Refer to the SCMS Baseline report for further explanation of trust anchors.	• Electors are owned, operated, and managed by the federal government. • 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. • Elector ownership and operation is split amongst the SCMS Manager, industry entities, and the government. • Elector ownership is split among industry entities and the SCMS Manager, with no ownership or operation by the federal government. • Elector ownership and operation is split among industry entities. In this case, the SCMS Manager does not own or operate any electors.
End Entity Certification Method. EEs will need to meet certain PKI requirements, as well as functional and performance requirements, for initial enrollment, and will need to maintain enrollment status with the SCMS regardless of the ownership and governance model. There will also be requirements regarding where and how the EEs are initially enrolled within the SCMS and provisioned with certificates. The requirements themselves, based on various device configurations and sub-components, will likely be determined within the PKI policy development processes. Requirements for	• The federal government establishes a new entity to accredit certification labs and could potentially conduct spot-check testing of devices. 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 (DCM) to enroll and provision the device. • 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

Description	High-level Examples
OBUs and RSUs will likely differ. There must be a process to ensure that devices are certified or qualified in some way against the requirements, and that device manufacturing environments and installers are certified. The level of control of the SCMS Manager over the certification process will depend on the established policies.	type certification to the DCM to enroll and provision the device. • An industry-led SCMS Manager stands up its own capability for device certification to maintain control of the certification processes. • 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.
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.	• New legislation and budget allocation is required to authorize and fund an existing (or new) government office to establish the SCMS and set and enforce policies. Legislation is also necessary to grant authority to set and collect fees to sustain the full-scale SCMS functions. • 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. • 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. • Policy is required to authorize a government entity (e.g., FCC, USDOT) to participate in and provide input to policies for the SCMS. • Potentially, some regulation may be required to assure that overall public interest objectives are met. • No legislation or regulation is necessary.
Competition. The ownership and governance model will greatly impact competition within the new SCMS ecosystem. Depending on the final goals and objectives of the 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	• The only competition would be established through federal contracting practices to potentially operate SCMS components over a set time period. Competition would again be introduced at the end of a contract period of performance, when the incumbent would need to re-compete. • 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.

Description	High-level Examples
number 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.	• 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. • 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.
Adaptability and Resiliency. This is the ability for the SCMS technical components and SCMS Manager to adapt to changes in demand and anticipate, withstand, recover, and evolve based on malicious and non-intentional incidents. Adaptability and resiliency correspond to multiple public interest objectives, including performance and availability. At a minimum, the SCMS Manager should have the capability to address coordination and cooperation among technical component operators and address incidents.	• A single root CA to maintain rigid control of the system • Multiple root CAs to ensure no single point of failure, while the SCMS Manager determines the addition of new root CAs through policy conformance and the established trust anchor management processes • 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.
Overall Risk. Risk within the National 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—what is the impact of a specific governance model and CA structure on the ability of the National SCMS to provide services and meet the public interest objectives?	The overall risk of a model will depend on the how each of the previous attributes and objectives are addressed in the context of ownership, governance, and operations. For example, all risk falls on the government in the completely public model and gradually transfers to industry in the completely private model. For operational risk, the lowest overall risk model to ensure efficient operations while maintaining the necessary levels of security may include the government in some capacity, even if it is only in a minor oversight role.

Chapter 3: Ecosystem Stakeholder Group Analysis

This chapter identifies and analyzes the groupings of SCMS ecosystem stakeholders, documenting the team's estimation of the stake that each group holds. We define stake as the elements associated with the SCMS, its architecture, and its governance structure that will have a material impact on their organization from either a business, operational, or policy/public benefits perspective. This information will be used to tailor interview questions and workshop interactions, first to confirm that we have accurately characterized their stake (and to make refinements as necessary) and then to more fully understand each element that this stake comprises. Using this information, we can then better understand how various SCMS governance models and structures may impact these stakeholders, and thereby arrive at the most workable approach.

For analysis, stakeholders comprising the SCMS ecosystem (as presented graphically above in Figure 2) can be grouped into three major categories.

- SCMS Implementers: These are the companies and organizations that will ultimately stand up and operate the various technical components of the SCMS. They include PKI service providers and various software, hardware, and administrative operations focused on providing security management services.
- SCMS Users: These are the companies and 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.
- Other Interested Parties: These include public entities, such as the USDOT, or organizations with indirect, public, or technical interest in the CV enterprise who may not participate directly in the operation or use of the SCMS.

Some organizations and companies may fall into more than one of the above categories. For example, it is possible that the USDOT may play some direct role in the SCMS, so they are an SCMS Implementer to some degree. On the other hand, because the USDOT has a large stake in the public benefits of the CV enterprise (e.g., public safety), they also play a significant role as an OIP. Another group that falls into this dual role is the OEMs. The OEMs are likely to provide or provide for some SCMS services, but they also have a considerable interest in public safety, primarily from brand-image and customer-satisfaction perspectives. For these reasons, OEMs are likely to be both Implementers and OIPs in situations where an entity falls into multiple categories. We have tried to identify their specific stakes associated with each category.

It is also important to note that these various stakes may be interdependent: they may either combine to magnify the companies' interests in one or more aspects of the SCMS architecture and/or governance structure or, alternatively they may act in counterpoint, wherein one element offsets another.

The stakes for these categories vary widely and are described below.

3.1 SCMS Implementer Stakes

SCMS Implementers are those companies and organizations[1] who have made a business out of providing security management services, hardware, and software. As a result, the primary stakes for this group are directly business focused. These include:

- **Investment**: Specifically, how much company investment is likely to be required to stand up and operate the elements of the SCMS that they are qualified to perform, and how well does this required investment fit within their business plan and strategy? Is the company prepared and able to invest sufficiently and assure success?

- **Capital Assets**: Does the company have in its possession capital assets that can be deployed to support standing up and operating the elements of the SCMS that they are qualified to perform?

- **IP Assets**: Does the company have unique intellectual property assets that they can deploy to more effectively stand up and/or operate the elements of the SCMS that they are qualified to perform?

- **ROI Expectations**: What is the expected or required return on investment (or return on assets employed) necessary for the company to be willing or motivated to engage in standing up and/or operating the elements of the SCMS that they are qualified to perform?

- **Competitiveness**: What is the competitive landscape? Who will the company need to compete with, and how challenging is the competition for operating their desired elements of the SCMS?

- **Experience**: How qualified is the company to implement their desired elements of the SCMS? Have they implemented similar elements in other contexts?

- **Associated Opportunities**: Are there collateral opportunities that may supplement the company's SCMS enterprise? For example, does involvement in their desired element of the SCMS augment some other aspect of their business?

- **SCMS Internal Structure and Players**: How sensitive is the company to the internal architecture or structure of the SCMS, and how sensitive are they in relation to the other companies that will be implementing other elements of the SCMS? For example, how important is it that they may need to establish and maintain efficient interactions with a company that they may see as a competitor?

- **SCMS External Interfaces**: How sensitive is the company to the external interfaces of the SCMS, and how sensitive are they in relation to the other companies that will be using the SCMS? For example, will the external interfaces they provide cause them to interact with existing clients (which may have a positive or negative impact on their relationships with that client)? Will the external interfaces they provide cause them to interact with existing competitors, and will this cause them to operate differently?

3.2 SCMS User Stakes

SCMS Users are those companies and organizations whose business operations will depend upon interacting with one or more elements of 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. We also understand that there 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. These stakes include:

---

[1] In this chapter we will generally refer to these companies and organizations collectively as "companies," but it is understood that these entities may include non-profit organizations and associations whose goal is to perform the required services, not necessarily to operate a business.

- **Material Cost**: Material costs are those costs associated with complying with the security specifications for CVs in general, and specifically those costs required to comply with SCMS policies. For example, if the SCMS policy requires user vehicles to store substantial volumes of data (either certificate data or, for example, misbehavior data), then the cost of the hardware required to support that data storage would be reflected in this stake.
- **Service/Logistical Cost**: Service and logistical costs are those costs associated with performing process steps required by the SCMS policies. For example, 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.
- **Training/Equipment Cost**: Training and Equipment costs are those costs associated with training staff and/or providing specialized equipment to comply with SCMS policies. For example, if the SCMS policy requires a service facility to re-provision OBE following some service repair or software upgrade, and this requires both trained technicians and specialized and certified provisioning equipment, those costs would be reflected in this stake.
- **Customer Experience**: To the extent that the customer (presumably the next customer in the supply chain) is positively or negatively impacted by operations of the company that are implemented to comply with SCMS policies, the impact on good will and competitiveness would be reflected in this stake. For example, if compliance with SCMS policies were to render an end user's vehicle inoperative, and/or if rectifying a security problem required an inordinate amount of time and effort by an end user, then the frustration and/or potential loss of business would be reflected in this stake.
- **Safety Benefits**: Safety benefits are related to customer experience in that they reflect the customers' satisfaction (or lack thereof) associated with the system (or the hardware or application used to implement the system). Safety benefits, however, are specifically related to the customer's satisfaction associated with the overall safety benefits of the CV system, and specifically with the safety benefits associated with SCMS policies as implemented through the CV security system. For example, if it is shown that a major security breach was avoided because of the system, the end users would learn that they had been shielded from that breach by the system (and by the company's product). Similarly, if the security system avoids erroneous messages that might cause a safety hazard, then the benefit provided to the customer would be reflected in terms of good will and/or competitiveness.
- **Liability Exposure**: Liability exposure is the degree of direct or indirect exposure a company providing CV equipment or services may realize. This exposure may be associated with the products or services provided by the company. Specifically, in this context, it is associated with liability arising from errors and/or omissions in complying with SCMS policies. For example, if an end user's vehicle is breached through the reception of a message that should not have been processed, or perhaps if the CV security requirements are insufficient to prevent such an attack, then liability associated with that attack would be reflected in this stake. The degree of liability is unclear at this point. For example, if an erroneous implementation of SCMS policies caused the CV system to fail to warn a driver of an imminent hazard, would the company bear any of the resulting liability?
- **SCMS Internal Structure**: How sensitive is the company to the internal architecture or structure of the SCMS, and how sensitive are they in relation to the other companies that will be implementing other elements of the SCMS? For example, does the internal structure of the SCMS result in additional costs (e.g., any of the costs outlined above), or does it cause greater or lesser liability exposure?
- **SCMS External Interfaces**: How sensitive is the company to the external interfaces of the SCMS, and how sensitive are they in relation to the other SCMS Implementer companies that will be providing those interfaces the SCMS? For example, will the external interfaces they must use cause them to interact with existing clients (which may have positive or negative impact on their relationships with that client), or will the external interfaces they use cause them to interact with existing

competitors? Additionally, are these interfaces cumbersome or otherwise difficult to use, and does the interface result in additional costs?

