National Security Credential Management System (SCMS) Deployment Support

Literature Search Report

www.its.dot.gov/index.htm

Final Report – March 12, 2018
FHWA-JPO-18-687

U.S. Department of Transportation

Produced by Booz Allen Hamilton
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology

Notice

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-18-687		

4. Title and Subtitle	5. Report Date
National Security Credential Management System (SCMS) Deployment Support: Literature Search Report	March 12, 2018
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Joshua Kolleda, Tyler Poling, David Fitzpatrick, Scott Andrews, James Marousek, Lawrence Frank, Joanne Thornton	

9. Performing Organization Name and Address	10. Work Unit No. (TRAIS)
Booz Allen Hamilton 8283 Greensboro Drive McLean, VA 22102	11. Contract or Grant No.

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
	Final Report
	14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

This report provides an overview of publicly available literature and documentation describing efforts around the world to deploy connected vehicle (CV) technologies, and the supporting credential management systems; large-scale public key infrastructure (PKI) systems; and other relevant industry governance model developments, deployments, and operations. This report explores the best practices, lessons learned, and takeaways that will be leveraged in developing recommended National Security Credential Management System (SCMS) ownership and governance models.

17. Keywords	18. Distribution Statement
Security Credential Management System (SCMS), Proof of Concept, Connected Vehicles, Pilots, Public Key Infrastructure (PKI), Ownership and Governance Models	

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
		104	

Table of Contents

List of Tables

List of Figures

Executive Summary

This report provides an overview of publicly available literature and documentation describing efforts around the world to deploy connected vehicle (CV) technologies, and the supporting credential management systems; large-scale public key infrastructure (PKI) systems; and other relevant industry governance model developments, deployments, and operations. This report explores the best practices, lessons learned, and takeaways that will be leveraged in developing recommended National Security Credential Management System (SCMS) ownership and governance models.

The National SCMS Deployment Support project is intended to help identify and explore potential strategies for the establishment and governance of a National SCMS ecosystem through thoughtful engagement with stakeholders to seek guidance and potentially gain consensus on these strategies. Ideally, the outcome will produce next steps to implement the consensus strategy or strategies.

In leading up to the development of potential National SCMS ownership and governance models, the project team reviewed the activities and models developed by international vehicle-to-everything (V2X) deployment efforts, other large and distributed PKIs across private and public sectors, and the history and details of other industry ownership and governance models. While the National SCMS has a unique design and is more complex than other PKIs to ensure privacy, it is still useful to review and consider information and benchmarks from other deployments. Finally, the team conducted a scan of other industry policy development and governance organizations to learn more about models that may not have been covered by only researching other V2X system and PKI implementations. Based on this high-level methodology, the team reviewed each organization in the context of its ecosystem structure, internal organizational structure, oversight and governance approach, funding approach, and policy development and approval approach.

Through this literature and documentation review, the project team identified best practices, lessons learned, and takeaways in the design, development, and deployment of policy setting, governance, and accreditation organizations. Proposed ownership and governance models will incorporate the unique public interest objectives, design and deployment criteria, and interest areas explored within the SCMS Baseline Summary Report. All recommended models will need to fulfill those objectives and criteria to ensure a functional, secure, and sustainable SCMS that maintains vehicle privacy.

International V2X Security System Development and Deployment Efforts

Based on existing deployments and available information, this analysis primarily focuses on the European Commission, which has a full-fledged and separable SCMS work program. To a lesser extent, the analysis summarizes known information on the research, development, and deployment efforts in Japan, Korea, China, Australia, Canada, and Mexico.

Takeaways from international solutions are limited to the European Union (EU), which has a maturing V2X security system development and deployment effort. The European Commission's trust model

concept for multiple roots provides additional redundancy and interoperability, while also allowing for more flexibility in expanding and decentralizing operations. Their common policies ensure interoperability among the cooperative intelligent transportation system (C-ITS) stations (e.g., vehicles or infrastructure stations), which will be enrolled and authorized under various root certificate authorities (CAs). The EU's governance structure concept has addressed trust anchor management coordination through the Trust List Manager (TLM), European Certificate Trust List (ECTL), and C-ITS Point of Contact (CPOC). The European Commission's trust model has also effectively structured audit procedures through the Accredited PKI Auditors. Also, the EU has already developed their initial certificate policy (CP), which provides an input to the governance model and describes a structured process for developing, modifying, and approving policies for certificates. Finally, the European Commission has developed potential high-level funding models for each role within the trust model, as well as a registration fee structure to sustain the TLM and CPOC.

PKI-Specific Ownership, Governance, and Operational Models

This analysis provides a summary of three PKI models: CA/Browser (CA/B) Forum (private sector); US Government Federal PKI (public sector); and EU Digital Signature Infrastructure (public sector). While the SCMS has a more complex design to protect the privacy of vehicle owner/operators, each one of these PKIs is a large-scale, distributed system with its own unique challenges and objectives.

The CA/B Forum is a good example of an industry-deployed PKI policy development body. In 2005, the CA/B Forum was formed as a collaborative and voluntary group of commercial CAs, Internet browser software vendors, and suppliers of other applications that use X.509 v.3 digital certificates for Secure Sockets Layer/Transport Layer Security (SSL/TLS) and code signing after several high-profile security breaches. Browser vendors include Microsoft, Mozilla, Google, and Apple. PKI providers include DigiCert, Entrust, LetsEncrypt, and Comodo. Members of the CA/B Forum have worked closely together in defining the guidelines on how to implement best practices as a way of providing heightened security for Internet transactions and creating a more intuitive method of displaying secure sites to Internet users. PKIs that meet the criteria of one or more product vendors are called "publicly trusted." The CA/B Forum performs the policy development portion of the SCMS Manager function. It does not operate or provide oversight and governance of the PKIs, which adhere to the policies developed by the CA/B Forum. It also does not have any role in the certification of the products consuming the certificates or the implementation of misbehavior and revocation processes beyond specifying the requirements for them as part of the policy. The CA/B Forum policy development process is well thought-out and provides an appropriate level of transparency to ensure that the policies properly balance security and cost. While the distributed oversight and governance model simplifies the CA/B Forum's roles and responsibilities, it also presents the potential for certificates from compliant PKIs to fail because they did not meet a specific vendor requirement that may not be a requirement of other product vendors.

The US Government Federal PKI is a good example of a PKI model with multiple roots and multiple certificate policies. The US Government Federal PKI establishes policies and provides oversight and governance to Federal Agency PKIs, such as those for the Department of Defense, Department of Treasury, and Department of State. It also operates a bridge PKI to facilitate trust with externally operated PKIs. Among the PKIs overseen and operated by the Federal PKI are the Federal Bridge Certificate Authority (FBCA) and the Common Trust Framework (Common) PKIs. The Federal PKI performs all the functions that are expected of the SCMS Manager except operation of the misbehavior authority. It

conducts policy development, oversight, and enforcement of the policies. It also directly manages the roots for the primary PKIs, for which it is responsible. The policy development and approval process used by the Federal PKI is a standard practice for a government policy body. It provides significant opportunity for participants to have their voices heard on both the substance of the change and the decision to approve it for implementation. It lacks the public discussion and transparency that will be expected of a PKI that impacts the majority of Americans. The mapping of member PKI certificate policies to the FBCA CP would serve as a good example if the SCMS will have multiple roots operated by separate entities. If the SCMS will have a single PKI operated under a single root managed by the SCMS Manager, the Federal PKI method of performing compliance analysis would serve as an appropriate model.

The EU Digital Signature Infrastructure is a good example of a PKI model with multiple roots and multiple certificate policies. Additionally, the EU Digital Signature Infrastructure is a good comparison to the US Government Federal PKI regarding oversight and governance. In 1993, the European Commission issued the Electronic Digital Signature Directive (EDSD). It established the initial requirements for member nations to harmonize the use of digital signature technologies to enhance business and commerce (i.e., electronic identification and trust services for electronic transactions in the European Single Market). The Electronic Identification and Trust Services Regulation (eIDAS) replaced the EDSD. It provides a consistent legal framework for recognition of electronic signatures and identities across the EU. The eIDAS infrastructure consists of a policy development and oversight mechanism and uses trust lists to provide consuming applications with a current list of trusted service providers (TSPs). Trust lists are maintained by national level authorities within each member country (e.g., Ministry of Interior of the Czech Republic, Danish Agency for Digitisation). While individual nations maintain the trust lists, all the lists are consistent with the EU standards. The infrastructure is responsible for the implementation of electronic signatures in applications and software and for the security and interoperability of the PKIs implemented by TSPs. The diverse nature of funding that supports eIDAS infrastructure provides several potential funding streams for the National SCMS. While not all of these funding streams are relevant, some of them may point to potential methods of funding depending on the model ultimately selected for the SCMS Manager.

Other Ownership, Governance, and Operational Models in Industries and Ecosystems Analogous to the National SCMS

In this review, the team discusses high-level approaches to ownership, policy development, and governance across multiple industries and domains to gain perspective on the different governance needs and methods. The report also dives into brief case studies of organizations that the team believes exhibit potential best practices and/or lessons learned that could help the team and stakeholders develop an efficient and effective ownership, governance, operational, and initial deployment model. Table 1 summarizes each reviewed organization's policy development and governance responsibility and authority.

Table 1. Summary of Select Industry and Domain Policy Development and Governance Models

Example Policy and/or Governance Organization	Policy Development Responsibility and Authority	Governance Responsibility and Authority
Vehicle Information and Communications System (VICS) – Automotive	Originally sponsored by the Japanese National Police Association, Ministry of Construction, and the Ministry of Posts and Telecommunication to develop a national system for the provision of traffic information. Developed the early guiding policies for the VICS system through collaboration between the sponsoring ministries and the participating organizations (car makers, equipment manufacturers, academia, and other public and private organizations and institutes)	Governed by a combination of ministry policies, usually jointly developed by the ministries associated with or responsible for a given technical area and the industries who are responsible for implementing the system. These policies guide the establishment of P3s such as the VICS center. The companies that provide staff for the center also sit on the management board and provide the overall governance implemented jointly between the government ministries who have established the operation and the private companies, institutes, and universities that operate it. The cooperative nature of Japanese society, and the general level of trust between the various parties facilitates the effectiveness of this approach
AUTomotive Open System ARchitecture (AUTOSAR) – Automotive	Develop standards for automotive software architecture through an alliance of 230 original equipment manufacturers (OEMs), Tier 1 automotive suppliers, semiconductor manufacturers, software suppliers, tool suppliers, consulting firms, and universities	None
GENIVI Alliance – Automotive	Develop and drive the broad adoption of open source, In-Vehicle Infotainment (IVI) software and providing open technology for the connected car through an alliance of OEMs, Tier 1s, middleware suppliers, hardware suppliers, and semiconductor manufacturers	Manages a members-only GENIVI Compliance program
International Civil Aviation	United Nations (UN) specialized agency, established in 1944 to manage the administration and governance of the Convention on	ICAO's Universal Security Audit Program (USAP) conducts documentation-based, oversight-

Example Policy and/or Governance Organization	Policy Development Responsibility and Authority	Governance Responsibility and Authority
Organization (ICAO) – Aviation	International Civil Aviation. Develop and reach consensus on international civil aviation Standards and Recommended Practices (SARPs) and policies in support of a safe, efficient, secure, sustainable, and environmentally responsible civil aviation sector through 192 member states and industry groups	focused, and compliance-focused audits for states
NAV CANADA – Aviation	NAV CANADA develops air navigation system policies through a market driven approach, collaboratively developed and enforced via the Advisory Committee, the Board of Directors, and the executive management team	NAV CANADA manages air traffic operations but does not have an enforcement role. Instead, NAV CANADA is governed by the Aeronautics Act and the Canadian Aviation Regulations (CARs). Audits are conducted internally and externally by third parties
Payment Card Industry Security Standards Council (PCI SSC) – Banking	Sets industry-wide security standards through collaboration and consensus among members, and providing education and training to the larger industry. Developed and maintains the Data Security Standard, Personal Identification Number (PIN) Transaction Security Requirements, and Payment Application Data Security Standard	Enforcement of the standards through compliance programs, and imposing of non-compliance penalties such as fines, is the responsibility of individual payment card brands. Penalties for non-compliance with any required standards would be dictated by the voluntary agreement between the payment card brands and the merchants and service providers under contract
Responsible Business Alliance (RBA) – Manufacturing	Works with its more than 110 members and their Tier 1 suppliers to develop supply chain capabilities to assess and address social and environmental risks as they relate to its Code of Conduct	Holds members accountable to their Code of Conduct commitment via a range of mandatory accountability and assessment means, including self-assessment questionnaires, audits, and corrective actions where necessary. RBA applicant members have two years from the date they join the RBA to conform to the requirements
SEMATECH – Manufacturing	Originally created as a partnership between the United States Government and 14 US-based semiconductor manufacturers to	None

Example Policy and/or Governance Organization	Policy Development Responsibility and Authority	Governance Responsibility and Authority
	solve common manufacturing problems and regain competitiveness for the US semiconductor industry that had been surpassed by Japanese industry in the mid-1980s. Now, an international consortium that performs research and development to advance chip manufacturing	
Internet Corporation for Assigned Names and Numbers (ICANN) – Communications/Internet	Originally established by the Federal government, through a proposed rulemaking to privatize the management of Internet names and addresses allowing for the development of competition and facilitation global participation in Internet management as well as address issues relating to Domain Name System (DNS) management	Responsible for coordinating the maintenance and procedures of several databases related to the namespaces of the Internet, ensuring the network's stable and secure operation
The Joint Commission – Healthcare	Develop standards with input from health care professionals, providers, subject matter experts, consumers, and government agencies (including the Centers for Medicare & Medicaid Services). Standards are informed by scientific literature and expert consensus and reviewed by the Board of Commissioners	Accredits more than 21,000 US health care organizations and programs. The international branch accredits medical services from around the world. A majority of US state governments recognize Joint Commission accreditation as a condition of licensure for the receipt of Medicaid and Medicare reimbursements

Best Practices, Lessons Learned, and Takeaways Applicable to a National SCMS

While the National SCMS is a unique, large-scale, distributed PKI system, deployers can apply concepts and lessons learned from other policy development and governance organizations (PKI-related or not). Themes and commonalities start to emerge as one reads the descriptions of the international V2X development and deployment efforts, public and private PKI systems, and other industry policy and governance organizations. Many of the same concepts can be implemented within the National SCMS and the SCMS Manager to increase the internal organizational efficiency and ability of the SCMS Manager to provide effective industry governance and enforcement to fulfill public interest objectives.

Of the organizations reviewed, the European Commission's V2X credential management system approach and the large, distributed PKI systems (i.e., CA/B Forum, US Government Federal PKI, and EU Digital Signature Infrastructure) provide the most direct applicable best practices, lessons learned, and takeaways in standing up a functional, secure, and sustainable National SCMS ecosystem. However, the policy development and governance organizations from other industries provide unique perspectives and ideas for developing industry consortia, ensuring sufficient stakeholder representation, implementing funding mechanisms, developing the governance organization's internal structure, and phasing organizational deployment. All of these factors should be considered when developing ownership, governance, and deployment models for the National SCMS.

Chapter 1. Introduction

This chapter provides the National SCMS Deployment Support project's background and purpose, a brief discussion of the organizations reviewed within subsequent chapters of the report, and a justification for why the team selected to evaluate these organizations. Later sections of the report identify best practices, lessons learned, and takeaways that could be used to assist in the deployment of the National SCMS ecosystem, as well as ownership and governance model.

1.1 Background and Purpose

The National SCMS Deployment Support project is intended to help identify and explore potential strategies for the establishment and governance of a National SCMS ecosystem through thoughtful engagement with stakeholders to seek guidance and help drive towards consensus on these strategies. Ideally, the outcome will also produce next steps and milestones to implement the consensus strategy or strategies. The strategies will include guidance and plans regarding:

- Establishment of an SCMS Governance Board (or similar oversight entity), 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"
- Establishment of management entities that will be part of the larger SCMS delivery system (and whose authority is directly dependent on and linked to the SCMS Manager)
- High-level policies and procedures that define and guide interactions among the various entities that make up the SCMS
- 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, and industry associations)
- Business and financial options for initial deployment and sustainable operations.

In leading up to the development of potential National SCMS ownership and governance models, the project team reviewed the activities and models developed by international vehicle-to-everything (V2X) deployment efforts, other large and distributed PKIs across private and public sectors, and the history and models of other industry ownership and governance models. Through this literature and documentation review, the National SCMS Deployment Support team identified best practices, key takeaways, and lessons learned in the design, development, and deployment of policy setting, governance, and accreditation organizations. The team will use these lessons and benchmarks in our follow-on task to develop a range of recommended National SCMS ownership and governance models. These models will also incorporate the unique public interest objectives, design and deployment criteria, and interest areas explored within the SCMS Baseline Summary Report. All recommended models will need to fulfill those objectives and criteria to ensure a functional, secure, and sustainable SCMS that maintains vehicle privacy.

1.2 Organization and Deployment Efforts Within this Report

This subsection discusses how the National SCMS Deployment Support team must research existing ownership, governance, operations, and deployment models to identify potential concepts to include within the National SCMS.

First, the team determined types of systems and organizations that could provide benchmarks or takeaways in the development of National SCMS ownership and governance models, as well as the deployment of those models.

An obvious area to explore are other V2X system development and deployment efforts globally. The team engaged personnel involved with standards harmonization and internal working groups to gather publicly-available information on the general deployment efforts, as well as the specific credential management system deployments.

Because the National SCMS is a large, distributed PKI implementation, the team decided to research other large-scale PKI implementations in the public and private sectors. While the National SCMS has a unique design and is more complex than other PKIs to ensure privacy, considerable information and benchmarks can be taken from other deployments. The team already has extensive experience with the US Government Federal PKI and conducted additional research on other PKI implementations using publicly-available information.

Finally, the team conducted a scan of other industry policy development and governance organizations to learn more about models that may not have been covered by only researching other V2X system and PKI implementations. The team reviewed existing reports and analyses, such as those conducted by the Vehicle Infrastructure Integration Consortium (VIIC) and the USDOT during the National Highway Traffic Safety Administration's (NHTSA's) Advanced Notice of Proposed Rule Making (ANPRM) and Notice of Proposed Rule Making (NPRM) development efforts. The team also scanned publicly-available information.

Based on this high-level methodology, the team reviewed each organization in the context of its ecosystem structure, internal organizational structure, oversight and governance approach, funding approach, and policy development and approval approach.

1.2.1 International V2X Security System Development and Deployment Efforts

Chapter 2 provides a summary of international V2X technology and security system development and deployment efforts. This information will be used to identify takeaways and best practices to be leveraged within potential ownership and governance models for the National SCMS. These international efforts also provide varying perspectives on goals and objectives for their deployments, which may shape our model evaluation criteria. Based on existing deployments and available information, this section primarily focuses on the European Commission, which has a full-fledged and separable SCMS work program. To a lesser extent, this chapter also summarizes known information on the research, development, and deployment efforts in Japan, Australia, China, Korea, Canada, and Mexico.

1.2.2 PKI-Specific Ownership, Governance, and Operational Models

Chapter 3 reviews three PKI models: (1) Certification Authority/Browser Forum (private sector), also known as the CA/Browser Forum or CA/B Forum; (2) US Government Federal PKI (public sector); and (3) EU Digital Signature Infrastructure (public sector). While the SCMS has a more complex design to protect the privacy of vehicles and their operators, each one of these PKIs is a large-scale, distributed system with its own unique challenges and objectives. Each section analyzes the general system purpose as well as the ownership, governance, operational, and initial deployment models, focusing on the same questions as in Chapter 2 (e.g., approach to funding). This chapter uses this information to identify takeaways and best practices to be leveraged within potential ownership and governance models for the National SCMS.

1.2.3 Other Ownership, Governance, and Operational Models in Industries and Ecosystems Analogous to a National SCMS

Chapter 4 focuses on analyzing the ownership, governance, operational, and initial deployment models of other policy development and governance bodies. The first subsection discusses high-level approaches to ownership, policy development, and governance across multiple industries and domains to gain perspectives on the different governance needs and methods. The second subsection dives into brief case studies of organizations that the team believes exhibit potential best practices and/or lessons learned that could help the team and stakeholders develop an efficient and effective ownership, governance, operational, and initial deployment model. Specifically, the team conducted reviews of the following organizations:

- Automotive: Vehicle Information and Communications System (VICS), AUTomotive Open System ARchitecture (AUTOSAR), GENIVI Alliance
- Aviation: International Civil Aviation Organization (ICAO), NAV CANADA
- Banking: Payment Card Industry Security Standards Council (PCI SSC)
- Manufacturing: Responsible Business Alliance (RBA), SEMATECH
- Communications/Internet: Internet Corporation for Assigned Names and Numbers (ICANN)
- Healthcare: The Joint Commission.

Chapter 2. International V2X Security System Development and Deployment Efforts

This chapter provides a summary of international V2X technology and security system development and deployment efforts. This information will be used to identify takeaways and best practices to be leveraged within potential ownership and governance models for the National SCMS. These international efforts also provide varying perspectives on goals and objectives for their deployments, which may shape our model evaluation criteria. Based on existing deployments and available information, this section primarily focuses on the European Commission, which has a full-fledged and separable SCMS work program. To a lesser extent, this chapter also summarizes known information on the research, development, and deployment efforts in Japan, Australia, China, Korea, Canada, and Mexico.

Where available, the sections below provide an overview of the international entity's V2X technology and security system development and deployment efforts. This includes multiple subsections, as information is available, focusing on a comparison to the National SCMS, description of the ecosystem structure and internal organizational structure, approach to oversight and industry governance, approach to funding for initial deployment, and approach to policy development and approval. The comparison to the National SCMS will provide information on the entity's concept to maintain security and privacy within the V2X ecosystem with a brief comparison to the SCMS technical and operational concept. Where information is available (specifically, for the EU), the descriptions also begin to:

- Explore how each entity plans to deploy the ownership and governance models for their concept and how those models fulfill the public interest objectives and evaluation criteria that the team has developed for the National SCMS ecosystem
- Provide information on the V2X security ecosystem structure and organizational structure of the security/credential management system ownership and governance model concept
- Provide information on the entity's approach to oversight and industry governance of the security/credential management system
- Provide information on how the governance organization and other entities within the operational concept are funded for initial deployment and sustainment
- Provide information on the approach to certificate (and general) policy development and approval.

2.1 European Commission

2.1.1 Overview

The C-Roads Platform is a joint initiative of European member states and road operators for testing and implementing cooperative ITS (C-ITS)[1] services for cross-border harmonization and interoperability. The C-Roads Platform approach will pursue cooperation on a holistic level to cover dimensions linked with the deployment of C-ITS, such as sharing experiences and knowledge regarding deployment, implementation issues, and user acceptance. It also follows a bottom-up approach that will include national pilots being deployed across Europe.

Within the European Commission, the initial research and development of C-ITS specifications are led by several working groups (WGs). These WGs address specific issues and factors that face the C-ITS Platform and have developed policy recommendations and proposals for action for both the European Commission and other C-ITS relevant actors. The Security WG has taken on the initiative to address concerns around the C-ITS trust model. The Security WG is chaired by the European Commission and consists of industry stakeholders (e.g., automotive manufacturers, infrastructure manufacturers, tier 1 suppliers) and member states. As a result of their efforts, the WG has developed initial versions of two key policies for the C-ITS trust model. The first is C-ITS Certificate Policy for Deployment and Operation of European C-ITS. This document defines the details on the roles and processes for how security certificates are issued to define a common level of trust in C-ITS messages in Europe. The second document is the Security Policy & Governance Framework for Deployment and Operation of European C-ITS. This document defines additional cyber security requirements and specifies who is responsible for all roles in the overall C-ITS scheme including security. While C-ITS does not currently include imminent crash preventative safety applications, the security policy does consider road safety[2] and safety[3].These factors are part of the classification impact types to be considered in terms of the degree of damage or costs to the C-ITS service and C-ITS stakeholders caused by an information security incident.

2.1.2 Comparison to National SCMS

The United States and the European Union are at similar stages of developing a trust model for the V2X ecosystem. Both have developed initial policies and both have CV pilot sites where initial concepts are being tested. The EU C-ITS trust model and the National SCMS are similar in the sense that both send secure and private messages within the V2X ecosystem using a model based on PKI. However, there are some differences as how each go about that process, specifically the trust anchor management method. The SCMS Proof of Concept's current design is the elector concept. Electors operate at a higher level than the root CA by signing trust management messages to be used by other PKI components. 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. End entities and other PKI components know the necessary

[1] C-ITS encompass a group of technologies and applications that allow effective data exchange through wireless communication technologies between components and actors of the transport system, very often between vehicles (vehicle-to-vehicle or V2V) or between vehicles and infrastructure (vehicle-to-infrastructure or V2I).

[2] Road Safety: When the impact places road users at imminent risk for injury

[3] Safety: When the impact places any of the stakeholders at imminent risk for injury

number of such signed trust management messages from non-revoked electors that will authorize the action contained in the messages (e.g., revoke root CA "A"). These messages contain a time frame for the operation to occur. The EU C-ITS is being deployed with a multiple root architecture run by EU members and commercial entities. For centralized coordination, the EU C-ITS uses the European Certificate Trust List (ECTL) to inform end entities of new and revoked roots. In the C-ITS model, there will be a single Trust List Manager (TLM) entity with a certificate trusted by end entities. An updated trust list will be published periodically.

2.1.3 Ecosystem Structure and Internal Organizational Structure

Figure 1 provides an overview of the C-ITS trust system's sub-roles.

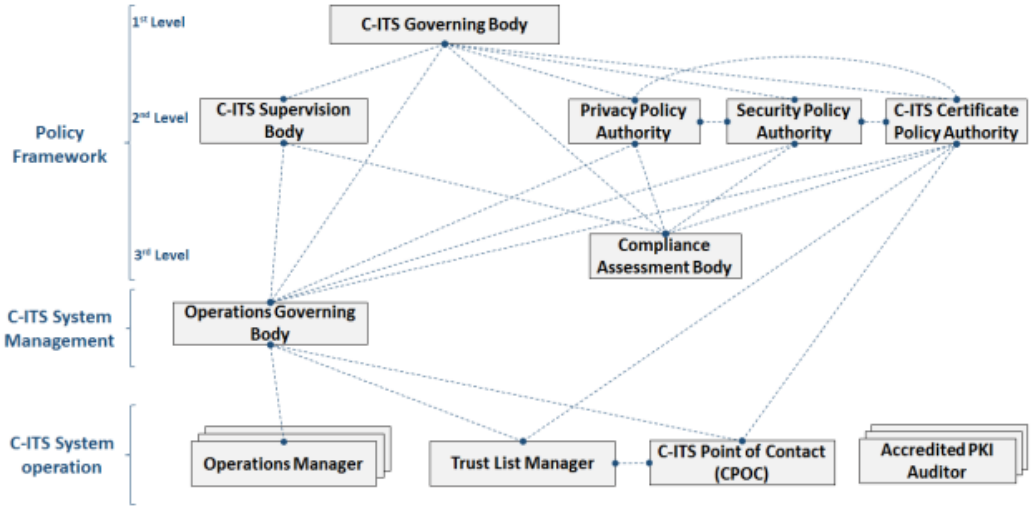

Figure 1. EU C-ITS Trust System Sub-Roles.[4]

C-ITS Governing Body: The C-ITS Governing Body is a single entity and is the top sub-role of the overall C-ITS governance architecture. The Governing Body defines the C-ITS strategy, including the security strategy, and derives rough guidelines from the strategy based on the input from the stakeholder groups. The C-ITS strategy is the high-level plan to enable C-ITS services to be deployed and operated. The C-ITS Governing Body functions in deployment and operation, compliance assessment, and the EU Central Configuration and Management System (CCMS). The C-ITS Governing Body defines rules (including conflict resolution process) for the resolution of issues detected by the C-ITS Supervision Body. The C-ITS Governing Body is the main contact to policy makers (e.g., European council, European parliament, member states' political figures) as well as to international counterparts responsible for the C-ITS infrastructures. The Governing Body should consist of the European Commission, member states, road infrastructure operators, and manufacturers and suppliers. It only reports to bodies outside of the C-ITS domain.