3.3   Other Interested Party Stakes

OIPs are those companies and organizations who have a material interest in having the SCMS implemented and in how it operates, but who may not otherwise have a direct stake in its implementation or use. 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 OIP stakes include:

- **Policy Input**: OIPs who are seeking to assure that certain objectives are met—for example, public safety, privacy, law enforcement, etc. —will have some level of interest in participating in, or assessing how SCMS policies (including governance policies) may affect, these interests. For example, consumer privacy advocates will likely be keen to assess and/or contribute to those policies that may adversely or positively impact end-user privacy. On the other hand, how SCMS policies affect the availability and/or effectiveness of the CV system to deliver safety benefits would be of interest to public agencies and, for example, insurance companies who are seeking to reduce the number and severity of automobile accidents. As a result, these stakeholders will either have a desire to participate in developing these policies or an interest in assessing how various policies may impact their objectives.
- **Public Good**: Public good is related to policy, but it would apply to those entities who are seeking to assure or promote public benefits (e.g., road safety, cyber safety). However, they may not have applicable expertise to participate in policy development or assessment.
- **Technical Elements**: Some OIPs have a stake in the technical elements of the SCMS. For example, academic institutions may carry an interest in the technical details of the systems and functions involved in the SCMS and/or the organizational details of the SCMS.
- **Standards**: Because the SCMS relies on heavily technical standards, the Standards Development Organizations (SDOs) both in the United States and abroad may all have interest in how the SCMS is composed and implemented.

3.4   SCMS Stakeholder Categories and Stake Assessment

In the following tables, we have provided our best estimate of which stakeholders may fall into which categories, as well as an initial assessment of how important each stake in that category may be for those entities based on a series of stakeholder interviews.

3.4.1   SCMS Implementers

The primary entities that are likely to be involved in implementing and operating elements of the SCMS are companies who currently provide various types of PKI services (e.g., CAs) and companies engaged in various levels of device and/or software certification.

PKI Security Services: PKI Services companies include companies typically engaged in providing various types of security functionality and services. For example, companies that today operate CAs, registration authorities, and their associated operations would be likely candidates to stand up and operate the various certificate and registration authorities in the SCMS. These companies will presumably invest in the implementation of their elements of the SCMS and will operate it as a business. As a result, they will have a

high level of interest (i.e., their stake will be substantial) in all the business-related elements described above. In addition, because they will be responsible for both interacting with other SCMS elements and, in some cases, for providing interfaces to SCMS Users, they will have a high stake in both the internal SCMS structure and the interfaces.

Certification Services: Certification services will either audit and certify certain elements of the overall SCMS or be responsible for certifying devices, software applications, and/or internal processes associated with conforming to SCMS policies. For example, these entities might audit and certify that the operations of a device manufacturer comply with SCMS policies, and then also evaluate a device design and certify that it is acceptable to be provided with certificates. In this way, the basic design is certified and the manufacturing processes are also certified. A device manufactured to that design and using those processes can be assured of proper operation under the SCMS policies, and thereby is entitled to be provisioned with certificates. These entities thus have a high stake in all business-related factors described above. They also have a high stake in the implementation of the SCMS interfaces (at least those they must interact with), and a somewhat lower stake in the internal operations and structure of the SCMS.

Device Providers: Depending on how the device configuration is performed, various entities may be responsible for implementing and providing DCM functions. Who these entities are depends entirely on where in the supply chain the devices are configured. Since it is possible to tamper with a device before it is provisioned with certificates, and because a tampered device with certificates could masquerade as a certified device, it is desirable to certify and configure the devices as early in the manufacturing process as possible. On the other hand, because the certificates have a finite life span, it may be desirable to provision certificates as late in the manufacturing cycle as possible. As a result, it is not yet possible to identify which entities are likely to perform DCM services. These may be performed by Tier 1 suppliers when they deliver CV equipment to the OEMs (early configuration), by dealers at the point of sale (late configuration), or by service centers at the point of replacement sale.

Vehicle Manufacturers: Depending on the specific OEM, the company may be likely or unlikely to directly implement and operate elements of the SCMS. Because of the variation in business priorities among OEMs, the automobile and commercial truck manufacturers may have a somewhat lower level of interest in the business-related factors associated with SCMS implementers. However, if an OEM does not take an active role in SCMS technical component implementation, it is likely that they may either directly contract with (and fund) implementers to stand up OEM-specific intermediate certificate authorities (ICAs). They may also simply contract for these services from a general services provider. In the latter case, their business interest would be somewhat lower than in the former. To the extent that OEMs are involved in the SCMS beyond purchasing services from existing entities, they may also be interested in collateral business opportunities, and they will maintain a high level of interest in the internal structure and interfaces of the SCMS. However, as their degree of involvement decreases, this interest will be more expected from the perspective of an SCMS User and promoter.

Communications Service Providers: While communications is not directly a part of the SCMS, in terms of the performance of SCMS operation, the SCMS depends heavily on communications services. For example, even if all over-the-air provisioning, updating, and reporting is performed using DSRC, the roadside and service facility systems that provide the localized communications interfaces (e.g., Roadside equipment) must still be connected to the SCMS functions, and this will be carried by Telecos and other communications service providers (i.e., via wireline, cellular, or satellite backhaul). Thus, in this case, the Telcos would have a direct pay-for-connection-and-service interest in the SCMS governance and implementation. Other delivery architectures that have been considered include a direct cellular backhaul between the vehicle and the SCMS, and a one-way satellite link that would be used to deliver certificate access information (a scheme described

by Sirius XM). The wireline/cellular approaches depend on the SCMS governance directly since the SCMS ecosystem structure will determine the direct telco customers. At one extreme would be a single SCMS operator (possibly the Federal government or a government contractor) who would presumably contract with regional telcos and/or cellular providers for service, and at the other extreme, every vehicle would require a service contract. In the latter case, it is possible that these contracts could be individual relationships between a telco and a system user, although it is also possible that such services could be bundled as a public service (much like TTYS services for the deaf are bundled) and the reimbursement for this service would be in the form of a surcharge on all phone contracts. The stakes for communications providers reside primarily in how the SCMS structure and governance affects who the communications services customers are (i.e., the government, an array of SCMS performers or individual customers) and the business arrangements.

US Department of Transportation: Because the CV enterprise is a direct result of USDOT-sponsored research and may be associated with regulation, it is likely that the USDOT will have some role in the SCMS. This involvement may be limited to high-level governance, or it may involve some level of operational activity. It may be the case that some level of investment will be required to stand up at least portions of the SCMS, especially if it is determined that there is limited business interest for commercial entities. As a result, the level of investment required to stand up and operate the SCMS will be of high interest to the USDOT. However, other business-related aspects of the SCMS (e.g., ROI) are likely to be somewhat less important. And, because the integrity of the entire CV enterprise depends on the SCMS, the USDOT will have a high level of interest in most aspects of the SCMS architecture, its operation (including interfaces), and its governance.

Table 4: SCMS Implementer Stakeholders Assessment

		SCMS Implementers				
		Vehicle Manufacturers	USDOT	Certification Services	PKI Security Services	Communications Service Providers
Stake	Investment	High	High	High	High	Low
	Capital Assets	Mid	Mid	High	High	Mid
	IP Assets	Mid	Low	High	High	Low
	ROI Expectations	Mid	Low	High	High	Mid
	Competitiveness	Mid	Low	High	High	Low
	Experience	Mid	Low	High	High	Low
	Associated Opportunities	High	Low	High	High	High
	SCMS Internal Structure	High	High	Mid	High	High
	SCMS External Interfaces	High	Mid	High	High	High

3.4.2   SCMS Users

SCMS Users comprise the largest body of the SCMS ecosystem. This category includes various types of end users, equipment manufacturers, service providers, and other entities that will interact in some way with SCMS elements through the various SCMS interfaces. These entities are:

Vehicle Owner/Operators (Private, Public, and Fleet): Vehicle owner/operators, which include private vehicles; public fleet vehicles, such as emergency vehicles; transit vehicles and public works vehicles; private fleet vehicles—for example, taxis; and eventually trucks all have an interest in the costs associated with CV systems. The initial cost concern will be the acquisition of CV equipment, but in most cases, this cost will be presumably buried in the overall cost of the vehicle and will not be particularly apparent. Depending on how the ongoing security management is structured, there may be costs that to the end users (for example, if these life-cycle costs are not included in the purchase price of the vehicle). To the extent that these costs visibly increase the cost of the vehicle, or to the extent that the end users will be required to pay for security life-cycle costs (for example, by subscribing to security updates, etc.), these end users will have a high level of interest in the costs associated with material and services. They will presumably be somewhat separated from training- and equipment-related costs, since these will be amortized across many end users. The other key areas of interest for end users, especially private vehicle owner/operators, will be the customer experience. To the extent that an end user must go through additional processes or steps to manage the security functionality of their vehicle, or to the extent that they must support additional service requirements, service interruptions, etc., they will support the CV system to a greater or lesser extent. This will be less of a concern for public and private fleet owner/operators, because they are already subject to a variety of regulations of this sort. Generally, none of these stakeholders will be overly concerned about the internal structure of the SCMS or the SCMS interfaces (unless either of these result in increased costs or inconvenience), nor are they likely to be overly concerned about liability, which they will likely assume is owned by others in the ecosystem. These end-user stakeholders obviously have a high level of interest in the safety benefits provided by the CV system, and this will include both roadway safety as well as the security and integrity of the system.

In addition, because the SCMS and the overall security system for CVs has a substantial impact on the privacy of the vehicle users and owners, these stakeholders will have a keen interest in how effectively the SCMS does its job without unduly infringing on the privacy of the driving public. Additionally, to the extent that any infringements are necessary, they will also be concerned with the nature and scope of those infringements.