[4] "Detailed Structure View of the Governance Architecture", December 2017. Quoted in the European Commission "Results of C-ITS Platform Phase II: Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)", Release 1, Pp. 12.

C-ITS Supervision Body: The C-ITS Supervision Body is a single entity and deals with technical aspects of the deployment and operation of the C-ITS system. It reports to the C-ITS Governing Body and provides its output to the other roles in the policy framework and to the roles in system management. The C-ITS Supervision Body functions in deployment and operation, compliance assessment, and the EU CCMS. The C-ITS Supervision Body is responsible for detecting issues in the deployment and operational phase, which can be reported to the C-ITS Governing Body and to the Compliance Assessment Body for further analysis and action, based on rules defined by the C-ITS Governing Body. This requires a hierarchical organization to be able to solve issues at the appropriate level and/or report them to the appropriate level. Its responsibilities also include identification, assessment, and monitoring of newly identified security vulnerabilities, as well as ambiguous, unclear, or 'impractical to implement' statements in requirements, regulation, or standards defining the design and operation of the EU CCMS and the C-ITS system. Once identified, the C-ITS Supervision Body makes sure that appropriate changes are made within the requirements and the other documents by the sub-governance body responsible for the particular area that the change affects, including the C-ITS Governing Body if general changes of strategy are required. In that manner, the Supervision Body is responsible for leading the continuous improvement process.

In addition, the C-ITS Supervision Body is responsible for managing large-scale and high-severity incidents, as reported by the Operations Governing Body. This includes providing directives, guidelines, and recommendations to the Operations Governing Body. The Supervision Body should consist of the European Commission, member states, road infrastructure operators, manufacturers, and suppliers.

Certificate Policy Authority: The Certificate Policy Authority is a single entity top-level sub-role of the CCMS domain. It is a second level sub-role in the policy framework that reports to the C-ITS Governing Body and only functions within the EU CCMS. The Certificate Policy Authority is responsible for the approval and maintenance of the Certificate Policy (CP) document. It manages (e.g., reviews, approves or denies, modifies) change requests submitted by other PKI participants or entities, and updates the relevant documents if needed. The Certificate Policy Authority also defines, decides, and publishes the Certificate Practice Statement (CPS) approval and CA audit procedures (collectively referred to as CA approval procedures). They are responsible for authorizing the C-ITS Point of Contact (CPOC) and the TLM to operate and report regularly. The Certificate Policy Authority oversees the approval of the root CA's CPS, if in line with the common and valid CP. Furthermore, the Certificate Policy Authority oversees scrutiny of the audit reports from the Accredited Auditor for all root CAs. They also notify the TLM about approved and not approved root CAs and their certificates based on the received approval reports of the root CAs and the regular operations reports. The Certificate Policy Authority should consist of a common steering committee among the stakeholders (e.g., member states, equipment manufacturers, vehicle manufacturers, infrastructure managers).

Privacy Policy Authority: The Privacy Policy Authority is single entity and is the top level sub-role committee for personal data protection aspects in C-ITS. It is a second level sub-role in the policy framework that reports to the C-ITS Governing Body. The Privacy Policy Authority functions in deployment and operation, compliance assessment, and the EU CCMS.

The Privacy Policy Authority defines and manages the data protection rules for all the users in the C-ITS. It is also responsible for being the central point of contact for the Data Protection Authorities in Europe. Data Protection Authorities can also participate in the implementation of the sub-role Privacy Policy Authority. The Privacy Policy Authority also drafts and maintains the data protection rules for C-ITS, including the ones defined in the CP (in this aspect, the Privacy Policy Authority will work with the

Certificate Policy Authority). The Privacy Policy Authority should consist of a common steering committee among the stakeholders (e.g., member states, equipment manufacturers, vehicle manufacturers, infrastructure managers).

Security Policy Authority: The Security Policy Authority is a single entity and is the top-level sub-role for information security aspects in C-ITS. It is a second level sub-role in the policy framework that reports to the C-ITS Governing Body. The Security Policy Authority functions in deployment and operation, compliance assessment, and the EU CCMS. The Security Policy Authority defines and manages the Security Policy document of the European C-ITS system. It is responsible to draft, publish, and maintain the Security Policy document of the European C-ITS system. The Security Policy Authority should consist of representatives from public and private stakeholder groups (e.g. member states, vehicle manufacturers) participating in the C-ITS trust model.

Compliance Assessment Body: The Compliance Assessment Body is a single entity and is the top level sub-role for C-ITS compliance assessment. It is a third level sub-role in the policy framework that reports to the C-ITS Supervision Body. The Compliance Assessment Body is responsible for operating the Device Registry Database as a central service. This database lists all devices that have been validated for compliance with the criteria defined by the Compliance Assessment Body by accredited test laboratories. The Compliance Assessment Body should be taken over by a committee or working group of stakeholder experts in this area (e.g., for vehicle ITS stations, the security compliance assessment criteria will be provided by a group of security experts from the automotive industry with input from other relevant stakeholders), this includes the C-ITS Governing Body (owner of the process) as well as testing laboratories.

Operations Governing Body: The Operations Governing Body is a single entity at the top level sub-role in system management. The Operations Governing Body reports to the C-ITS Governing Body and the C-ITS Supervision Body in the Policy Framework. It functions in the deployment and operation area and provides its output to the sub-roles of system operation.

The Operations Governing Body is responsible for defining operational requirements derived from the high-level requirements defined by the C-ITS Supervision Body. It coordinates and manages incidents reporting from the Operations Manager as well as checks and ensures compliance of the operation managers with the operational requirements. The Governing Body defines the minimum commissioning/ decommissioning requirements for operational performance, and implements necessary security changes during the operation lifetime of an ITS-Station (ITS-S). It also defines and maintains ITS-S operational requirements. Additionally, it coordinates and manages incidents reporting from the Operations Manager, decides on their global relevance, aggregates those incidents to a global view, and reports to the C-ITS Supervision Body. It is also responsible for receiving directives, guidelines, and recommendations from the Supervision Body and updates the requirements accordingly. Since the Operational Governing Body is unique at European level, it also has the responsibility to coordinate the respective Operation Managers for all the activities and issues, which goes beyond the jurisdiction of a specific Operations Manager. The Operational Governing Body should consist of a common steering committee among the stakeholders (i.e., member states, equipment manufacturers, vehicle manufacturers, infrastructure managers).

Operations Manager: The Operations Manager is a multiple entity, sub-role in system operation. It functions in deployment and operations and reports to the Operations Governing Body in system management. It is responsible to implement the operational requirements as published by the Operations

Governing Body at the C-ITS Station Operation roles. The proper way to enforce the criteria depends on the actual criteria to be set. In addition, the Operations Manager is responsible to manage incidents and report incidents to the upper layers of the Operations Governing body and the C-ITS Supervision body when it does not have the capabilities to address a specific incident or set of incidents in the C-ITS security infrastructure. The Operations Manager may be responsible only for a portion of the EU C-ITS security infrastructure (e.g., a member state or a privately-owned C-ITS infrastructure). It should consist of infrastructure managers (public or private).

Trust List Manager: The Trust List Manager (TLM) is deployed by the European Commission to support common rules to ensure EU wide interoperability and trust in a 4-year, fully-funded pilot phase. The Security WG proposes that the TLM will be taken over by the Commission as an impartial neutral body recognized by all member states, industry representatives and other involved stakeholders; however, long-term ownership and operation is still to be defined. The TLM is a single entity sub-role in system operation that functions in the EU CCMS, and reports to the Operations Governing Body and to the Certificate Policy Authority in system management. The TLM is responsible for the generation and update of the European Certificate Trust List[5] (ECTL) according to the common valid CP and regular activity reporting to the Policy Authority for the overall secure operation of the C-ITS trust model.

C-ITS Point of Contact: The C-ITS Point of Contact (CPOC) will be run by the European Commission. It is a single entity sub-role in system operation and reports to the Operations Governing Body and to the Certificate Policy Authority in system management. The CPOC is responsible for handling all communication with individual root CA managers, publishing the common trust anchor (i.e., public key certificate of the TLM) and the ECTL.

Accredited PKI Auditor: The Accredited PKI Auditor is a sub-role in system operation and will be accredited by a member listed by the European cooperation for accreditation. It is responsible for assessing the compliance of a PKI entity to the European certificate policy by carrying out an audit procedure. The exact responsibilities of the Accredited PKI Auditor are defined in the European C-ITS certificate policy. The Accredited PKI Auditor will have multiple instances and its function will be separate from all other sub-roles.

2.1.4 Approach to Oversight and Industry Governance

Figure 2 defines the EU C-ITS trust system's main organizational roles. There are three main roles of the trust system, which are policy framework development, system operations, and system management.

[5] A list of all operational root CAs by either public or private entities

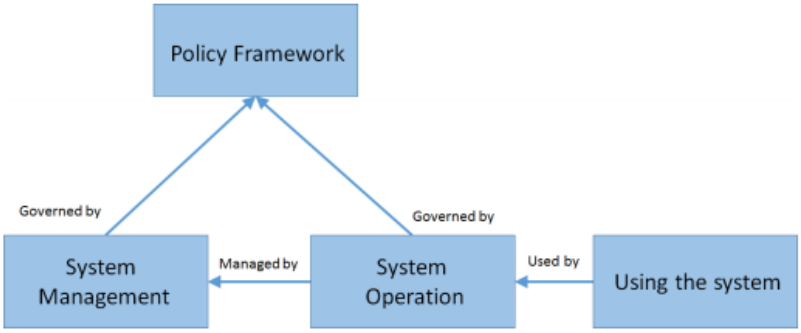

Figure 2. EU C-ITS Trust System Organizational Roles.[6]

The policy framework role is responsible for all the governance and policy management activities required in the system. The actors in this role define policies and regulations to the actors in the European C-ITS trust system, including the actors of system operation and system management. The policy framework consists of three levels for its C-ITS governance architecture. Within the policy framework, the C-ITS Governing Body provides output to the C-ITS Supervision Body, all the Policy Authorities, as well as the Compliance Assessment Body. It also provides output to the roles in system management and only reports to bodies outside of the C-ITS domain. The system operations role is responsible for the proper execution of the applications that provide the end-to-end ITS service(s). The system management role is responsible to fulfill all required management activities within the system, including the definitions of requirements and guidelines for the actors in the system operations role.

The actors in the system operations role support the actors in the system management role to enable and facilitate system management behavior and responsibilities. The actors in the system management role support the actors in the policy management role to enable and facilitate policy management behavior and responsibilities. The legal entities, which are responsible for the governance and operation of the EU C-ITS trust system can have one or more roles or sub-roles. In some cases, a legal entity only fulfills a specific role or sub-role.

The C-ITS trust model is based on a PKI and allows both public and private entities to set up root CAs. These are responsible for issuance of security certificates and revocation of the same certificates under the conditions established in the certificate policy. The definition of common policies is needed to ensure interoperability among the C-ITS stations (e.g., vehicles or infrastructure stations), which will be enrolled and authorized under different root CAs. However, this distributed system design still demands some central coordination role. The coordination role will consist of the TLM and the CPOC. The architecture is composed by a set of root CAs enabled by the TLM. The TLM issues the ECTL that provides trust in the approved European root CAs to all participants of the C-ITS system. Since the C-ITS trust model is based on a multiple root CA architecture, the CPOC is also needed to periodically receive information from the participating root CAs via secure communication. The CPOC role has a close link to the TLM role and takes over operational security functions like the actual certificate verification of root CA certificates and the actual publication of the ECTL. Both the TLM and the CPOC are appointed by the Certificate Policy

[6] "Main Organizational Roles", December 2017. Quoted in the European Commission "Results of C-ITS Platform Phase II: Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)", Release 1, Pp. 10.

Authority. The C-ITS Platform Security WG proposes that these centralized roles will be taken over by the Commission as an impartial neutral body recognized by all member states, industry representatives, and other involved stakeholders.

In general, a root CA can be operated by a governmental (i.e., European member state) or a private organization. However, to guarantee the functioning of the C-ITS security scheme with a high level of availability, there is a need that at least one root CA is always available in the C-ITS trust model architecture. Therefore, an EU root CA will be provided to all the entities participating in the C-ITS trust model that do not set up their own root CA. This is especially needed in the start-up phase of the C-ITS trust model to ensure that C-ITS deployment initiatives (e.g., gathered under the C-ROADS platform) can test and operate their initial deployments in an interoperable manner. The Security WG proposes that the set-up of the EU root CA will be started by the Commission as an impartial neutral body recognized by all member states and industry representatives, but the actual operation of the EU root CA could be the contracted responsibility of a commercial company. The sub-CAs of the EU root CA (Enrollment Authority and Authorization Authority) could also be run by contracted entities.