Dealers and Installers: Dealers and installers may be the entities responsible for initially provisioning new equipment.[2] Dealers would be provisioning complete vehicles, and installers may be provisioning aftermarket equipment. Depending on SCMS policies, they may also be responsible for the physical security of end-user equipment prior to it being transferred to the end-user owners (i.e., vehicle purchasers): without such security, it could be possible to tamper with the equipment prior to provisioning, and this would render the certification process ineffective. These stakeholders will have a moderate-to-low interest in the cost of the equipment (unless the cost makes it difficult to sell the vehicle or equipment), but they will have a relatively higher level of interest in the process costs for such provisioning. They will presumably have a high level of interest in the training and equipment costs required to provision end-user equipment, since they will bear these costs directly. Generally, other than the fact that the CV system will make the vehicle or equipment either easier or more difficult to sell (depending on safety benefits and perceived value), these stakeholders will not be particularly concerned with the specific safety benefits provided by the system, nor will they be particularly concerned with the internal structure of the SCMS. However, because they will need to interface directly with

---

[2] Assuming that the equipment is provisioned earlier in the supply chain; if that is not the case, then these stakes will shift to that point in the supply chain.

SCMS entities during the provisioning process, these stakeholders will have a high level of interest in the SCMS interfaces in terms of efficiency and ease of use. Lastly, to the extent that they are responsible for assuring the integrity of the end-user equipment and then provisioning it with security credentials that attest to the integrity of the equipment, they may carry some level of liability. For example, if a dealer does not properly secure equipment prior to provisioning and the equipment is compromised, they may be liable in a variety of ways, ranging from end-user product liability to liability for the unlikely compromise of the entire CV security system.

Service and Parts Facilities: Service facilities and spare parts providers, which are often the same entities, will carry most of the same interests as dealers and installers. In this case, these stakeholders will, for example, be responsible for provisioning new replacement equipment used to repair a vehicle. They may also be responsible, for example, for provisioning certificates to a vehicle after installing a new application. In this case, the specific steps involved may be somewhat different, but the concerns are the same.

CV Equipment and Application Suppliers: CV equipment providers and application suppliers will be responsible for complying, at a design level, with SCMS policies through processes and design and equipment reviews or testing (for example, by a certification lab). They will also be responsible for assuring the integrity of the equipment while it is in inventory before it is finally installed into the vehicle. These stakeholders will have a high level of interest in the material costs associated with CV security, although, other than assuring in-process device integrity, the specific SCMS policies are likely to have limited impact on material costs (aside from the need to meet security requirements). These suppliers will carry some potential product liability exposure. For example, if their device carries an internal design flaw that ultimately results in a large-scale compromise of the CV system, they will presumably bear some of the liability and costs for that compromise.

Vehicle Manufacturers: As described above in relation to SCMS implementation, the OEMs will carry a high level of interest in all elements of the SCMS User stakes. They will care about costs both from a business perspective and from a customer-value perspective. They will care about safety benefits from a general-industry perspective as well as because they can use safety to make their vehicles more attractive to buyers. As with other aspects of the vehicle, they will also carry front-line product liability exposure.

State and Local DOTs: To the extent that CV applications depend on local infrastructure systems—for example, using roadside equipment to provide security updates—state and local transportation authorities may be responsible for specifying, procuring, installing, and maintaining CV equipment. In some cases, they may also be responsible for providing various safety applications that make use of the CV equipment installed in vehicles (e.g., roadside-based safety applications). Because of this, they will have a high level of concern regarding equipment costs, as well as any costs associated with managing and maintaining the equipment. They are likely to be somewhat less concerned about costs for personnel training or equipment associated with security management, since this will likely be provided by a system integrator. They will generally be highly interested in the potential safety benefits and any loss of those benefits that may result from security compromises, and they will presumably carry some level of liability for the operation of these applications. They may have some level of interest in the SCMS structure and the interfaces that must be used, but this is expected to be relatively minor, since they are likely to be less involved in provisioning their equipment than they are their system integrators.

Public Infrastructure System Integrators: System integrators of public infrastructure will carry many of the same responsibilities and concerns as the OEMs. Like the OEMs, they are providing CV equipment to end users. The key difference is that the provisioning activity is much less complicated (because the security needs of this equipment are easier to meet), and there is less potential for security breaches. Because these systems do not require substantial privacy-related measures, the management of the security credentials for these

systems is significantly simpler. Certificates do not need to be replaced as frequently, and there is less of a need to rotate certificates, so the volume of credentialing material is lower and turns over less frequently. The result is that the scope of security management experienced by these stakeholders will be much lower than that for some other stakeholders. System integrators will be likely to be less concerned with the structure of the SCMS or the SCMS interfaces.

Table 5 below illustrates the various SCMS User stakeholders and an assessment of the stakes held by these stakeholders.

Table 5: SCMS User Stakeholders and Stake Assessment

		SCMS Users									
		Users			Retailers	Maintenance & Repair	Other				
		Private Vehicle Owners	Public Fleet Operators	Private Fleet Operators	Dealers and Installers	Service and Parts	CV Equipment and Application Suppliers	Vehicle Manufacturers	State/Local DOTs	Public Infra System Integrators	Advocacy Groups
Stake	Material Cost	High	High	High	Low	Low	High	High	High	High	High
	Service/Logistical Cost	High	High	High	Mid	Mid	Mid/Low	High	High	High	High
	Training/Equip Cost	Low	Low	Low	High	High	Mid/Low	High	Mid	High	High
	Customer Experience	High	Mid	Mid	High	Mid	Mid/Low	High	Mid	High	High
	Safety Benefits	High	High	High	Low	Low	Low	High	High	High	High
	Liability Exposure	Low	Low	Low	High	High	Mid	High	High	Mid	High
	SCMS Internal Structure	Low	Low	Low	Low	Low	Low	High	Mid	Low	High
	SCMS External Interfaces	Low	Low	Low	High	High	Mid	High	Mid	Low	High

3.4.3   Other Interested Parties

This stakeholder group includes other parties who are not necessarily directly involved in implementing elements of the SCMS, and who may not directly interface with the SCMS as users. However, these parties may have a substantial overall interest in the SCMS for a variety of reasons. For example, USDOT has a deep overall interest in CVs and in the SCMS to assure public safety, assure the integrity of the overall transportation system, and to generally provide for the public good.

US Department of Transportation: Because the CV enterprise is, or will be, a direct result of USDOT regulation, it is highly likely that USDOT will have some role in the SCMS. This involvement may be limited to high-level governance, or it may involve some level of operational activity. It is also likely that some level of investment will be required to stand up at least portions of the SCMS, especially if and where it is determined that there is limited business interest for commercial entities. As a result, the level of investment required to stand up and operate the SCMS will be of high interest to the USDOT. However, other business-related aspects of the SCMS (e.g., ROI) are likely to be somewhat less important. Because the integrity of the entire CV enterprise depends on the SCMS, the USDOT will have a high level of interest in most aspects of the SCMS architecture, its operation (including interfaces), and its governance.

Academia: Various academic institutions may be interested in the SCMS from a variety of perspectives, including public policy, privacy, and various technical and organizational elements.

Standards Organizations: Because the CV security system relies heavily on technical standards, the Standards Development Organizations both in the United States and abroad may all have interest in how the SCMS is composed and implemented.

Advocacy Groups: Advocacy groups are organizations seeking to protect, or advocate for, the interests of various other stakeholders. These groups may include, for example, consumer privacy or product liability groups, automobile dealer trade associations, auto service and aftermarket trade organizations, etc. As a result, while individual advocacy groups may only be concerned about relatively limited issues, the full suite of advocacy groups across all stakeholders will have high levels of interest in all the various types of stakes discussed above.

Chapter 4: Potential CME Groupings and Owner/Operators

This chapter assesses the various SCMS functions and technical components and provides a possible first-order mapping among stakeholder groups and these functions. As noted in Chapter 3, SCMS Implementers comprise a small subset of the overall SCMS stakeholder population. These functions are summarized below. Refer to the SCMS Baseline report for a full description of the SCMS functions and components.

4.1   SCMS Component Grouping Assessment

Table 6: SCMS Functions and Technical Components[3]

Function Name	Activities
SCMS Manager	The SCMS Manager will likely provide the core policy and governance foundation for the SCMS ecosystem in general, and the SCMS technical components in particular.
Electors	Electors represent a distributed body of trust anchors who authorize themselves and root CAs to operate within the PKI. Essentially, an elector is similar to a root certificate, except that the actual root must be affirmed by the signatures of multiple electors.
Root Certificate Authority (CA)	The Root CA provides system-wide trust through CME certificates issued to all CMEs. It represents the basis of trust for the system.
Pseudonym Certificate Authority (PCA or EE CA)	The Pseudonym Certificate Authority (PCA) issues pseudonym, identification, and application certificates for EEs. There may be multiple PCAs in the SCMS.
Registration Authority (RA)	The RA receives and responds to requests for certificates from EEs via the Location Obscurer Proxy (LOP), and initiates certificate requests to a PCA to generate certificates for a requesting EE.
Intermediate Certificate Authority (ICA)	The ICA authorizes all other non-central components including ECAs, PCAs, RAs, LAs, or additional ICAs.
Enrollment Certificate Authority (ECA)	The ECA receives and responds to requests from one or more DCM(s) and signs enrollment certificates for EE devices.
Location Obscurer Proxy (LOP)	The LOP obscures the locations of requesting EEs (e.g., OBEs requesting certificates) from other functions, such as the RA.
Linkage Authority (LA)	The LA generates linkage values for a given EE based on a request from the RA.

---

[3] Reference(s): SCMC PoC Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.2.1

Function Name	Activities
Misbehavior Authority (MA)	The MA receives misbehavior reports from EEs, investigates potential misbehavior, and blacklists or revokes other components in the system.
CRL Store	The CRL Store is a repository that contains the most up-to-date CRLs generated by the MA.

When assessing these roles against the SCMS functions, it is important to note that some of the SCMS components are mutually exclusive. That is, 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 other 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. These exclusivity requirements are illustrated in Table 6.

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.

Other than requiring slightly different internal processes and certificate content unique to the CV security design, the functions of the Root CA, ICAs, Enrollment CA, PCAs, 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 that must be provided with certificates and certificate updates, the implementation of these functions must be done in a scalable manner, and this will require implementers with experience and resources to support this scale.

The LAs, LOP, MA, and 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, including in many field elements spread across the country. 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.

Table 7: 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 Technical Components	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

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.

4.2 High-level SCMS Component Owner/Operator Assessment

4.2.1 SCMS Manager

A key outcome of the project will be to identify and characterize the various ways of implementing the SCMS in general, and the SCMS Management functions in particular. For example, an all-public implementation would presumably involve the USDOT establishing a new agency or office to set policies and oversee the operation of the SCMS. Alternative models include not-for-profit administrative bodies along the lines of the Electronic Frontier Foundation (EFF) or the Internet Corporation for Assigned Names and Numbers (ICANN), both of which manage aspects of the internet through policies and oversight.

4.2.2 Electors

Electors represent the end of the trust chain. They are independent of one another and operate as a distributed means for assuring the trustworthiness of a root. Electors authorize themselves and root CAs to operate within the PKI. Trust management messages are signed by one or more electors and can add a Root CA certificate, add an Elector Certificate, revoke a Root CA certificate, and revoke an Elector Certificate. EEs and other PKI components know the necessary number of such signed trust management messages (e.g., 2 of 3) from non-revoked electors that will authorize the action contained in the messages (e.g., revoke Root CA "A").

It is assumed that candidates for operating an elector would be PKI service provider companies. As shown in Table 7 above, an elector may also participate in other SCMS functions, but the SCMS functions cannot be represented by a majority of the electors. Thus, there will be some requirement for at least a few independent electors. Standing up and operating an elector is like standing up and operating a root, except that the scale is substantially lower, and the level of security is somewhat higher. An elector generally only needs to sign trust management messages infrequently. As a result, there is some concern as to the motivation for a PKI service provider to participate as an elector, since the commercial opportunity is somewhat small and the responsibility relatively high.

4.2.3 Root Certificate Authority

Because it represents the trust anchor for the system, the Root Certificate Authority should be separate from the other entities in the SCMS. In general, it is desirable to have multiple roots to assure that a compromise of one root does not disrupt the entire CV enterprise, although doing so complicates the security processes since every vehicle must be able to chain a received certificate to any root (this because it may receive messages from vehicles that are linked to any one of the roots).

If multiple roots are used, then there must be some mechanism for assuring that every vehicle has the public key for every root, and, depending on the SCMS governance model, this may be difficult. For example, if the

SCMS is entirely privately operated, then it will be more challenging to ensure that all roots are coordinated so that every device on the road can verify certificates to any root. On the other hand, if the SCMS is entirely public, the coordination issue will be easily dealt with since there is only one body to coordinate with (e.g., a federal government agency), but the logistics of communicating the root information to every maker to be included in every device will remain.

Regardless of the governance model, it is likely that at least one PKI service provider will implement and maintain any given root. In the public governance model, it is expected that this would be implemented by a PKI service provider under contract to the federal government, while in a private model each root would likely be operated as a for-profit enterprise by one or more PKI service providers.

There has been some speculation that the OEMs themselves might own and operate the root CAs. This is no different from the private governance model since the root(s) would likely be operated in a way similar to that of a PKI service provider or may be operated by private PKI service providers on behalf of the auto makers. Since many car makers themselves may not necessarily have the facilities or experience to stand up and operate a root CA, this is just a question of who pays and who is in control, not of who implements.

4.2.4   Intermediate Certificate Authority

The security system allows for multiple ICAs. These CAs are expected to provide intermediate certificates for the various sub-components of the SCMS. Within the boundaries of the technical isolation requirements outlined in Table 7 above, it seems likely that these ICAs will either be fully independent commercial entities or directly associated with and operated by the companies implementing the various SCMS technical components. It is likely that the reality will be a little of both. Existing CAs will presumably fill a portion of this need, and those companies that are implementing other SCMS functions and have the capability to stand up an ICA to support those activities may do so.

4.2.5   Pseudonym Certificate Authority

The PCA is somewhat unique. First, it will require significant scale, since it must generate certificate sets for many vehicles, and these certificates will need to be replaced regularly. It also must securely store the partial linkage values provided by the LAs, and provide these values to the LAs when a misbehavior event is identified. It is likely that the PCA will be distributed, possibly among car makers or equipment makers, and will comprise a relatively large number of independent PCAs. This will reduce the scale requirements somewhat, but the overall implementation of a PCA is likely to be challenging from a bandwidth and volume perspective. Because the existing PKI industry is fully capable of providing this service from a technical perspective, it is likely that these companies will ultimately implement the PCA(s). However, because the scale is daunting, the PCAs may need to be subsidized early on to assure they exist and remain in existence. This may take the form of government-based financial support, or it may take the form of institutional investments. Another key element of the PCA is the management of connectivity and bandwidth.

4.2.6   Registration Authority

The RA is a unique element of the SCMS. It plays a key role in assuring the privacy and anonymity of the vehicles during the certificate provisioning process, but the operation is only a pass-through of information, with modest transient storage and processing requirements. Other than the requirement for relatively high volume and bandwidth, the operation of the CV RA is not substantively different than any other RA. The RA provides a key initial touch-point between the SCMS and the vehicles. Depending on how the certificates are updated, this may require substantial infrastructure (at the roadside and/or in fixed locations such as parking garages and service facilities), or it may require some sort of arrangements with cellular carriers. It is possible that these

carriers themselves (DSRC or cellular) may provide the RA services as part of an overall connectivity bundle. Because SCMS operations require two-way communications, it is unlikely that services such as satellite radio will provide this connectivity[4].

4.2.7 Enrollment Certificate Authority

The Enrollment Certificate Authority is a relatively small function of the overall SCMS. The volume of enrollment certificates is, at full production, about equivalent to the overall vehicle production, and this represents about 20 million certificates per year. Since these certificates do not require updating (as is the case with pseudonym certificates), the ECA volume is steady and well-defined. Generally, any PKI service provider should be able to implement and operate the ECA.

4.2.8 Location Obscurer Proxy

The need for the LOP is currently being debated. Conceptually, the LOP exists to isolate requests for certificate updates from the locations where the request originated. It is not clear, however, how necessary this is. There are many examples of mobile terminals making network contact at known locations. Because subsequent requests are likely to be substantially separated in both time and location, it is unlikely that any location information derived from any individual request could be used effectively to subvert the user's privacy.

To the extent that the LOP is found to be needed, the implementation is not substantially different from other internet services. It is likely that, to limit the overall bandwidth of any LOP implementation, the function will be geographically distributed, with perhaps several LOPs in each large metro region and the balance spread uniformly across the remaining road network. Any internet service provider would be able to provide LOP services.

4.2.9 Linkage Authority

The LAs are unique to the SCMS. These entities must receive request for linkage and carry out crypto-processing to generate linkage values for each certificate generated in a set. These are derived from a single linkage seed value. Because this is necessary for every pseudonym certificate issued, the LA must generate and provide a corresponding linkage value from a single linkage seed value. This represents a high volume of processing and communications bandwidth, like the PCA.

In addition, the LA must securely store each linkage value and the symmetric key used to create it together with the linkage seed value corresponding to those linkage values and keys. This is so that, when asked, it is able to produce the linkage seed value(s) necessary to revoke those certificates.

Because each LA must operate independently, and because it is desirable that the LAs operate independently from other elements of the SCMS (e.g., the PCA and RA), it may be challenging to identify suitable implementation partners, and this element may also require some early support from the federal government.

4.2.10 Misbehavior Authority

The MA implements the mechanisms for identifying bad actors in the system and subsequently removing them from the system through certificate revocation. It is unclear if the MA also has the responsibility for assuring that such vehicles are subsequently physically inspected and repaired but, lacking any other such functions in the SCMS, we are assuming that the MA will also facilitate this. While these overall functions of the MA are

---

[4] See, however, CRL Store and CRL delivery.

reasonably well understood, the specific operations it will carry out are not. For example, the initial step in addressing misbehavior must include some means for the MA to become aware of misbehaving vehicles. While some obvious examples of misbehavior have been informally identified, there is no uniform definition of those actions that warrant revocation (and this is likely to be a moving target requiring continual updating and revision, especially as the system is subjected to cyber-attacks), and there is no currently defined mechanism for the reporting of potentially misbehaving vehicles. In addition, beyond revocation, the role of the MA 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 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 would 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 would 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).

The MA thus represents a dual role. On the one hand, it 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. On the other hand, it must also either 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.

Clearly, the overall misbehavior detection concept must be better defined before these roles are undertaken.

4.2.11 CRL Store

The CRL Store is related to the MA in that the CRL entries will be provided by the MA. The CRL Store will then update the CRL, and make it available in an authenticatable form through various facilities. For example, the CRL store could be provided as a function on a server that could be accessed by vehicles via cellular interfaces, or via roadside DSRC equipment. It is also possible that the updated CRL could be simply broadcast using a variety of radio communications systems (e.g., DSRC, FM sub-carrier, satellite radio). It is expected that the CRL Store would not only update and maintain the CRL but would also interface with these various information outlets to assure the availability of the CRL to vehicles on the road. It is possible that communications carriers may provide the CRL Store service in exchange for consumer-purchased air time; for example, by including a fee in their data plans for making the information available, as is currently done for other public service functions provided by these carriers (e.g., teletyping services for the deaf). To the extent that state and local authorities provide various V2I capabilities, the CRL store could also be accessed through these systems. In this case, the cost of operating a public CRL store would presumably be a public expense, since it is unrealistic to have a critical resource such as a CRL only available to paying subscribers.