2.1.4.1 Enrollment

The PKI participants (Enrollment Authority [EA], Authorization Authority [AA], C-ITS stations [ITS-S]) will be able to use public keys for encryption of enrollment and authorization requests/responses with selected algorithms listed below. The actual algorithm that is used will be defined in the CPS of the CA that issues the certificate for the corresponding public key, in accordance with this CP.

- Mandatory: EA, AA, ITS-S: ECIES_nistP256_with_AES128_CCM
- Mandatory: EA, AA, Optional: ITS-S: ECIES_brainpoolP256r1_with_AES128_CCM.

2.1.4.2 Auditing

The CA to be audited will select an independently acting and accredited company/organization ("Auditing Body") or Accredited Auditors to audit the CA according to the Common Certificate Policy. The Auditing Body will be accredited and certified by a member of the European Accreditation Body.[7]

The purpose of a compliance audit is to verify that the TLM, root CA, EA, and AA operate in accordance with the applicable CP. The TLM, root CAs, EAs, and AAs will select an independent acting and certified auditor for auditing this CP and its CPS. The audit will be combined with the physical security controls compliance in ISO 27001 and ISO 27002. When requested, an accredited auditor will perform a compliance audit on one of the following levels:

1. Conformity of the TLM, root CA, EA, AA Certification Practice Statement with the CP
2. Conformity of the TLM, root CA, EA, AA intended practices with its Certification Practice Statement prior to operation
3. Conformity of the TLM, root CA, EA, and AA practices and operational activities to its Certification Practice Statement during operation.

[7] Members of the European Accreditation Body are listed at: http://www.european-accreditation.org/ea-members

In case of a TLM with a non-compliant audit report, the Policy Authority (PA) will order the TLM to take immediate preventive actions.

In case of a new application of a root CA with a non-compliant audit report, the PA will reject the application and send a corresponding rejection to the root CA. In this case, the root CA will be suspended and it will need to take corrective actions, re-order the audit, and request a new PA approval. The root CA will not be allowed to issue certificates during the suspension.

In case of a regular root CA audit, or in case of a change of root CA's CPS – and depending on the nature of the incompliance described in the audit report – the Policy Authority may decide to revoke the root CA and communicate this decision to the TLM, causing the deletion of the root CA certificate from the ECTL and insertion of the root CA on the CRL. The Policy Authority will send a corresponding rejection to the root CA. In this case, the root CA will need to take corrective actions, re-order a full audit, and request a new Policy Authority approval. Alternatively, the Policy Authority may decide to not revoke the root CA, but to give it a grace period in which the root CA will undertake corrective actions, re-order an audit, and re-submit the audit report to the Policy Authority. In this case, the root CA operation must be suspended and it is not allowed to issue certificates and CRLs.

In case of an EA/AA audit, the root CA/private company will decide to accept the report. Depending on the audit result, the root CA will decide whether to revoke the EA/AA certificate according to rules defined in the root CA's CPS. The root CA will always ensure compliance of the EA/AA to this CP.

2.1.5 Funding for Initial Deployment and Sustainment

The initial funding for deployment of the trust model will come from the European Commission. The member states have allotted €300 million to infrastructure-side deployment. Currently, member states are funding the development and operation of the roots through commercial contracts. Sustainable funding models for the roles within the trust management system are being developed. The table below shows initial funding approaches developed by the European Commission for each role.

Table 2. EU C-ITS Funding Model

Funding Model	Role
Funded by a public private partnership or by public funding with the presence of the European Commission	• C-ITS Governing Body
Funded by a public private partnership and/or by public funding	• C-ITS Supervision Body • Privacy Policy Authority • Security Policy Authority • Compliance Assessment Body • Operations Governing Body • Certificate Policy Authority
Member state or private funding	• Operations Manager
Initial public funding with a sustainable business model funded by the C-ITS users	• Trust List Manager • C-ITS Point of Contact

Funding Model	Role
Organizations based on the necessity to accredit the PKI elements, which must participate to the EU CCMS	• Accredited PKI Auditor

One principle of the implemented EU C-ITS trust model is that the root CAs together are fully financing the regularly recurring costs of operation of the Policy Authority and the central elements (TLM and CPOC) for performing the activities as defined in this Certificate Policy. The root CAs and the EU root CA are entitled to take fees from their sub CAs. For the full time of operation at least one root CA, EA and AA shall always be available for every C-ITS trust model participant. Each root CA pays fees to the Policy Authority and the central elements. Each root CA is entitled to charge those fees to the registered participants including the enrolled and authorized C-ITS stations. According to the certificate policy, the initial establishment of a root CA shall at least cover three years of operation to become member of the C-ITS trust model. Each root CA needs to demonstrate the financial viability of the entity implementing the root through a financial viability plan, which needs to be updated every three years and reported to Policy Authority. Each root CA must report the applied charges structure for EA /AA and the enrolled and authorized C-ITS Stations per year to the Operations Manager and the Policy Authority to demonstrate its financial sustainability. Furthermore, all responsible entities for the roots CA, EA, AA and the central elements are required to cover their operational duties with insurance adequate to financially compensate for errors of operations of their duties if one of the technical elements fails.

2.1.6 Approach to Policy Development and Approval

The Policy Authority administers policy on behalf of the entities of the EU C-ITS trust model.

2.1.6.1 Updating Certificate Policy

The CP is subject to continuous improvement. The update process is managed by the Certificate Policy Authority. This policy will be checked and updated every 3 years. The steps for updating the CP are listed below.

1. **Submission of the change request**. The change process is initialized by a change request from a stakeholder. The request contains information, including a brief description and rationale of the change, a criticality classification for security of the system, and the change requester contact. The change requester should be prepared to answer requests for additional information and/or defend the change proposal at the Policy Authority.
2. **Change processing.** The Policy Authority confirms reception of the change request and processes the change by assessing the applicability, completeness, criticality, and impact of the change. If change processing confirms the change as critical for the security of the C-ITS system or due to a disaster recovery scenario, it becomes an emergency change request resulting in an expedited process.
3. **Change approval.** The Policy Authority conducts change approval meetings to discuss and decide if a change request is accepted. Following the meeting, the Policy Authority can fully or partially accept the change request or decide on a modified change request. They can also request modification of the change request and resubmission of the request, or fully reject the change request.

4. **Change publication and announcement.** After approval, the Policy Authority will publish an updated provisional version of the CP and announce the implementation with an effective due date and an implementation time frame for the transition beginning once the new policy becomes effective to all root CAs listed on the ECTL.
5. **Change implementation.** Each root CA listed on the ECTL will implement changes and provide evidence to fulfill the changed requirements to the Policy Authority. The Policy Authority updates the CP to match the provisional CP and the updated CP replaces the previous version of the CP.

2.1.6.7 Updating of CPS' of CAs Listed in the ECTL

Each root CA on the ECTL will publish its own CPS compliant to this policy. A root CA may add additional requirements but will ensure all CP requirements are met at all times. Root CAs will also implement a suitable change process for its CPS document and key properties will be documented within the public part of the CPS.

The change process will include appropriate measures to verify CP compliance for all changes to its CPS. Any changes to the CPS will be clearly documented. Before implementing a new version of a CPS, its compliance to the CP must be confirmed by an accredited auditor. The root CA will notify the Policy Authority about any change made to the CPS.

2.1.6.8 CPS Approval Procedures

A prospective root CA will present its CPS to an Accredited Auditor as part of an order for a compliance audit and to the Policy Authority for approval before starting its operations. A root CA will present changes to its CPS to an Accredited Auditor as part of an order for compliance audit and to the Policy Authority for approval before those changes become effective. An EA/AA will present its CPS or changes to its CP to the root CA. The root CA may order a certificate of conformity by the national body/private entity responsible for approval of the EA/AA. The Accredited Auditor will assess the CPS according to the Compliance Audit and Other Assessments section of the C-ITS Certificate Policy for Deployment and Operation of European C-ITS. The auditor will also communicate the CPS assessment results as part of the audit report.

2.2 Japan

Besides its history deploying electronic toll collection systems, Japan has invested in a 700 MHz band suite of V2X services – called ITS Connect – that Toyota has deployed in Japan on its Prius models and other models. ITS Connect could also be deployed across other OEMs. With its different strategy in spectrum use for V2X applications, it is limiting how instructive comparisons can be between the US and Japanese approaches.

Figure 3 provides an overview of Japan's published strategy with regards to major roles. The specifications for securing ITS Connect have broadly been handled by two Japanese organizations:

- The Ministry of Internal Affairs and Communications (MIC) has general responsibility in Japan for information and communications technologies (ICT) policy. Beginning in 2014 they convened an ITS working group at the Information Security Advisory Board, producing two normative documents: "*Security Requirements for 700 MHz Band Safe Driving Support System,*" and "*Security Guidelines for*

the Construction of a 700 MHz Safe Driving Support System." Though apparently only available to implementing members, summaries are available to all. MIC's Security Requirements document specifies requirements for the entities (e.g., onboard system vendors) involved in implementing and managing the V2X services. The guidelines document specifies policies for implementing the V2X services based on the security requirements.

- The ITS Info-Communications Forum is a consortium of nearly 100 industrial members, and with participation from the Japanese national government, including the Ministry of Land, Infrastructure, Transport, and Tourism. The National Police Agency is a member and is particularly vested in the ITS Connect project. The forum's mission is to promote research, development, and standardization of ITS-related communications technologies. They have a liaison relationship with Japan's domestic ITS standards bodies. The forum produced the guiding report, "*Security Guidelines for Driver Assistance Communications System*," last updated in November 2013. This report is publicly available.

An "ITS Connect Promotion Consortium" was established in October 2014 to promote the practical use of V2X services in Japan. The members are OEMs, suppliers, and Ministries. This consortium has worked to implement the security guidelines and provides operational management support for ITS Connect, including the security implementation. While we have no clear indication of Japan's strategy around a governing body, this consortium may already have that role or could take it on.

The *ITS Info-Communications Forum's Security Guideline* document does not mandate a specific security approach. For example, it describes two methods for verifying authenticity and integrity: (1) application of a digital signature using a public key algorithm; and (2) using a message authentication code with a shared key algorithm.

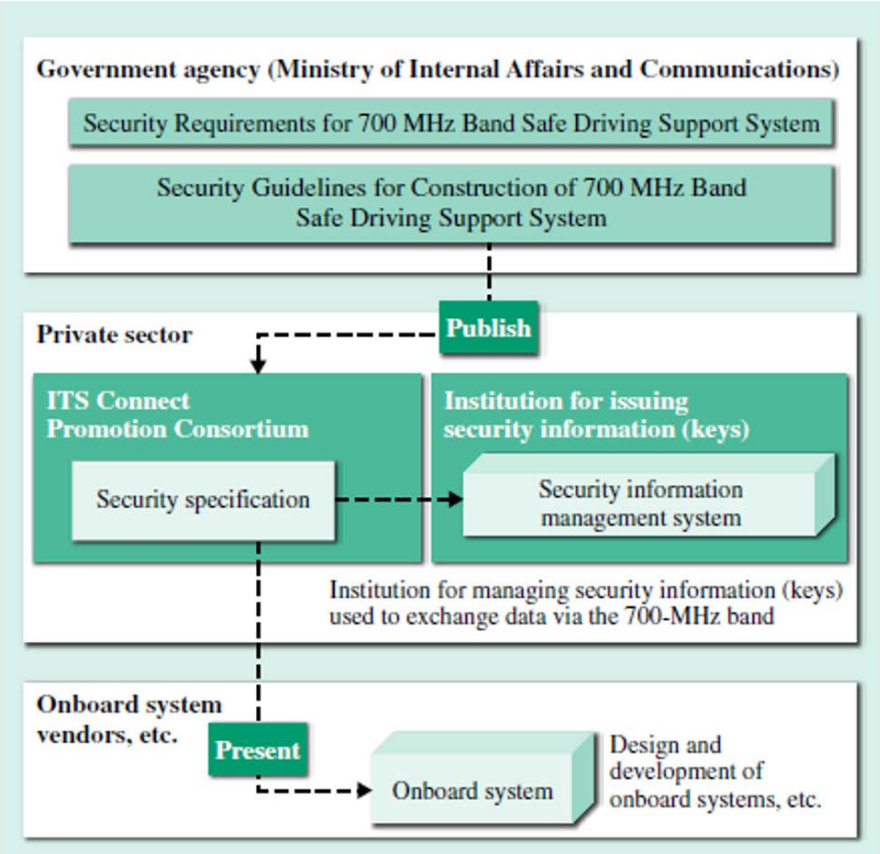

Figure 3. Overview of Public and Private Roles in Establishing V2X Security in Japan.[8]

2.3 Korea

Since 1999, Korea has established a national PKI, which is in use across industries, including Internet banking, online stock trading, and the government's delivery of social services. This is operated under the Information Ministry of Science and Information and Communications Technologies (ICT) and with the organization Korea Internet Security Agency (KISA) acting as the single root CA. This is operated under a national legislative authority that includes specifications and regulations around CA accreditation and the operation of accredited CAs. While there is appreciation for the differences between these types of PKI environments and a vehicular environment – such as use of multiple pseudonym certificates, use of linkage values for efficient verification of the multiple pseudonym certificates, and separate operation of a Misbehavior Authority to verify misbehaviors in vehicles and roadside equipment – Korea is examining

[8] "Security Guidelines for Construction of 700 MHz Band Safe Driving Support System," Japan Ministry of Internal Affairs and Communications, July 2015. Quoted in Mizutani, A., M. Kawamura, E. Ando, and T. Owada, "Security Operation Management Initiatives in Cooperative Vehicle-Infrastructure Systems for Safe Driving," *Hitachi Review*, Vol. 65 (2016), No. 1. Pp. 747-751.

how to leverage its existing infrastructure. In the 2019 timeframe they intend to finalize a decision on whether legal ownership of the vehicular system will be within the ICT Ministry or in the Ministry of Land, Infrastructure, and Transport (MLIT).