4.2.12 Device Configuration Manager

The Device Configuration Manager (DCM) is a peripheral element pf the SCMS. It is responsible for establishing a secure connection to an EE (i.e., an end-user device) and providing initialization credentials

(elector certificates and various trust chain documentation), and then also providing enrollment credentials (specifically the enrollment certificate that may be subsequently used to request certificates). The DCM must include secure operational processes and a chain of custody for devices, device firmware, and any other data to be injected into the device by the DCM to ensure only properly certified devices receive enrollment certificates. This secure operational process involves some physical protection as well as assurance that only certified devices are provisioned with certified software. Because the CV system will eventually have hundreds of millions of EEs, the DCM is likely to be highly distributed and require additional management effort to assure consistency in terms of operation and security across multiple DCM service providers in multiple locations.

4.2.13 SCMS Implementers vs. Roles

Table 8 below summarizes the types of SCMS Implementer companies and the likely or possible roles they may play based on information gathered from stakeholder engagement activities. Of course, the future ownership and governance model will impact the intentions and motivations of these companies.
The types of entities identified in the table are generally self-evident, but are described briefly below.

- Non-profit entities are self-governing industry associations, such as ICANN or EFF.
- PKI service providers are those companies currently engaged in providing CA services in other industries.
- Certification services are those entities currently engaged in performing technical assessments and testing of equipment, as well as providing certifications of that equipment relative to specifications or regulations.
- Data analytics companies are those entities engaged in the analysis of large data sets to identify key information or trends within the data sets. These companies include both large data storage and analysis facilities and sophisticated algorithm development.
- Administrative services providers provide record-keeping and other general administrative functions for various industries (e.g., claim administration, financial services, records management, general IT services).
- Enforcement and compliance are typically companies with some physical security capability. They may also be administrative services companies with experience managing compliance, potentially in partnership with public justice organizations.
- Vehicle manufacturers are those entities engaged in the manufacture of end-user equipment.

Table 8: SCMS Implementer Types and Potential Roles

		SCMS Technical Components												
		SCMS Manager	Elector 1	Elector N	Root CA	Int CA	ECA	PCA	RA	LA1	LA2	LOP	MA	CRL Store
Types of Entities	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

Chapter 5: SCMS Manager Internal Organizational Structure and Governance

Ensuring that the organizational structure of the SCMS Manager supports its mission helps create effective organizational units that can function at high levels of performance. Management control, employee cooperation, stakeholder collaboration, and business responsiveness to changes in the marketplace are characteristics of different organizational structures that must match the mission of the SCMS Manager. The mission of the SCMS Manager defines the business operation priorities while its organizational structure supports its mission.

The SCMS Manager's internal organizational structure keeps all the participants of the SCMS functioning cohesively. It informs the participants as to how the SCMS Manager is constructed and how it works; more specifically, it details the participant and leadership selection processes as well as the decision-making processes.

An effective SCMS Manager structure facilitates management and clarifies relationships, roles, responsibilities, levels of authority, supervisory and reporting lines, decision-making processes, and procedures among all stakeholders and organizational elements. An effective structure also enables defining tasks and activities, resource (e.g., human, financial, and technical) availability and allocation, information flows, and accountability for achieving the SCMS Manager's goals and objectives. A clearly established structure gives the SCMS participants a means to maintain order and resolve disagreements. It gives meaning and identity to the entities who join SCMS, as well as to the SCMS Manager.

5.1 Potential SCMS Manager Responsibilities and Activities

5.1.1 SCMS Manager Design Attributes and Assumptions

The list below describes key attributes of the SCMS that drive both the external and internal organizational structures. These are based on the assumptions that the SCMS Manager can operate select technical components of the SCMS or solely function as a policy and standards development and enforcement entity. These attributes relate to the public interest objectives and design/deployment criteria described within Chapter 2.

1. There may be only one SCMS Manager entity with full responsibility for oversight and governance of the SCMS technical components that grant and revoke certificates.
2. The SCMS Manager may (or may not) operate specific technical components of the SCMS (e.g., an elector), but will have overall responsibility and governance of the SCMS technical components.
3. **Organizational separation** – Within the National SCMS, and within the SCMS Manager, the managing entity needs to be carefully implemented and maintained to assure privacy by design, provide needed checks and balances, and make collusion more difficult and more easily detectable.
4. **Privacy by design** – As conceived, the system will contain multiple technical, physical, and organizational controls to help limit potential privacy impacts on consumers, including those related to vehicle tracking by individuals and government or commercial entities. The SCMS Manager may have

multiple committees consisting of experts from member organizations to develop policies and standards. The SCMS Manager may or may not have the authority and capability to enforce these policies.

5. **Authority** – The complex ecosystem of the technical SCMS components requires the SCMS Manager to have a set level of authority which will differ based on the ownership and industry governance model.

6. **Broad stakeholder engagement** – There are multiple business entities in multiple industries that will likely participate in SCMS operations. Only through broad stakeholder engagement can the SCMS facilitate market competition and fair and transparent policy- and standards-making processes. This requires the SCMS Manager to have internal policy and standards development capabilities. It behooves all participants in the SCMS ecosystem to be actively engaged in developing, implementing, monitoring, and self-enforcing the bylaws, policies, standards, and business practices of the SCMS Manager. Stakeholder engagement will necessitate some level of oversight or advisory structure to accommodate the needs of stakeholders who do not directly participate in the organization. There may need to be an oversight/advisory structure for day one stakeholders, such as auto makers and PKI service providers.

7. **Transparency** – Development and implementation of rules, policies, and standards, as well as the accompanying enforcement mechanisms, must be transparent in order to achieve accountability and fairness. In many organizations, transparency is provided through a board of directors that includes key stakeholders and participants from outside of the specific industry stakeholders. An activity responsible for public reporting of actions and decisions may be needed. Government open meeting requirements may apply.

8. **Accountability** – Accuracy, authenticity, and privacy are paramount in V2X communications. The SCMS Manager will likely have some level of accountability for SCMS technical operations, as they are associated with policies and activities specifically managed by the SCMS Manager. Accountability refers to how well an organization can meet the expectations of its customers, and has a significant impact on the public acceptance of and confidence in the SCMS. Included in this attribute is the reliability of day-to-day operations, such as the ability to quickly respond to system incidents (e.g., attack or failure), loss of an SCMS technical component (e.g., by corruption or bankruptcy), revised regulatory environment, changing technology, and evolving policies. Other aspects include implementing stakeholder directions, providing reporting measures on the performance and results achieved by SCMS elements, requesting and responding to user feedback, and providing information to the public on composition and operating procedures.

9. **Stability** – Significant effort is required to stand-up the technical components necessary to provision and maintain V2X communication hardware and software. As the useful life for most vehicles is more than a decade, sufficient stability is necessary within the legal basis of the SCMS Manager. While providing stable direction, the organization needs to be nimble in order to accommodate the pace of technical and policy evolution.

10. **Fairness** – Transparency and fairness are key for all participants in the SCMS ecosystem to operate according to set expectations. The SCMS Manager's structure is critical to delivering the foundation for fairness among stakeholders. The two clear areas where fairness will drive the organizational structure are risk management (both internal and external to the SCMS) and dispute resolution.

Industry, government, and academic governance structure experts and leaders have previously discussed, analyzed, and concluded that, for the SCMS Manager to operate successfully, multi-stakeholder engagement is critical. Accountability structures should be in place to prevent certain players from dominating the process. Technology and policy should be developed simultaneously. A lesson learned from current best practices is that, if technical standards have been established early without considering governance, it becomes more difficult to integrate and implement a sound governance structure later in the process.

As the external governance is developed in concert with the appropriate business model, the internal governance is expected to facilitate consensus-building, development, improvement, and adaptation of the various bylaws, policies, and standards. Technical decisions are rarely only technical decisions; instead, they tend to have social and economic implications. The public may need representation within external governance processes and potentially even within internal governance activities (e.g., be represented in a privacy working group).

There is likely to be more than one governance structure involved. Indeed, multiple governance mechanisms are usually necessary for managing complex information systems. The SCMS Manager is expected to have a multi-layered, multi-level, multi-stakeholder structure, and actual deployment is likely to be multi-phased.

5.1.2 High-level Potential Functions, Roles, and Responsibilities of the SCMS Manager

External and internal governance overlap in terms of their structure issues, funding, and business models. It is a complex undertaking to fully separate activities, impacts, decisions, and resolutions. There have been numerous research projects and articles written about the many questions, issues, tasks, roles and responsibilities, standards, compliance, advocacy, processes, and approaches related to implementing a National SCMS. These areas of interest can be grouped into three categories and addressed in three overlapping models:

1. External governance (e.g., ownership) determines the overall structure of ownership and oversight over the entire SCMS ecosystem, including the DCM and certification labs and all SCMS technical components.
2. Internal governance (e.g., institutional and management responsibilities) determines the policies, bylaws, rules or code of conduct, standards, etc. that internal SCMS Manager members and SCMS ecosystem participants must observe and follow while fulfilling the basic requirements set forth by the external governance structure.
3. The business model (e.g., long-term sustainable business operations and funding mechanisms, which must offset costs) is closely tied to the external governance model as it deals with the initial implementation and sustainment of the financial and business aspects of the entire SCMS ecosystem.

As the SCMS Manager's business model is more dependent on the external governance structure, its internal organizational structure is less dependent on the external governance structure. As an organization's external governance processes focus on governance principles and overall direction setting, its internal organizational governance activities focus on the process by which decisions are implemented (or not implemented), and how the decisions can best reflect the collective wisdom, intelligence, and know-how of stakeholders. The SCMS Manager internal organization and governance is expected to support the development and implementation of operational policies, standards, and technologies, and to facilitate monitoring and potentially enforcing compliance with rules, regulations, and policies.

The SCMS Manager supports and facilitates consensus-building and a bottom-up approach for continuous improvement and changes in policies, rules, and innovative ideas for optimum operation. Whatever structure or model the SCMS Manager will operate in is expected to best encourage support, cooperation, and collaboration of entities from a broad spectrum of industries with a wide range of subject matter expertise.

The internal governance structure may support and facilitate:

- Standards and policy development, promoting a sense of ownership from all participants
- Development of rules and standard operating and maintenance procedures that ensure consistency across jurisdictional boundaries
- Enforcement procedures
- Certification procedures
- User authentication and access procedures, and rules for removing a user from the system
- Processes for solving conflict among stakeholders
- Processes for setting and measuring progress toward performance standards
- Processes for identifying and addressing the evolution of technology and incorporation of that technology
- Technological innovation and intellectual property protection and adaptation
- Risk management and mitigation
- Communication within the SCMS Manager's various functions and divisions as well as with all participants in the SCMS ecosystem
- Financial management and proper use of funds.