Korea has and is running C-ITS pilots featuring V2X use cases, and has plans under development for an automated vehicle focused research test. It has reviewed the PKI designs developed in the EU and the US, and is currently implementing parts of the US design.

An initial proof-of-concept of a V2X PKI system was developed beginning in 2016. This was used in its recently completed C-ITS pilot project, and is a part of the installation of its Cooperative Automated Driving Roadway System (C-ARS) research and development project currently being planned. It will also be employed on additional C-ITS projects including an expressways model deployment and an urban area-focused model deployment.

A security team is focused on the V2X PKI problem specifically, including drafting versions of a C-ITS PKI model; conducting a legal analysis to support an expected, future national rollout; and developing technical guidelines.

The C-ITS PKI model is implementing portions of the CAMP Technical Design of the Proof of Concept SCMS for V2X Communications that our team has described in our *National SCMS Deployment Support: SCMS Baseline Summary Report*. Korea has taken an evolutionary approach, initially building a segment of the technical architecture that included enrollment CAs, pseudonym CAs, a Registration Authority (RA), and CRL generator. They have also included LAs but have expressed concern regarding the added cost of this, and have noted a less expensive alternative that the EC is developing.

Korea is working with its OEM community on implementing misbehavior detection, and plan to build a full Management Authority (MA), which could be a public entity or a consortium of OEMs.

Figure 4 below depicts their intended “to be” architectural state in 2018, which will support the upcoming research efforts and model deployments noted above.

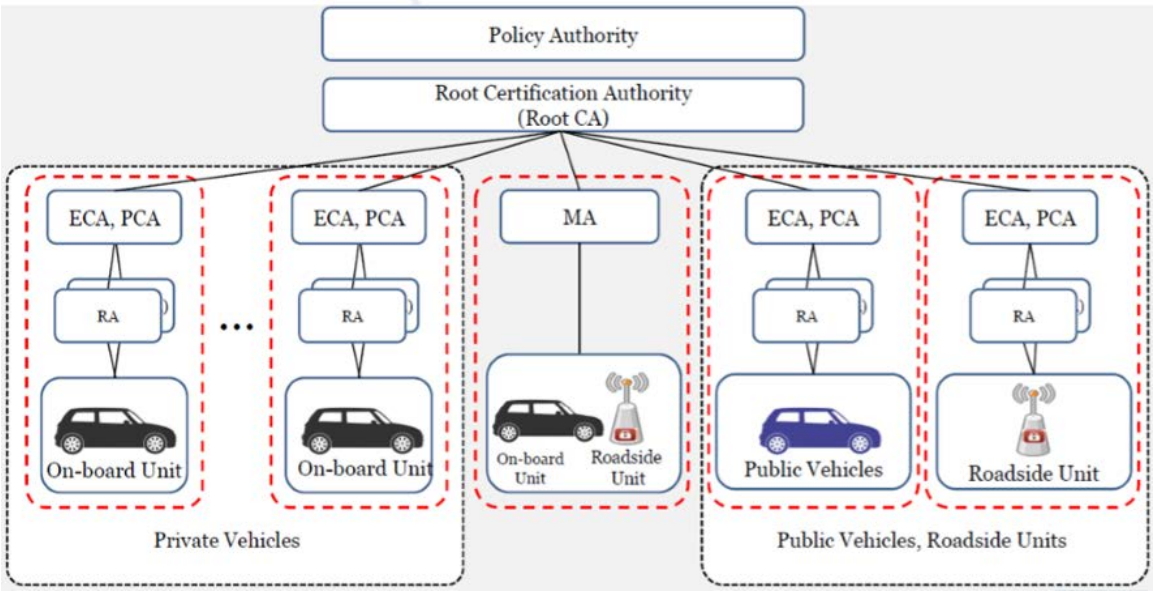

Figure 4. Intended Architecture for Korea C-ITS Trust Model.[9]

2.4 China

China has numerous connected vehicle pilots being conducted or planned, including a National Intelligent Connected Vehicle Pilot in Shanghai. China appears to be looking to extend its investments in LTE cellular-based technology to the connected vehicle environment. A 2015 study conducted by the China Academy of Telecommunication Technology on behalf of the China Ministry of Industry and Information Technology defined general security requirements for C-ITS. Further information regarding China's security development was unavailable to the project team.

2.5 Australia

Australia's C-ITS development has included substantial outreach with the US and EU in exchanging information on requirements, designs, and best practices; and in creating a security framework that will result in implementations with appropriate levels of interoperability between these regions. Australia has been an equal partner in the EU-US Standards Harmonization Working Group (part of the EU-US-Japan ITS Steering Group) that has included development of both technical security standards and security policies.

Security installation is also informed by the in-country regional (that is, the states and territories) autonomy, including each region potentially having their own adaptations to elements of their C-ITS that manifests itself as unique requirements for their SCMS. Australia recognizes the need for different states' implementations to be harmonized, but not necessarily identical. Coordination at a policy level, including

[9] As presented by the Korean delegation to the USDOT at the January 10, 2018 Joint Meeting between USDOT and the Korea Ministry of Land, Infrastructure and Transport, for ITS Cooperation.

the criteria used to determine the system's trustworthiness, is recognized as a requirement. Australia has developed a tailored set of foundational requirements for a national SCMS (as a matter of terminology, they are adopting the EU's preferred CCMS term). These requirements include a nation-wide security solution manifested as a national SCMS. This national SCMS will be available in initial deployments and will be scalable to support national deployments.

Historical precedents also inform Australia's security framework. They have previously developed a PKI security solution for commercial vehicle regulations. Since 1999, Australia has deployed a national PKI-based security structure called Gatekeeper, defined at the commonwealth level and in use in various governmental functions within its states and territories. Its objective has been to provide a safe and secure environment for electronic transactions that were beginning to emerge in that era. During the ensuing years, Gatekeeper became a national framework and was touted as the first such government-wide PKI in the world. More recently it has become owned and maintained by the Commonwealth's Digital Transformation Office, which calls it, "a whole-of-government suite of policies, standards, and procedures that governs the use of PKI in government for the authentication of individuals, organizations, and non-person entities – such as devices, applications or computing components…." The framework is mandatory for agencies using PKI to authenticate their clients through the use of digital keys and certificates issued by Gatekeeper-accredited service providers."[10]

One application family that emerged under the framework was in telematics for heavy vehicles. The National Telematics Framework is a platform for delivery of certain telematics and related intelligent technologies in Australia, including the provisioning of security. It is administered at the commonwealth level (by Transport Certification Australia) and used in various ways by Australia's states and territories. One of the specifications made available through the NTF is the Intelligent Access Program, a certified service that addresses the regulatory access of heavy vehicles to the Australian road network.

"Current IT security policies might set constraints to the publicly developed subsystems. The international developments of the security system for C-ITS are likely to determine the operational constraints in Australia, so these international developments have been taken as guidance in the [Core C-ITS] Concept of Operations. It is noted that the Australian Government's Gatekeeper PKI Framework provided guidance to the PKI approach used for the Intelligent Access Program (IAP), and while not mandatory, should be given consideration with C-ITS also."[11] However, it currently seems unlikely that Gatekeeper will be part of the C-ITS operational solution since it is not sufficiently robust to address the unique technical requirements of a C-ITS operation.

The Australian IAP business model is sustained by truck drivers/fleet owners wanting permissions to be on certain roads as well as wanting to carry larger cargos, which are sometimes defined by weight and sometimes by the number of trailers. The truck drivers/fleet owners pay PKI vendors, who are certified to be part of IAP to gain access to applications, services, as well as permissions. In return, the government - Transport Certification Australia (TCA) – gets access to specific, trusted commercial vehicle systems to collect data to support auditing and enforcement of commercial vehicle regulations.[12] PKI vendors sell the credentials to the truck drivers/fleet owners and then pay the government to be a service provider and get

[10] Australian Government Digital Transformation Office. (December 2015). Gatekeeper Public Key Infrastructure Framework. V 3.1, p. 10.

[11] Austroads Research Report AP-R479-15, "Concept of Operations for Core C-ITS Functions", March 2015

[12] https://tca.gov.au/tca

access to credentials on behalf of the truck drivers/fleet owners. TCA's role is to do the core policy, auditing, and evaluation work including accreditation of the credentials. TCA sets parameters and audits these PKI vendors regularly. To become a vendor, there is a process for certification and recertification.

2.6 Canada

Canada is largely following the US lead as it develops its security solution for CVs. There are six test beds that appear to be currently underway.[13] The tests, which have limited involvement from Transport Canada, are largely run by universities. In the team's outreach to Canadian representatives, there was no unique contribution to SCMS approaches that have been developed.

2.7 Mexico

The USDOT maintains contact with its Mexican counterparts on various transport topics. From our team's discussions, Mexico has not initiated a V2X program at the national level (it does have Electronic Toll Collection installations). There is no research available to the team on how Mexico might view security implementations of a V2X program. While cross-border topics may become an important topic in the future, from the viewpoint of documenting best practices from other regions and countries, there is no contribution from Mexico.

2.8 Best Practices and Takeaways

Takeaways from international solutions are limited to the EU, which has a maturing V2X security system development and deployment effort. The European Commission's trust model concept for multiple roots provides additional redundancy and interoperability. Their multiple root structure allows for more flexibility in expanding and decentralizing operations. Their common policies ensure interoperability among the C-ITS stations (e.g., vehicles or infrastructure stations), which will be enrolled and authorized under different root CAs. Their multiple root concept also addressed coordination through the TLM, CPOC, and the ECTL. The European Commission's trust model has effectively structured audit procedures through the Accredited PKI Auditors. Also, their CP describes a structured process for developing, modifying, and approving policies for certificates. Additionally, the European Commission has developed potential high-level funding models for each role within the trust model, as well as a registration fee structure to sustain the TLM and CPOC.

The European Commission has defined the specific sub-roles within the trust model, many of which can be operated under one entity. The European Commission identifies sub-roles that should be separated with the intention of segregating duties and avoiding conflicts of interest. The separation of sub-roles is based on high level organizational roles.[14] However, the European Commission has not specified a need

[13] http://transportation.ualberta.ca/News%20and%20Events/2013/December/TheCSTandtheFirst ConnectedVehicleTestBedinCanada.aspx

[14] The Structure of the organizational roles defined in the "Security Policy & Governance Framework for Deployment and Operation of European C-ITS" is based off "the ETSI EN 302 637-3 V1.2.2 Intelligent Transport Systems (ITS);

or a way to combine them. For instance, all the Policy Authority sub-roles (certificate, privacy, and security) do not necessarily need to be separated by their functions. To streamline processes, many of these specific sub-roles could be centralized within the SCMS Manager. The European Commission identifies how many entities within a sub-role can exist within the trust model. The number of entities within a sub-role is based on the overarching main organizational roles and their function. For example, the Policy Authority sub-roles within the policy framework role are all single instances, meaning there can only be one of each within the trust model. Another factor the European Commission defines are potential entities that can undertake a sub-role. The Policy Authority sub-roles all have the same entities who can potentially take on this function, therefore they can potentially centralize these sub-roles. These two factors create limitations as to who can take on sub-roles, thus outlining potential centralized roles.

Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service."

Chapter 3. PKI-Specific Ownership, Governance, and Operational Models

This chapter provides a summary of three PKI models: (1) CA/Browser Forum (private sector); (2) US Government Federal PKI (public sector); and (3) European Union Digital Signature Infrastructure (public sector). While the SCMS has a more complex design to protect the privacy of vehicles and their operators, each one of these PKIs is a large-scale, distributed system with its own unique challenges and objectives. Each section analyzes the general system purpose as well as the ownership, governance, operational, and initial deployment models, focusing on the same questions as in Chapter 2 (e.g., approach to funding). This information will be used to identify takeaways and best practices to be leveraged within potential ownership and governance models for the National SCMS.

3.1 CA/Browser (CA/B) Forum[15]

The team selected the CA/B Forum for benchmarking because it is a good example of an industry-deployed PKI policy development body. The CA/B Forum is a collaborative group that was formed by commercial X.509 PKI vendors and the commercial entities that field products that consume PKI products (e.g., web browsers, operating system) after several high-profile security breaches. Browser vendors include Microsoft, Mozilla, Google, and Apple. PKI providers include DigiCert, Entrust, LetsEncrypt, and Comodo.[16]

The CA/B Forum does not control the use of the policy it develops. The decision on whether to trust a specific PKI is left to the product vendors. The mechanism used is a trust list. Each vendor has its own process for determining what roots will be included in their products and how those root trust lists are maintained.

3.1.1 Forum Overview

The CA/B Forum was organized in 2005, as a voluntary group of commercial CAs, vendors of Internet browser software, and suppliers of other applications that use X.509 v.3 digital certificates for SSL/TLS and code signing. CA/B Forum members have worked closely together in defining the guidelines on how to implement best practices as a way of providing heightened security for Internet transactions and creating a more intuitive method of displaying secure sites to Internet users. PKIs that meet the criteria of one or more product vendors are called "publicly trusted."

The forum has a formal charter that details its purpose, membership requirements, policy change process, and voting process. Currently, the US Government is an associate member (non-voting status)

[15] Primary reference was the Bylaws of the CA/Browser Forum Version 1.7 – Adopted effective as of 6 July 2017

[16] https://cabforum.org/members/

but is developing a PKI that is intended to be publicly trusted and, when approved, the US government could apply for voting membership.

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

3.1.2 Comparison to the National SCMS

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

3.1.3 Ecosystem Structure and Internal Organizational Structure

The CA/B Forum organization is described in the by-laws.[17] The CA/B Forum has no corporate or association status. It is simply a group of CAs and browsers which communicate or meet from time to time to discuss matters of common interest relevant to the CA/B Forum's purpose.

The CA/B Forum has a chair and a vice chair, each appointed for a two-year term. The chairs come from voting member organizations. The chair may not serve consecutive terms or be elected to the vice chair position after their term as chair.

The chair appoints a web master to oversee operation of the forum web site and listserv.

There are no other formal structures prescribed. Working groups may be formed with the approval of the chair.

3.1.4 Approach to Oversight and Industry Governance

Most of the voting members of the CA/B Forum are PKI operators. The remainder represent products that consume PKI services. The product vendors control how the policy is applied, and each maintains a separate trust list. Each has different rules and requirements, but all use the CA/B policy as a baseline.

The technical mechanism for trusting a PKI is the trust list. The trust list maintenance is performed through updates to the products (e.g., Microsoft in Windows, Mozilla in Firefox, Apple in iOS, Google in Chrome).

This distributed model allows the CA/B Forum to focus on the development of policies that can achieve an industry consensus, simplifying the CA/B Forum organizational structure and funding requirements.

[17] https://cabforum.org/bylaws/

On the negative side, the distributed approach means that different vendors may not trust the same PKIs, potentially providing unwanted impacts on users when they visit web sites.

3.1.5 Approach to Funding

The costs of operating forum websites or mailing lists will be covered by voluntary contribution from forum members (who may seek voluntary contributions from other members to help defray such costs). Because the forum has no corporate status, it does not maintain funds or banking accounts. Forum members may propose other group activities (e.g., research projects), which they propose to sponsor, that require funding and may seek voluntary contributions from other members for such activities.

All costs associated with participation in CA/B Forum meetings and working groups is funded by the representative's employer.

3.1.6 Approach to Policy Development and Approval

The CA/B Forum's by-laws detail the formal policy approval process based on voting by members.

Generally, policy is developed using a publicly-accessible web site and discussed through a public mailing list. The forum maintains a private web site and private mailing list for sensitive items where discussion on the public mail list could reasonably be detrimental to the implementation of security measures by members.

The forum has working groups that conduct primary development of policies and other documents. Participation is open to members and other interested parties. All initial and final drafts are distributed via the public mail list. Drafts are not considered final until approved by two-thirds of the working group members. Working groups may implement separate listservs, wikis, and web pages for their communications. Any such communications means must follow the rules for public access established by the forum.

Any voting member can call for a ballot on any proposed change to a document. Before moving to a ballot, two additional voting members must endorse the proposal. There will be a formal discussion period of between 7 and 14 days and then votes are cast. The voting members are divided into categories – CA operators and product vendors. For a vote to succeed, two-thirds of the CA operators and half of the product vendors must vote to approve.

3.1.7 Best Practices and Takeaways

The CA/B Forum policy development process is well thought-out and provides an appropriate level of transparency to ensure that the policies properly balance security and cost.

While the distributed oversight and governance model simplifies the CA/B Forum's roles and responsibilities, it also presents the potential for certificates from compliant PKIs to fail because they did not meet a specific vendor requirement that may not be a requirement of other product vendors.

3.2 US Government Federal PKI

The team selected the US Government Federal PKI for benchmarking because it provides a good example of a PKI model with multiple roots and multiple certificate policies.

3.2.1 Overview

The US Government Federal PKI establishes policies and provides oversight and governance to Federal Agency PKIs, such as those for the Department of Defense, Department of Treasury, and Department of State.[18] It also operates a bridge PKI to facilitate trust with externally operated PKIs. Among the PKIs overseen and operated by the Federal PKI are the Federal Bridge Certificate Authority (FBCA) and the Common Trust Framework (Common) PKIs.

The FBCA PKI facilitates trust among PKIs operated by separate entities. The FBCA has two separate roots – one operated at the current security standard (SHA-2) and the other operated as part of a legacy infrastructure to support PKIs that supply certificates to end users who cannot consume the higher security standard. The Common PKI provides a trust anchor for issuing CAs that provide certificates for personal identity validation (PIV) cards issued to Federal employees and contractors.

The Federal PKI consists of the Policy Authority (PA) and the Management Authority (MA) and operates under a charter approved by the US Government Federal Chief Information Officer Council.

There are several commercial PKI bridges that operate in a similar fashion to the Federal PKI. The primary difference is the way they are funded.

3.2.2 Comparison to the SCMS

The Federal PKI performs all of the functions that are expected of the SCMS Manager, except operation of the misbehavior authority. It does policy development, oversight, and enforcement. It also directly manages the roots for the primary PKIs for which it is responsible.

3.2.3 Ecosystem Structure and Internal Organizational Structure

The PA is a board that performs the policy approval, oversight, and governance of the various Federal PKIs.[19] Board voting members are from Federal Agencies. Non-voting members are from the external PKIs that belong to the FBCA, such as CertiPath, SAFE_Bio-Pharma, and the State of Illinois. The PA has established a certificate policy working group to address updates to the certificate policies and a technical working group to advise it on technical matters related to PKI. The PA has established procedures that specify how member PKIs adhere to its policies, auditing and reporting guidance, and how new PKIs can be added to the Federal infrastructure.

[18] https://fpki.idmanagement.gov/

[19] https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/FPKIPA_charter_1.0.0_Final.pdf

Trust among PKIs is established via cross certificates. Cross certificates establish bi-lateral trust between two PKIs. Each root issues the other root a certificate that maps the level of trust that it accepts from the other PKI. The trust is transitive – if A trusts B and B trusts C, then A trusts C.

The MA operates the FBCA and common root CAs. It performs all functions associated with operating roots (e.g., security, issuing certificates to subordinate CAs).

3.2.4 Approach to Oversight and Industry Governance

The PA oversees the creation of policy, the comparison of prospective members to that policy, and the decision on whether to accept an applicant for membership. It also reviews artifacts that member PKIs are required to submit (e.g., periodic audit reports) to maintain member PKIs in good standing as specified in its *Criteria and Methods* document.

In addition to the policy governance, the MA performs periodic scans of the member infrastructure to ensure that infrastructure components are meeting their required availability standards and have the appropriate artifacts properly posted (e.g., certificate revocation lists). The MA provides periodic updates to the PA on discrepancies it finds in these scans.

For a new member, the applicant maps its certificate policy to the appropriate security level(s) in the applicable Federal PKI policy and submits the mapping along with other required documentation to the PA. The PA refers the policy mapping documentation to the certificate policy working group, which reviews the mappings. Any discrepancies are discussed with the submitting organization. This can be an iterative process, continuing until there is agreement on the mapping and the appropriate security level(s) of the applicant's PKI. The documentation is forwarded back to the PA. In parallel, the MA conducts testing of the applicant's PKI artifacts (e.g., example certificates, certificate revocation lists) to ensure conformance with standards. Once all is complete, the PA approves the applicant and the MA and the applicant issue the appropriate cross certificates.

Periodically, current members are required to demonstrate that their PKI has been updated to reflect policy changes that occurred since the last mapping was completed. The process is similar to that for a new applicant but focuses on changes rather than the entire document.

For issuing CAs operated under Common Trust Framework PKIs, the PA reviews and approves the CA's practice statement, which demonstrates how the issuing CA conforms to the Common certificate policy.

Annually, member PKIs and issuing CAs under the Common Trust Framework submit copies of independent compliance audit reports and findings to the PA for review to ensure that the member PKI is being operated as specified by the policies and practice statement.

3.2.5 Approach to Funding

The Federal PKI is funded by a combination of appropriated funds for Federal Agencies and Federal Agency cost reimbursement to the General Services Administration (GSA), which provides the PA secretariat support and operates the MA.

Members that operate their own PKIs fund their operations directly.

Issuing CAs operated under the Common Trust Framework are operated under contract with the agency that receives certificates from the issuing CA and the agency pays (typically on a per card basis) for PKI services.

Commercial bridges are funded by subscriptions paid by the member PKIs. The member PKIs are either companies which operate PKIs for their own use or commercial PKI providers that sell PKI services to others. The bridges are typically aligned with business areas (e.g., Defense, Medical, First Responders.)

3.2.6 Approach to Policy Development and Approval

Any member of the PA may present a change request to one or more of the PA approved documents. The changes are reviewed and discussed at the certificate policy working group. The working group then forwards the final version of the change request to the PA, which reviews and votes whether to approve.

3.2.7 Best Practices and Takeaways

The policy development and approval process used by the Federal PKI is a standard practice for a government policy body. It provides significant opportunity for participants to have their voices heard on both the substance of the change and the decision to approve it for implementation. It lacks the public discussion and transparency that will be expected of a PKI that impacts the majority of Americans.

The mapping of member PKI certificate policies to the FBCA CP would serve as a good example if the SCMS will have multiple roots operated by separate entities. If the SCMS will have a single PKI operated under a single root managed by the SCMS Manager, the Federal PKI method of performing compliance analysis would serve as an appropriate model.

The Federal PKI requires member PKIs (Federal and external) to undergo annual independent compliance audits and provide an annual update, which includes changes to policies and practices and results of the annual audits. It also requires that members provide real time information concerning security incidents and status/resolution of those incidents. The MA conducts periodic testing of all member PKI artifacts (e.g., certificates, revocation lists) to ensure interoperability and conformance to standards. The MA also monitors public facing repositories for both currency of information and availability.

Although technically feasible, the use of cross certificates has proven to be a brittle trust mechanism and would not be recommended for the SCMS.

3.3 EU Digital Signature Infrastructure

The team selected the EU Digital Signature Infrastructure because it provides a good example of a PKI model with multiple roots and multiple certificate policies. Additionally, the EU Digital Signature Infrastructure is a good comparison to the US Government Federal PKI regarding oversight and governance.

3.3.1 Overview

In 1993, the European Commission issued the Electronic Digital Signature Directive (EDSD). It established the initial requirements for member nations to harmonize the use of digital signature technologies to enhance business and commerce (e.g., electronic identification and trust services for electronic transactions in the European Single Market). The Electronic Identification and Trust Services Regulation (eIDAS) replaced the EDSD. It provides a consistent legal framework for recognition of electronic signatures and identities across the EU.[20]

3.3.2 Comparison to the SCMS

The eIDAS infrastructure consists of a policy development and oversight mechanism and uses trust lists to provide consuming applications with a current list of Trusted Service Providers (TSPs). Trust lists are maintained by national level authorities (e.g., Ministry of Interior of the Czech Republic, Danish Agency for Digitisation, National Security Cabinet of Portugal) within each member country. While individual nations maintain the trust lists, all are consistent with the EU standards. The infrastructure has responsibility for the implementation of electronic signatures in applications and software and for the security and interoperability of the PKIs implemented by TSPs.

3.3.3 Ecosystem Structure and Internal Organizational Structure

The eIDAS uses the European Telecommunications Standards Institute (ETSI) as the body for the development of standards for electronic signature and TSPs. The ETSI has established the Electronic Signatures and Infrastructure (ESI) to facilitate the collaboration of all interested parties and stakeholders in the marketplace including vendors, operators, user organizations, and other standards bodies.[21] Using the standards developed by ETSI ESI, each nation maintains a trust list of qualified TSPs, which issue certificates to individuals.[22] Applications that make use of digital signatures import those trust lists as needed.

3.3.4 Approach to Oversight and Industry Governance

The oversight of TSPs is vested in the member countries, which must supervise qualified TSPs established within a nation's boundaries. Each nation performs validation of qualified TSP and includes the qualified TSPs in a trust list published by the nation. National organizations that perform the oversight conform to eIDAS standards for qualifying TSPs.

[20] https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/overview-of-electronic-signature-law-in-the-EU.pdf

[21] https://portal.etsi.org/TBSiteMap/ESI/ESIMissionStatement.aspx

[22] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0005

3.3.5 Approach to Funding

ETSI funding[23] comes from various sources including:

- Annual membership fees – provide the majority of income. Fees are calculated according to the size of the member company or organization but reduced fees are charged for user associations, academic and research bodies, and small businesses.
- European Union – the EC and the European Free Trade Association (EFTA) issue mandates and provide funding for ETSI to develop specific standards, particularly Harmonised Standards, or for other related work. This is often in support of European legislation. They also provide general funding in support of ETSI's activities as a European Standards Organization (ESO), together this funding amounts to 15 to 20 percent of the budget.
- Income from 'commercial' activities – including sales of standards, fees for events (such as interoperability testing events), and services to outside organizations.
- Contributions from partner organizations – e.g., services performed on behalf of collaborative activities, such as the Third Generation Partnership Project (3GPP™).

National organizations that provide oversight and governance of TSPs are funded through the national budget process.

3.3.6 Approach to Policy Development and Approval

ETSI has different processes for different types of standards. Most of the standards related to the eIDAS are classified as "European Standards." The approval process for a European Standard[24] is:

1) After the appropriate Technical Committee has approved the draft, the ETSI Secretariat makes the document available to the National Standards Organizations (NSO).
2) The NSOs carry out the Public Enquiry (PE). This involves consultation and submission of the national position (the "vote") on the standard.
3) If this vote is successful, and if no substantial comments are received from this consultation, the ETSI Secretariat finalizes the draft and publishes the standard.
4) Any technical comments received during PE are considered by the Technical Committee, which may revise the draft and resubmit it to the Secretariat.
5) If the changes are significant, the Secretariat may initiate another PE; otherwise the draft will be presented directly to a second vote.
6) After a successful vote, the Secretariat publishes the standard.

[23] http://www.etsi.org/about/what-we-are/funding

[24] http://www.etsi.org/standards/how-does-etsi-make-standards/approval-processes

3.3.7 Best Practices and Takeaways

The diverse nature of funding that supports eIDAS infrastructure provides several potential funding streams. While not all will be relevant to the SCMS Manager, some of them may point to potential methods of funding the SCMS Manager, depending on the model ultimately selected.