5.2 Types of Internal Organizational Structures

There are four traditional types of organizational structures (functional, divisional, matrix, and projectized) and three newer types (network, virtual, and hierarchy-community phenotype). In addition, there are many combinations of these in organizations as they adapt to their own unique business, industry, social-geographical, and political environments.

5.2.1 Traditional Organizational Structures

5.2.1.1 Functional Structure

A functional structure groups people who conduct similar tasks, have similar skills, and/or perform similar jobs in an organization. One advantage of this kind of structure is quick decision-making, because the group members can communicate easily with each other. People in functional structures usually advance and learn more quickly, as well, because they possess similar skill sets and interests to their group members. Typically, a manufacturing company with relatively linear processes has such a structure (e.g., supply, distribution, marketing, sales, and shared services groups).

5.2.1.2 Divisional Structure

In a divisional structure, the company will coordinate inter-group relationships to create a work team that can readily meet the needs of a certain customer or group of customers. The division of labor in this type of structure will ensure greater output of a variety of similar products. One type of divisional structure is geographical, where divisions are set up in regions to work with each other to produce similar products that meet the needs of the individual regions. An example is FEMA, which has 10 regional offices serving and responding to regional customers' needs. A divisional structure is similar in nature to a functional structure.

5.2.1.3 Matrix Structure

Matrix structures are more complex in that they group people in two different ways: by the function they perform and by the "product" team. In a matrix structure, the team members are given more autonomy and expected to take more responsibility for their work. This increases the productivity of the team, promotes greater innovation and creativity, and allows managers to cooperatively solve problems through group interaction.

Often, businesses have a mission that is broader and oriented more toward a product or system and a market (such as the SCMS ecosystem). The business may have to adjust rapidly to changes in the marketplace and the competitive environment, and must have more flexibility than what is permitted by more rigid hierarchical structures. The employees closest to the working level make the most effective decisions for such a business. The matrix organizational structure maintains the hierarchy for human resource functions such as discipline, salary, and promotions, but superimposes a second structure for the work. Employees report to an immediate supervisor for work questions and usually make decisions quickly.

Many consulting firms have a matrix structure: there are market-facing groups and teams, and each employee is often also part of a specific project team composed of people in different market groups and functional areas. NAV CANADA (refer to the Literature Search report for a full analysis) has a matrix structure. The industry standards and policies have already been well established; the focus is to maintain stable operations while keeping up with technological advancement and the evolving societal, environmental, political, and global developments.
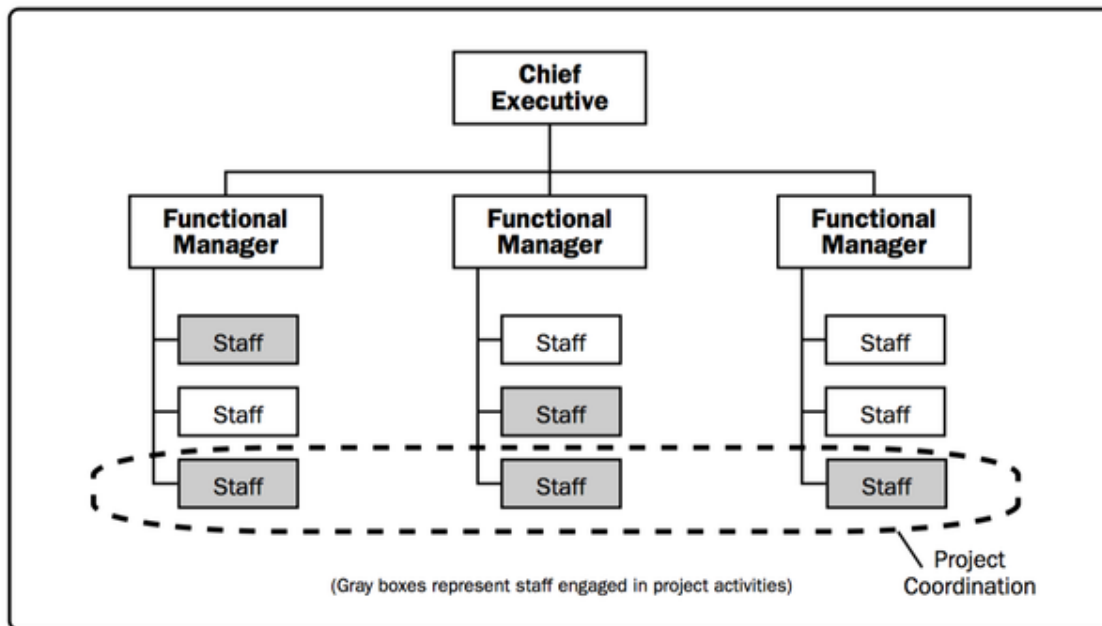

Figure 3: Matrix Organization[5]

---

[5] http://www.pmworkplace.com/PMP/A_Guide_to_the_Project_Management_Body_of_Knowledge_PMBOKGuide/LiB0014.html

5.2.1.4 Projectized Structure

In a projectized structure, groups or teams are constructed based on the number of members needed or interested in participating to produce a product, complete a project, or develop a specific area of a larger initiative. To ensure that the right members are chosen to participate in the project, the number of significantly different tasks is considered. The quality of the organizational structure depends on the competencies of the members of the team.

Larger bureaucratic organizations can benefit from the flexibility of teams within a projectized structure. Xerox, Motorola, and DaimlerChrysler are companies that actively use project teams to perform tasks. Best practices within various industry consortia suggest that mostly projectized teams tackle specific projects that their advisory or steering committees have directed to them.
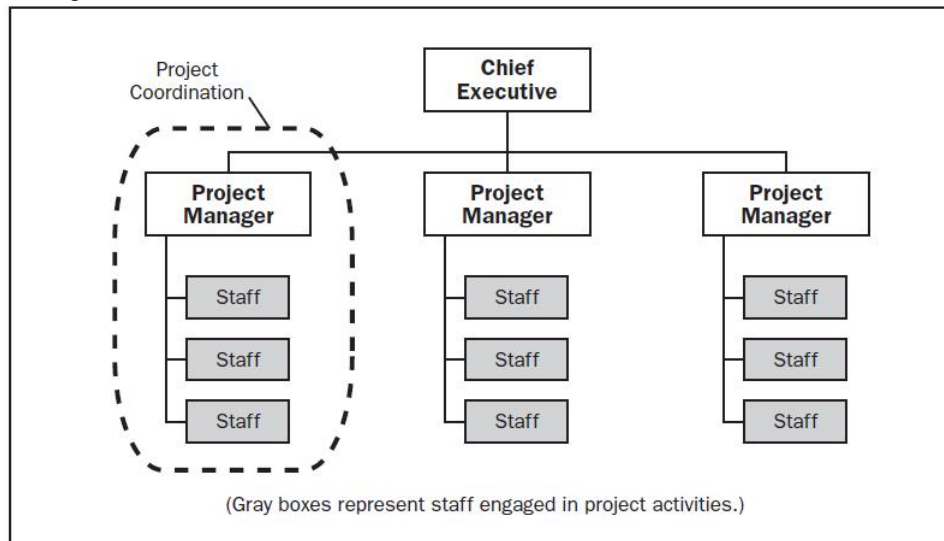

Figure 4: Projectized Structure[6]

---

[6]http://www.pmworkplace.com/PMP/A_Guide_to_the_Project_Management_Body_of_Knowledge_PMBOKGuide/LiB0014.html

Organization Structure / Project Characteristics	Functional	Matrix			Projectized
		Weak Matrix	Balanced Matrix	Strong Matrix	
Project Manager's Authority	Little or None	Low	Low to Moderate	Moderate to High	High to Almost Total
Resource Availability	Little or None	Low	Low to Moderate	Moderate to High	High to Almost Total
Who manages the project budget	Functional Manager	Functional Manager	Mixed	Project Manager	Project Manager
Project Manager's Role	Part-time	Part-time	Full-time	Full-time	Full-time
Project Management Administrative Staff	Part-time	Part-time	Part-time	Full-time	Full-time

Figure 5: Influence of Organizational Structures on Projects[7]

5.2.2 Newer Organizational Structures

5.2.2.1 Network Structure

While business giants risk becoming too clumsy to pro-act, act, and react efficiently, the new network organizations contract out any business functions that can be completed better or cheaper by other entities. Managers in network structures spend most of their time coordinating and controlling stakeholder relations, usually by electronic means. For example, H&M is outsourcing its clothing to a network of 700 suppliers, more than two-thirds of which are based in low-cost Asian countries. By not owning any factories, H&M can be more flexible than many other retailers in lowering its costs, aligning with its low-cost strategy. The Responsible Business Alliance (RBA) and many professional associations and industry alliances have a network structure.

5.2.2.2 Virtual Structure

A virtual organization is defined as being closely coupled upstream with its suppliers and downstream with its customers, such that where one begins and the other ends means little to those who manage the business processes within the entire organization. A special form of boundary-less organization is virtual. Virtual organizations are considered to not physically exist but are enabled by software. The virtual organization exists within a network of alliances using the internet. This means that, while the core of the organization can be small, the company can still operate globally and be a market leader in its niche. Because of the unlimited shelf space of the internet, the cost of reaching niche goods is falling dramatically. Amazon, for example, is successful because there are many niche products that individually don't sell in huge number but collectively sell enough to make a significant profit.

---

[7]http://www.pmworkplace.com/PMP/A_Guide_to_the_Project_Management_Body_of_Knowledge_PMBOKGuide/LiB0014.html

5.2.2.3 Hierarchy-community Phenotype or Informal Organizational Structure

The informal organization is the interlocking social structure that governs how people work together in practice. It is the aggregate of norms and personal and professional connections through which work is completed and relationships are built between people who share a common organizational affiliation(s). It consists of a dynamic set of personal relationships, social networks, communities of common interest, and emotional sources of motivation. The informal organization evolves, and so follows the complex social dynamics of its members. Starbucks, for example, has leveraged many of the benefits of an informal organization.