Chapter 4. Other Ownership, Governance, and Operational Models in Industries and Ecosystems Analogous to the National SCMS

This section focuses on analyzing the ownership, governance, operational, and initial deployment models of other policy development and governance bodies. The first subsection discusses high-level approaches to ownership, policy development, and governance across multiple industries and domains to gain perspective on the different governance needs and methods. The second subsection dives into brief case studies of organizations that we believe exhibit best practices and/or lessons learned that could help the team and stakeholders develop an efficient and effective ownership, governance, operational, and initial deployment model.

4.1 Ownership, Governance, Operational, and Initial Deployment Models of Policy Development and Governance Bodies Within Other Industries and Domains

In conducting research on other industries and their policy and governance frameworks, the team reviewed multiple previous reports, such as the USDOT's *Organizational and Operational Models for the SCMS: Industry Governance Models, Privacy Analysis, and Cost Updates* report and the Vehicle Infrastructure Integration Consortium (VIIC) *VIIC SCMS Manager Study*, that have evaluated governance models and deployment approaches in other industries. These projects had already reviewed select industries, such as the payment card industry, utilities, and healthcare. The reports also conduct deeper analysis of organizations such as the Internet Corporation for Assigned Names and Numbers (ICANN), Payment Card Industry Security Standards Council (PCI SSC), and The Joint Commission, and examine their relevance to a potential SCMS ecosystem and governance entity (i.e., the SCMS Manager). This report will also explore these organizations to a lesser extent and will focus on specific best practices and lessons learned as relevant to the most recent understanding of the V2X ecosystem and SCMS concept. In addition to existing reports and analyses, the team reviewed additional industries and their governance frameworks. Table 3 provides a scan of multiple industries and domains; examples of associated policy and governance organizations; and brief descriptions of the policy, standards, and governance challenges that these organizations aim to solve.

Table 3. Scan of Select Industry and Domain Policy Development and Governance Models

Industry/ Domain	Example Policy and/or Governance Organization	Policy, Standards, and Requirements Development Responsibility and Authority	Governance Responsibility and Authority
Automotive	Vehicle Information and Communication System (VICS)	Organization originally sponsored by the Japanese National Police Association, Ministry of Construction, and the Ministry of Posts and Telecommunication to develop a national system for the provision of traffic information. Developed the early guiding policies for the VICS system through a collaboration between the sponsoring ministries and the participating organizations (car makers, equipment manufacturers, academia and other public and private organizations and institutes)	Governed by a combination of ministry policies, usually jointly developed by the ministries associated with or responsible for a given technical area and the industries who are responsible for implementing the system. These policies guide the establishment of P3s such as the VICS center. The companies that provide staff for the center also sit on the management board and provide the overall governance implemented jointly between the government ministries who have established the operation and the private companies, institutes, and universities that operate it. The cooperative nature of Japanese society, and the general level of trust between the various parties facilitates the effectiveness of this approach
	AUTomotive Open System ARchitecture (AUTOSAR)	Develop standards for automotive software architecture through an alliance of 230 OEM manufacturers, Tier 1 automotive suppliers, semiconductor manufacturers, software suppliers, tool suppliers, consulting firms, and universities	None
	GENIVI Alliance	Develop and drive the broad adoption of open source, In-Vehicle Infotainment (IVI) software and providing open technology for the connected car through an	Manages a members-only GENIVI Compliance program

Industry/ Domain	Example Policy and/or Governance Organization	Policy, Standards, and Requirements Development Responsibility and Authority	Governance Responsibility and Authority
		alliance of OEMs, Tier 1s, middleware suppliers, hardware suppliers, and semiconductor manufacturers	
Aviation	International Civil Aviation Organization (ICAO)	UN specialized agency, established by states in 1944 to manage the administration and governance of the Convention on International Civil Aviation. Develop and reach consensus on international civil aviation Standards and Recommended Practices (SARPs) and policies in support of a safe, efficient, secure, economically sustainable, and environmentally responsible civil aviation sector through 192 member states and industry groups	ICAO's Universal Security Audit Program (USAP) conducts documentation-based, oversight-focused, and compliance-focused audits for member states
	NAV CANADA	NAV CANADA develops air navigation system policies through a market driven approach, collaboratively developed and enforced via the Advisory Committee, the Board of Directors, and the executive management team	NAV CANADA manages air traffic operations but does not have a governance or enforcement role. Instead, NAV CANADA is governed by the Aeronautics Act and the Canadian Aviation Regulations (CARs). Audits are provided internally and externally by third parties
Banking	Payment Card Industry Security Standards Council (PCI SSC)	Sets industry-wide security standards through collaboration and consensus among members, and providing education and training to the larger industry. Developed and maintains the Data Security Standard, PIN Transaction Security Requirements, and Payment Application Data Security Standard	Enforcement of the standards through compliance programs, and imposing of non-compliance penalties such as fines, is the responsibility of individual payment card brands. Penalties for non-compliance with any required standards would be dictated by the voluntary agreement

Industry/ Domain	Example Policy and/or Governance Organization	Policy, Standards, and Requirements Development Responsibility and Authority	Governance Responsibility and Authority
			between the payment card brands and the merchants and service providers under contract
Manufacturing	Responsible Business Alliance (RBA)	Works with its more than 110 members and their Tier 1 suppliers to develop supply chain capabilities to assess and address social and environmental risks as they relate to its Code of Conduct	Holds members accountable to their Code of Conduct commitment via a range of mandatory accountability and assessment means, including self-assessment questionnaires, audits, and corrective actions where necessary. RBA applicant members have two years from the date they join the RBA to conform to the membership requirements
	SEMATECH	Originally created as a partnership between the United States Government and 14 US-based semiconductor manufacturers to solve common manufacturing problems and regain competitiveness for the US semiconductor industry that had been surpassed by Japanese industry in the mid-1980s. Now, an international consortium that performs research and development to advance chip manufacturing	None
Internet	Internet Corporation for Assigned Names	Originally established by the Federal government, through a proposed rulemaking to privatize the management of Internet names and addresses allowing for the development of competition and facilitating global participation in Internet management	Responsible for coordinating the maintenance and procedures of several databases related to the namespaces of

Industry/ Domain	Example Policy and/or Governance Organization	Policy, Standards, and Requirements Development Responsibility and Authority	Governance Responsibility and Authority
	and Numbers (ICANN)	as well as address issues relating to DNS management	the Internet, ensuring the network's stable and secure operation
Healthcare	The Joint Commission	Develop standards with input from health care professionals, providers, subject matter experts, consumers, and government agencies (including the Centers for Medicare & Medicaid Services). Standards are informed by scientific literature and expert consensus and reviewed by the Board of Commissioners	Accredits more than 21,000 US health care organizations and programs. The international branch accredits medical services from around the world. A majority of US state governments recognize Joint Commission accreditation as a condition of licensure for the receipt of Medicaid and Medicare reimbursements

4.2 Specific Organization Analyses and Brief Use Cases

4.2.1 Vehicle Information and Communications System (VICS)

Overview and Initial Deployment: The Vehicle Information and Communications System (VICS) is a national system for the provision of traffic information (including road work, accidents, congestion, and travel times) to vehicle-based terminals. VICS was launched in selected regions of Japan in early 1996 and has achieved a fairly high level of deployment density across the entire country over the past 20 years. A key driver of the success of VICS has been the cooperation of private industry in the development, marketing, and sale of VICS-compliant terminal equipment, most of which is implemented as a feature in conventional in-vehicle navigation systems.

VICS was established on the confluence of several core elements in the ecosystem:

1) A road traffic data collection system had been established through the parallel efforts of several ministries. The National Police Association (NPA) had developed mechanisms for the collection of congestion, accident, and road work information for surface streets.
2) The Ministry of Construction (MOC), which had developed the Road/Automobile Communication System (RACS). RACS was a system of roadside beacons to provide communications with passing vehicles.
3) The Ministry of Posts and Telecommunication (MPT) who had worked with the NPA to establish the Advanced Mobile Traffic Information & Communication System (AMTICS).
4) By the early 1990s about 400,000 in-vehicle navigation systems had been sold, and this production rate increased rapidly.

In October 1991, the VICS Promotion Council was formed. This group, sponsored by the three ministries identified above, included about 200 member organizations and companies, and was focused on merging these earlier programs into a single cohesive effort to create a nationwide traffic information collection and distribution system. The organization of the Promotion Council is provided in Figure 5.[25]

[25] Toward Realization of VICS – Vehicle Information and Communications Kaoru Tamura, Makoto Hirayama, VICS Promotion Council, IEEE - IEE Vehicle Navigation & Information Systems Conference, Ottawa - VNIS © 1993 IEEE

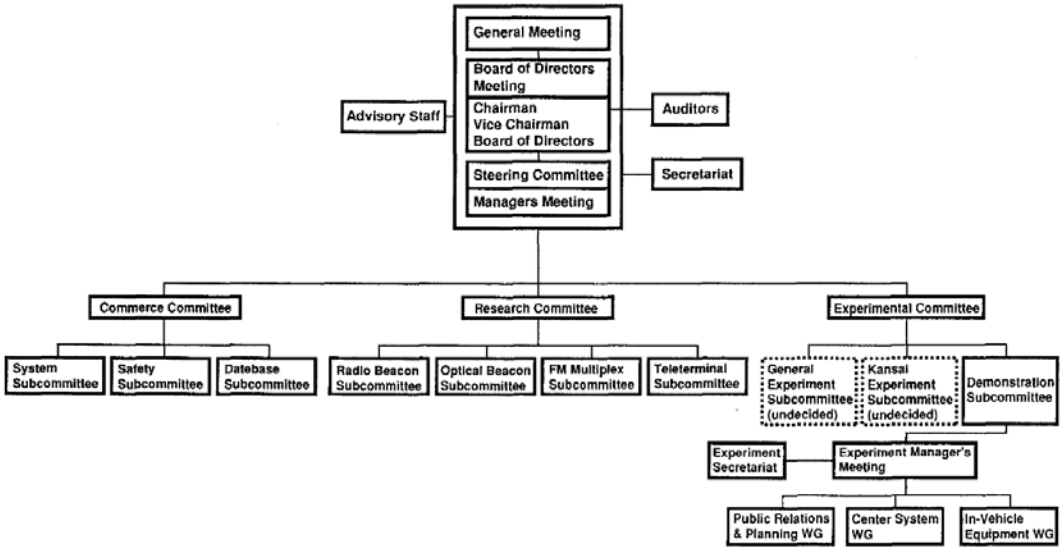

Figure 5. Organization of the VICS Promotion Council

The VICS Promotion Council developed the early guiding policies for the VICS system through a collaboration between the sponsoring ministries and the participating organizations (including car makers, equipment manufacturers, academia, and other public and private organizations and institutes).

In 1995, the NPA, MoC, and MPT established the VICS center in Tokyo. The primary functions of the center are gathering, processing, and editing road traffic information, and providing this data through communication and broadcasting media. The VICS center also performs surveillance and research on road traffic information systems, manages the intellectual property rights related to the road traffic information system, and organizes contracts with various suppliers, vendors and service providers. The VICS center is generally staffed with participants seconded from the various companies that make up the overall VICS ecosystem.[26] The core ministries have evolved over the past 20 years. Today the VICS center is operated by the NPA, the Ministry of Internal Affairs and Communications (MIAC), and the Ministry of Land, Infrastructure and Transport (MLIT).

In parallel with the establishment of the VICS center, a large number of equipment suppliers developed and sold various types of terminal equipment. While the original VICS system design included three levels of terminals, ranging from a simple text display to a detailed moving map data overlay system, the vast majority of terminals produced have been the more sophisticated systems integrated with moving map navigation systems, which are ubiquitous in Japanese vehicles.

It is important to note that a key element of the VICS strategy was to rely on competition and free enterprise, within constraints imposed by the overall VICS management. For example:

[26] In Japan, it is typical for employees of companies to be assigned to other companies, or operations, so the VICS center is staffed by numerous employees of the companies that comprise the overall VICS ecosystem. For example, car makers, suppliers, research institutes and academia all contribute people to the VICS center.

> "The costs associated with VICS administration are, in principle, to be borne by those who use and benefit from VICS' services. However, because it is drivers in general who will benefit from VICS' services, it would be extremely difficult to implement a fee-collecting system based on this principle. Furthermore, as the drivers who use the information provided by VICS trigger an effect that benefits all drivers, financing VICS by collecting fees for this information would be contrary to the principle of the equitable bearing of expenses among all beneficiaries.
>
> It was therefore decided to finance the administration of VICS primarily by collecting the appropriate fees when, in the course of VICS implementation, an associated project is launched or expanded. ***Specifically, this entails funding VICS with suitable fees collected from the corporations that will manufacture and market the onboard devices used to receive VICS information and build the infrastructure used by VICS."***[27]

VICS became operational in April 1996, with services available primarily in Tokyo. VICS information became increasingly available following this launch and, within about a year, traffic information services were available nationwide. Figure 6 illustrates the overall system:[28]

Figure 6. VICS' Traffic Information Services System

Comparison to the SCMS: VICS is not a security management system, and thus there is very little functional similarity between the VICS center and the SCMS. There is, however, substantial similarity

[27] The Strategy and Deployment Plan for VICS, by Shinsaku Yamada, Vehicle Information and Communication System Center, Published in the IEEE Communications Magazine • October 1996

[28] VICS Pamphlet, VICS Center, 2013

between these two operations in terms of participation and the constraints under which the participants carry out their work. For example:

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

Internal Organizational Structure: The current organizational structure of the VICS center is provided below. As noted above, many, if not all, of the staff for the VICS center are employees of the companies that make up the VICS ecosystem.