5.2.3   Industry Alliance and Consortium Models

Depending on the eventual SCMS ecosystem ownership and governance structure, there may be a need for an industry alliance or consortium to begin taking responsibility for next steps for initial deployment.

Typically, there are four types of governance models for an industry alliance or consortium.
1. Informal network
2. Loose partnership structure with lead body
3. Formal consortium set up as a new company
4. Existing Managing Agency infrastructure for contract management purposes

5.2.3.1 Informal Network

This type of model has the following key features:
- Informal partnership; possibly a partnership agreement
- No separate legal status outside of the members
- Members separately bid for and manage own funds

It is apparent that this type of governance model is not applicable to SCMS Manager, which needs to be a separate legal entity to assume likely required authority levels and fulfil management responsibilities.

5.2.3.2 Loose Partnership Structure With Lead Body

This type of model has the following key features:
- Loose consortium with lead organization
- Lead organization applies for contract funding on behalf of consortium members
- Uses some of the funding to deliver own services and to manage contract
- Distributes remaining funds to other members

This type of model could have an organization, such as an auto maker or a PKI service provider, in the leadership and/or coordinator role within the SCMS ecosystem. However, with a single "lead body," it would be hard to achieve the fairness, transparency, and risk mitigation that such a complex SCMS ecosystem requires.

5.2.3.3 Formal Consortium Set Up as a New Company

This type of model has the following key features:
- Formally constituted as an independent legal entity
- Single point of contracting
- Hub-and-spoke structure

A formal consortium involves providers coming together to establish a partnership that is then formally constituted as an independent legal entity (usually as a company limited by guarantee, and possibly with charitable status). The partner organizations—the business entities or stakeholders who participate in the operations of the SCMS ecosystem—become formal members of the consortium, creating a single point of contracting.

The elementary structure of a formal consortium of this nature is based upon a "hub and spoke" model. The hub is the central management unit that carries out certain executive functions on behalf of the partnership or membership network. It also provides certain support and development services for the member organizations and for the entire new business venture. This hub is sometimes described as a "support unit;" the SCMS Manager may be in this position. The spokes, on the other hand, are the various member organizations—participants in SCMS ecosystem.

5.2.3.4 Existing Managing Agency Infrastructure for Contract Management Purposes

The last model has the following key features:
- Need available managing agent that can hold contracts and distribute sub-contracts
- Managing agent charges management fee

This requires an existing management agent or accountable body to hold contracts and then sub-contract these to the service providers. As recompense for this work, the managing agent would charge a management fee by top-slicing contract funding. This model is not applicable for initiating the SCMS Manager, as there is no existing managing entity in place for the SCMS ecosystem.

5.3   Best Practices in Comparable Organizations

The nature of the SCMS Manager's responsibility of managing the largest PKI system in the world is unprecedented. Because of this, it is critical to examine industry alliances and organizations that could offer some insight into best practices, thereby ensuring an efficiently operated organization and facilitating effective industry governance.

Table 9: Overview Internal Organization Structure Best Practices and Takeaways

Organization	Internal Org. Structure	Reasons for Implementing the Internal Org. Structure
AUTOSAR	Network and projectized with functional groups for shared services such as Finance, HR, and IT	The organization was established to develop, populate, and implement a standardized architecture platform for automotive electronic control systems. This goal is best achieved by bringing together auto makers, device makers, software developers, end users, and researchers to work collaboratively under the authority and leadership of the funding auto makers. There are specific subject matter areas that need focused effort from personnel and business entities with SMEs. With the technologies ever evolving and improving, the goals may also evolve, hence the organized effort requires dynamic adjustment to keep up with or stay ahead of the technology advancement. A projectized structure best facilitates organizations to achieve such goals in this dynamic ecosystem.
GENIVI	Network and projectized with functional groups for shared services such as Finance, HR, and IT	The organization was established to develop and populate standards for in-vehicle "infotainment" applications. Similar to AUTOSAR, the mission requires a wide range of businesses and industries to collaborate, develop, and adapt the standards. The nature of the tasks and goals plus the level of complexity of the ecosystem are all similar to AUTOSAR. The task forces (or work packages) are set up to focus on specific areas with SMEs. This kind of organizational structure best facilitates new technology development, adaptation, and continuous improvement.
RBA (formally the EICC)	Network and projectized with functional groups for shared services and a dedicated training and compliance entity	RBA was established to support the rights and wellbeing of workers and communities worldwide affected by the global electronics supply chain. The organization develops and implements policies, rules, standards, and mechanisms within the electronics manufacturing supply chain focusing on social, environmental, political, cultural, and technological issues and challenges. This requires SMEs to exert focused efforts in their respective areas of expertise. A network and projectized structure, such as subject-specific initiative task forces, would best allow the organization to achieve its goals.
ICANN	Multi-layered and multi-leveled projectized structure led by subject-specific committees, with	The ICANN coordinates the maintenance and procedures of several databases related to the namespaces of the internet, ensuring the network's stable and secure operation. ICANN performs the actual technical maintenance work of the Central Internet Address pools and Domain Name System root zone registries. It has distinctive and highly technical subject areas.

Organization	Internal Org. Structure	Reasons for Implementing the Internal Org. Structure
	functional groups for shared services	Its three support organizations are run independently, with their own bylaws and processes and procedures, as they consist of countries from many global regions. A projectized structure organized by subject matter helps achieve the organization's mission.
NAV CANADA	Weak matrix structure with project teams under the Engineering Division; it has a network structure for policy and standard development via stakeholder-represented committees	The Canadian civil aviation communication services were originally government owned and operated. It was privatized to a no-share, non-profit organization: NAV Canada. It was already a well-established organization with stable operations prior to privatization. It is likely that it has kept the functional structures in the organization mostly unchanged, and the functional structure of its operations management suits its business model of a service delivery operation.
Vehicle Information and Communications System (VICS)	Medium matrix structure with projectized groups focusing on system and technology development	VICS delivers traffic and travel information to vehicles in Japan. The Japanese culture and mindset of striving for the wellbeing and benefit of their nation and their people promote the high level of trust between businesses and the Japanese government. This likely has contributed to a streamlined organizational structure, as the auditing, compliance, and enforcement functions are minimal. It has a simple structure of Business Planning, Systems Operation, System Development, and Research. In the Systems Development and Research divisions, the structure is project based.
SEMATECH (early days)	Strong matrix structure with dedicated project teams for technology research and implementation	The U.S. government spearheaded the formation of SEMATECH to centralize resources in advancing semiconductor technologies. In the first five years, the organization's goal was to surpass Japan in semiconductor technologies in the shortest amount of time. There were task forces dedicated to tackling specific areas of chip manufacturing as well as other related technologies. There was also a manufacturing facility operated in a traditional functional organizational structure.

5.4   Framing an Organizational Structure for the SCMS Manager

Organizational structures often reflect the level of growth, or current stage, of an institution. There are at least four levels of organizational growth recognized by management professionals.

- **Emergent/start-up/standing-up planning phase.** These organizations are at the beginning stages with "bootstrapping" management, few systems, and limited resources.
- **Launch or growth/bootstrapping/initial deployment.** These organizations have stabilized their structure framework, decided on their service mix, and are ready to expand.
- **Consolidation.** These organizations have determined a strategic focus, stabilized internal governance, strengthened systems, increased efficiency, and made progress toward greater sustainability.
- **Mature.** These are self-sufficient organizations that can effectively manage and adjust mission, strategy, structure, and systems in response to internal and external trends and challenges.

An organization's structural requirements may be different based on different stages of growth, development, and capacity. The SCMS Manager's internal governance model needs to ensure that the structure can grow and expand along with its mission, staff, programs, policy changes, and technological evolutions. An organization should be able to carry out more functions at each successive level of growth. Organization structures evolve over time. With each successive stage, it is necessary to reexamine the structure to see if it is keeping pace with the new realities of the business operations and the National SCMS ecosystem.

To continue down this path of thought—although the actual approach change drastically based on the final ecosystem ownership and industry governance model—the SCMS Manager can take a projectized approach in the initial deployment stage. Committees would function as project teams focusing on specific issues to establish initial operating capability. This includes identifying stakeholders and forming initial leadership groups to develop SCMS management structures, processes, procedures, and bylaws (i.e., rules to govern how the SCMS Manager will operate). An initial board of directors can be selected or appointed with seats filled by key stakeholders, such as the automakers, device manufacturers, PKI service providers software developers, communication services, and federal and state governments. The number of seats in total and for each stakeholder, along with the requirements for being on the board, are subject to revision and changes.

Key stakeholders may be represented on the committees in which they have a strong interest in contributing to developing work products. Selection of members in each committee will be transparent and fair. Committees are to be accountable for delivering the expected products effectively and systematically.

It is yet to be determined whether the SCMS Manager will operate technical SCMS components. In either case, the Manager's structure may evolve into a hybrid of matrix, network, and projectized structures, with functional groups carrying out internal operational responsibilities (e.g., Finance, IT, and Operations) as the SCMS technical components are being fully deployed. There may also be multi-leveled structures within each functional area. For example, there can be departments or divisions within Operations, such as Systems Operations (if the SCMS Manager also operates a part of SCMS), Audit, Compliance, etc.

Various committees and sub-committees can work collaboratively as project teams on matters such as proposing, developing, and revising policies, standards, rules, processes, and procedures pertinent to SCMS technical component operations and PKI security and efficiency.

The sub-sections below begin to frame the high-level process of deploying an SCMS Manager, but this example is for illustrative purposes only. An actual implementation plan would have much more detail, including an integrated master schedule with aligned task owners. The hypothetical plan below also assumes a private or public-private ownership governance model. It will differ based on the nuances of the future ecosystem ownership and industry governance model.

5.4.1   Outline the Internal Governance Plan

The internal governance plan determines what type of governance is needed to make decisions and identify the roles in the organization. Typically, an initial steering committee writes the business plan, obtains initial funding, and develops the first proposals. The governance plan identifies leadership entities to coordinate, inspire, and support the work. A board of directors may be identified to coordinate activities, make contacts, network with industry leaders, and clear the way for the organization to meet its objectives. As the SCMS technical components are deployed and the SCMS Manager takes on governance authority, explicitly showing the hierarchy in an organizational chart helps all parties to understand decision authorities and their specific responsibilities.

Depending on the joint decisions of the stakeholders and the owner of the SCMS Manager, the SCMS Manager itself may or may not operate any part of the SCMS ecosystem. For this reason, the SCMS Manger's internal structure may vary accordingly to be suitable to the actual determined roles and responsibilities.

Functions of the SCMS Manager may include:

- **Finance** – This function manages the funds from the various government entities, charitable organizations, stakeholders, and users and consumers. It makes sure the funds are expensed, invested, and recorded properly according to the SCMS Manager's bylaws as well as any agreed-upon rules and policies. It develops and manages the budget, and communicates with the rest of the functions in the SCMS Manager in a timely fashion so that all stakeholders are apprised of the financial health and management soundness of organization operations.
- **Legal** – The SCMS Manager deals with a multitude of issues that will likely need to be addressed by legal professionals, such as:
    - Patent, intellectual property ownership and use, restrictions or limitations to developing innovative SCMS products/technologies/services;
    - Labor disputes;
    - Stakeholder disputes;
    - Public privacy or other legal issues related to the public; and
    - Criminal actions (internal and external).
- **Audit** – This function ensures that all entities in the SCMS ecosystem are abiding by the established and implemented rules, policies, standards, regulations, laws, mandates, and codes of conduct. Any arising issues can be brought up for discussion and correction. Best practices can be studied, communicated, and implemented for continuous improvement.
- **Compliance** – Through its Compliance function, the SCMS Manager addresses misbehavior and conduct-enforcement actions.
- **Communications** – This function communicates with stakeholders who participate in the SCMS as well as with external stakeholders, such as federal and local governments, non-profit organizations,

the general public, and the media. The communications function also collects, aggregates, and compiles feedback, opinions, desires, and suggestions from various stakeholders, including the government and the public, and provides the feedback to the relevant participating entities.

- **Information Technology** – IT is responsible for managing all SCMS Manager office equipment, communication systems, equipment, devices, software, hardware, and internal cybersecurity measures.
- **Technology Innovation** – Technology will inevitably advance as the SCMS is deployed and running in steady-state. Technologies might be developed by member companies independently or jointly, with or without funds from the SCMS Manager. In addition to the legal functions of the SCMS Manager, the technology innovation function can support the effort in developing, testing, piloting, adapting, upgrading, or implementing any new technologies, standards, etc. It can also develop ways to mitigate certain risks related to technology advancement.
- **Human Resources and Marketing** – These two functions are typical in most organizations, but may not be critical in the beginning stages of SCMS Manager deployment.
- **Operations** – If the SCMS Manager is to operate certain parts of the SCMS ecosystem, such as the MA or electors, there must be a function in the SCMS Manager dedicated to operating these technical components. Consequently, all other functions will likely have increased workloads and responsibilities to accommodate these operations. Even if the SCMS Manager does not operate any technical components, the SCMS Manager may need the operations function to oversee high-level technical component operations and ensure that they meet specified levels of service.

5.4.2 Establish Rules for Operation

The internal SCMS Manager's structure is expected to establish rules stating how formal and informal groups (e.g., task forces, various task-specific committees, working groups), SCMS ecosystem participants, and various SCMS components will operate to achieve the mission of the SCMS. For example, committees typically use Robert's Rules of Order and/or consensus decision-making to conduct meetings. Rules make up an organization's culture and facilitate cohesive and smooth operation. Misunderstandings and confusion can be minimized by documenting operating procedures and processes—especially in a culturally diverse environment such as the SCMS, where numerous business entities of different industries must work collaboratively. Groups formed to resolve a single issue may not need a formal structure; however, when forming long-standing groups to address a series of ongoing topics, and when managing a large, complex SCMS ecosystem, the SCMS Manager must establish and document clear rules and authority levels. These include:

- Board membership and leadership elections, number of seats, voting rights, and meeting frequency
- Committees' (e.g., task forces, working groups) membership levels, fee schedules, number of seats, voting rights, meeting and conflict-resolution rules
- Codes of conduct, bylaws
- Standard operating, reporting, and communication processes and procedures
- Processes and procedures for changing and updating existing processes and procedures
- Consequences and punishment for violations.

5.4.3 Distribute the Work for Initial Deployment

The SCMS Manager internal structure may establish task forces and action committees to carry out certain activities, such as policy and standards development for SCMS operations, risk identification and mitigation, and procedures for handling misbehaving entities. These groups (e.g., teams, task forces, committees) can make specific changes to policies and practices to achieve SCMS goals. In this case, the internal structure defines conditions when a temporary support group, such as a task force, working group, or a committee, is

necessary to respond to new requirements. The SCMS Manager also distributes routine internal operational work to appropriate internal functional groups, such as Finance, Legal, and Audit.

An organizational structure usually evolves over time. As the SCMS ecosystem evolves with technological advancement; stakeholder and market changes; and political, social, and economic environment changes, its organizational structure will inevitably evolve to adapt and thrive under the new circumstances. For example, NAV CANADA evolved from a small, government-run entity to a complex government agency, and then to a successful, no-share, non-profit business operation governed by a board of directors. Throughout the past 20 years, ICANN evolved from a one-person operation to a large, international organization with sophisticated policy-making and operations management processes and procedures.

After considering organizational structure theories, best practices, the SCMS ecosystem, the scope and scale of the SCMS management requirements, and the mission of SCMS, the SCMS Manager internal governance structure may be a multi-phased, multi-layered, and multi-leveled hybrid of projectized, network, and functional organizational structures (illustrated in the following figure). However, the future SCMS Manager structure will be heavily influenced by the ecosystem ownership and industry governance model, which could necessitate a structure far different than the high-level example in Figure 6.
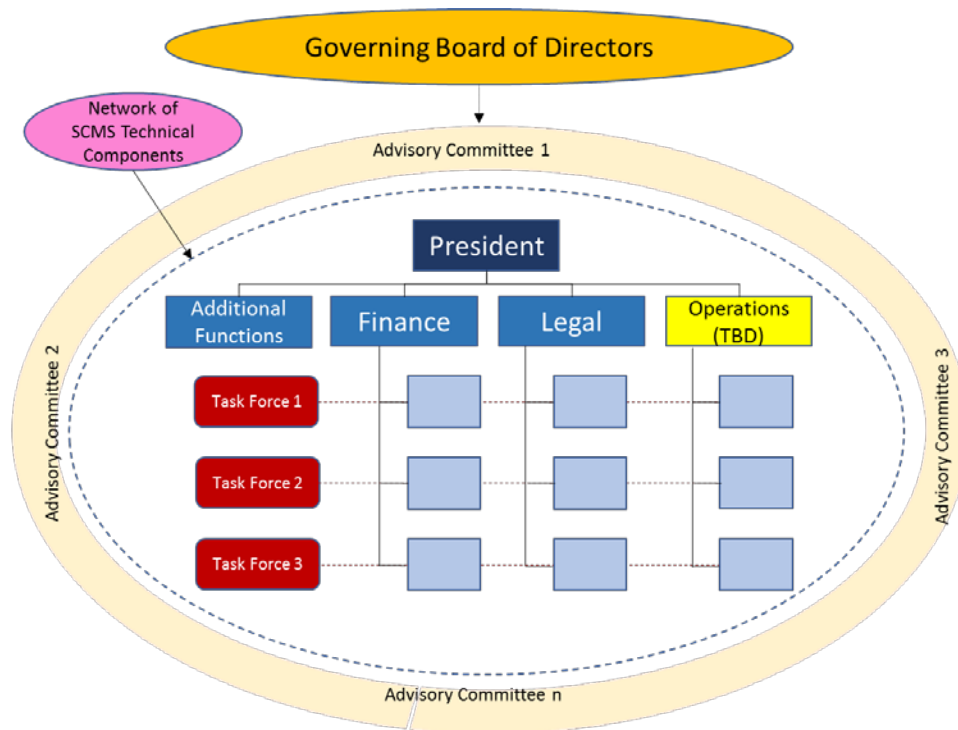

Figure 6: High-level Illustrative Example of an SCMS Manager Organizational Structure

In this case, traditional functional groups such as Finance, Legal, Audit, and Communications are at the core of the SCMS Manager. It is likely that a president will be initially appointed or elected by the governing board of the SCMS Manger to lead the organization. There may be various committees taking leadership roles to address numerous policy- and standards-setting responsibilities, working closely with the functional groups. Meanwhile, there can be working groups and task forces consisting of SMEs from the functional groups and the committee member companies collaborating with each other to address specific issues as project teams.

Under each topic- or component-specific committee, there can be sub-committees tasked with developing and updating policies and standards for specific areas of SCMS.

Acronyms

Table 10: Acronyms

Acronym	Definition
AUTOSAR	Automotive Open System Architecture
CA	Certificate Authority
CME	Certificate Management Entity
CRL	Certificate Revocation List
CV	Connected Vehicle
DCM	Device Configuration Manager
DG MOVE	Directorate-General for Mobility and Transport
DMV	Department of Motor Vehicles
DSRC	Dedicated Shortrange Radio Communication
ECA	Enrollment Certificate Authority
EE	End Entity
EFF	Electronic Frontier Foundation
EICC	Electronic Industry Citizenship Coalition
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FHWA	Federal Highway Administration
ICA	Intermediate Certificate Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IP	Internet Protocol
IT	Information Technology
ITS	Intelligent Transportation Systems
LA	Linkage Authority
LOP	Location Obscurer Proxy
MA	Misbehavior Authority
MOU	Memorandum of Understanding
NHTSA	National Highway Traffic Safety Administration
PKI	Public Key Infrastructure
OBE	On-board Equipment
OBU	On-board Unit
OEM	Original Equipment Manufacturer
OIP	Other Interested Parties
PCA	Pseudonym Certificate Authority
SME	Subject Matter Expert

Acronym	Definition
RA	Registration Authority
RBA	Responsible Business Alliance
RFC	Request for Comments
RFP	Request for Proposal
ROI	Return on Investment
RSE	Roadside Equipment
RSU	Roadside Units
SCMS	Security Credential Management System
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VICS	Vehicle Information and Communication System

U.S. Department of Transportation