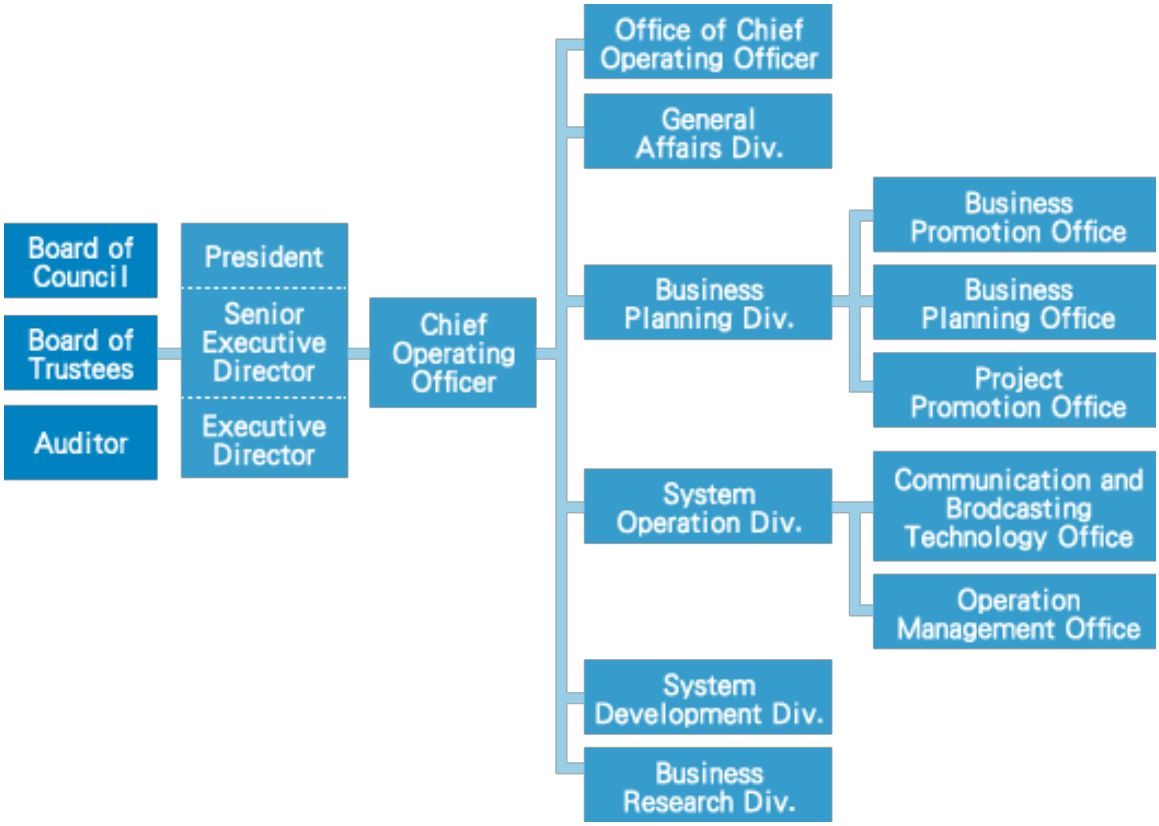

Figure 7. VICS Organizational Structure.[29]

Oversight and Industry Governance: The VICS system is governed by a combination of ministry policies, usually jointly developed by the ministries associated with or responsible for a given technical area (e.g., in the case of VICS, road traffic management), and the industries who are responsible for

[29] "VICS Center Organizational Chart" as presented on the Introduction of VICS center webpage. http://www.vics.or.jp/en/about/index.html. VICS website, accessed January 2018.

implementing the system. These policies then guide the establishment of public-private partnerships, such as the VICS center. The companies that provide staff for the center also sit on the management board, and thus provide the overall governance, which is implemented jointly between the government ministries who have established the operation and the private companies, institutes, and universities that operate it. The cooperative nature of Japanese society, and the general level of trust between the various parties, facilitates the effectiveness of this approach. This is outlined in the Figure 8.[30]

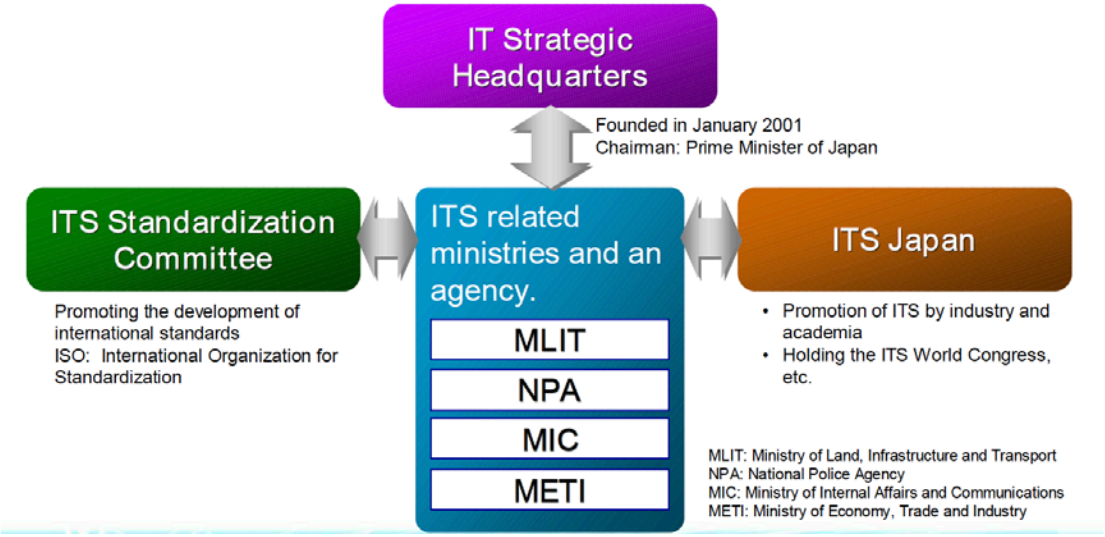

Figure 8. VICS Partnership Structure

Once established, this approach requires relatively limited oversight because generally all of the participants follow the plan, and when things go awry the combined public-private partnership works cooperatively to resolve any problems.

Policy Development and Approval: It appears that policies are developed collaboratively between the ministries responsible for VICS, and the companies that manufacture and sell VICS equipment. This was especially the case in the formative years of the system. For example, as described by Tamura:[31]

> "The VICS Promotion Council was inaugurated in October 1991 with over 200 corporations and organizations participating including most members of the AMTICS Practical Promotion Council and the RACS Practical Promotion Council, which had previously been disbanded to make way for VICS. VICS Promotion Council Review Organization:

[30] ITS Policy in Japan and Smartway, by Mitsuo Arino, ITS Policy and Program Office, Road Bureau, Ministry of Land, Infrastructure and Transport, Government of Japan, October 2007

[31] Toward Realization of VICS – Vehicle Information and Communications Kaoru Tamura, Makoto Hirayama, VICS Promotion Council, IEEE - IEE Vehicle Navigation & Information Systems Conference, Ottawa - VNIS © 1993 IEEE

> The VICS Promotion Council is an organization, which currently has 207 members from the private sector (including eight members from the US and Europe) origin and receives support from the government sector and academic sector."

Japan enjoys a unique level of cooperation between the government and industry. From a policy standpoint, as noted above under Governance development perspective, the government generally sponsors policy development activities, and develops long-range planning documents that government policy developers and industry planners both use to guide their efforts. An example of this is the sequence of policy efforts that eventually led to, among other systems, VICS. This process was summarized by Hideo Tokuyama, and is partially excerpted below:[32]

> "In August 1994, Japan created the Advanced Information and Telecommunications Society Promotion Headquarters, headed by the Japanese prime minister. In 1995, the Japanese government released its "Basic Guidelines on the Promotion of an Advanced Information and Telecommunications Society." These guidelines established a goal to promptly develop a high-performance information and telecommunications infrastructure to accelerate and advance the development of a society in which information and knowledge is freely generated, circulated, and shared. Under these guidelines, six fields were placed under the leadership of the central government. ITS was one of these six fields.
>
> Based on the above "Basic Guidelines," the Interministerial Council of five ITS-related ministries and agencies the Ministry of Transport, Ministry of Construction, Ministry of Posts and Telecommunications, Ministry of International Trade and Industry, and National Police Agency produced "Basic Government Guidelines of Advanced Information and Communications in the Fields of Roads, Traffic and Vehicles." These guidelines, published in August 1995, contain 11 policies for promoting ITS research and development and integrating individual projects into one coherent ITS program. These policies include development of a system architecture, research and development (R & D), standardization and international cooperation, and so on. The Interministerial Council works in cooperation with the national and international organizations -- such as the Vehicle, Road, and Traffic Intelligence Society (VERTIS) -- and supports a variety of activities, including the ITS World Congress in Yokohama in November 1995.
>
> By approving nine ITS areas of development, the government has officially defined the future direction of ITS in Japan. The nine areas of development include navigation systems, automatic fee collection, safe driving efforts, optimization of traffic management, road management methods, public transit, commercial vehicle operations, programs for pedestrians, and emergency vehicle operations."

One benefit of this approach is that the industry can then plan and develop their products with reasonable confidence that they understand the longer-term policies and the resulting support in terms of legislation and government funding. As a result, they are then generally motivated to independently develop products that will take advantage of the market that is created by these policies and programs.

[32] Intelligent Transportation Systems in Japan, by Hideo Tokuyama, FHWA Public Roads, Issue No: Vol. 60 No. 2, Fall 1996

Interestingly, there is not a great deal of assurance built into this process. There is, for example, no certainty that every participant will do as they have promised, but, generally in Japan, organizations do not change their minds once a decision has been made and, as a result, while there is no formal assurance, all of the participants operate with strong confidence.

Funding: Initial funding of the VICS center (About $US 20 million) was established through donations from the participating companies. Most of the infrastructure had already been established by the various ministries who had been carrying out related projects that were ultimately merged to form VICS. Ongoing funding for the center is generally obtained from per-unit fees collected from the equipment manufacturers. While the specific details of how these fees are levied and collected are unclear, conceptually, this appears to operate like a license fee. In exchange for bearing the VICS logo, which attests to some level of VICS certification, the manufacturer pays a per unit fee to the VICS center to maintain and operate the center so that the subject equipment will have data to provide its value to the end user.

Best Practices and Takeaways: Trust and cooperation between the government and the industry companies, and among the private business entities, are essential for the VICS governance model to work. Japan is a small country with a homogenous culture and deeply subscribed beliefs to collectively contribute and even sacrifice for the benefit of the society. These factors may have played a role in the success of this governance model.

4.2.2 Automotive Open System Architecture (AUTOSAR)

Overview and Initial Deployment: AUTOSAR is a worldwide development partnership of vehicle manufacturers, suppliers, service providers and companies from the automotive electronics, semiconductor, and software industry. The partnership established a de-facto open industry standard for an automotive software architecture. It serves as a basic infrastructure for the management of functions within both future applications and standard software modules. The AUTOSAR development partnership was formed in July 2003 by BMW, Bosch, Continental, DaimlerChrysler, Siemens VDO, and Volkswagen. Goals include the scalability to different vehicle and platform variants, transferability of software, the consideration of availability and safety requirements, a collaboration between various partners, sustainable utilization of natural resources, and maintainability throughout the whole product life cycle. Since 2003, AUTOSAR has provided four major releases of the standardized automotive software architecture and one release of Acceptance Tests.[33]

The work of AUTOSAR can be divided into three phases:

- Phase I (2004-2006): Basic development of the standard
- Phase II (2007-2009): Extension of the standard in terms of architecture and methodology
- Phase III (2010-2013): Maintenance and selected improvements.

In 2013, the AUTOSAR consortium entered a continuous working mode to maintain the standard and provide selected improvements.

[33] https://www.autosar.org; https://www.engineersgarage.com/articles/autosar-automotive-open-systems-architecture

Since 2017, the consortium has been working on an Adaptive Platform which implements the AUTOSAR Runtime for Adaptive Applications (ARA).

Comparison to the SCMS: AUTOSAR is an alliance/consortium of many organizations that have an interest in vehicles' electronic controls, which include the OEMs, Tier 1 suppliers, semiconductor and tool/device manufacturers, researchers, developers, and consultants. SCMS Manager governance could involve a broad spectrum of organizations in the connected vehicle space. An alliance or consortium type of governance is possible. Funding of the SCMS Manager could also come, at least partially, from the fees of the products, services, and support that the SCMS Manager provides. The standards and policy development and approval mechanism within the SCMS Manager could also be similar to the self-governed AUTOSAR, driven by the market and the participants of the consortium.

Ecosystem Structure: The AUTOSAR partnership is an alliance of OEM manufacturers, Tier 1 automotive suppliers, semiconductor manufacturers, software suppliers, tool suppliers, consulting firms, universities, and others. There are four levels of membership within AUTOSAR. The contribution of partners varies depending on the type of partnership:

- Core Partners
- Premium Partners
- Associate Partners
- Development Partners.

Core Partners include the founding partners: BMW, Bosch, Continental, Daimler AG, Ford, General Motors, PSA Peugeot Citroën, Toyota, and Volkswagen. These companies are responsible for organization, administration, and control of the AUTOSAR development partnership. Within this core, the Executive Board defines the overall strategy and roadmap. The Steering Committee manages day-to-day non-technical operations and admission of partners, public relations, and contractual issues. Premium and development members contribute to work packages coordinated and monitored by the Project Leader Team established by the Core Partners. Development Partnership provides an opportunity for small companies and start-ups to develop software and products. Associate Partners make use of the standards while attendees collaborate with Core, Premium, and Development Partners to define the AUTOSAR standards.

As of December 2017, about 230 companies participate in the AUTOSAR development partnership.

Internal Organizational Structure

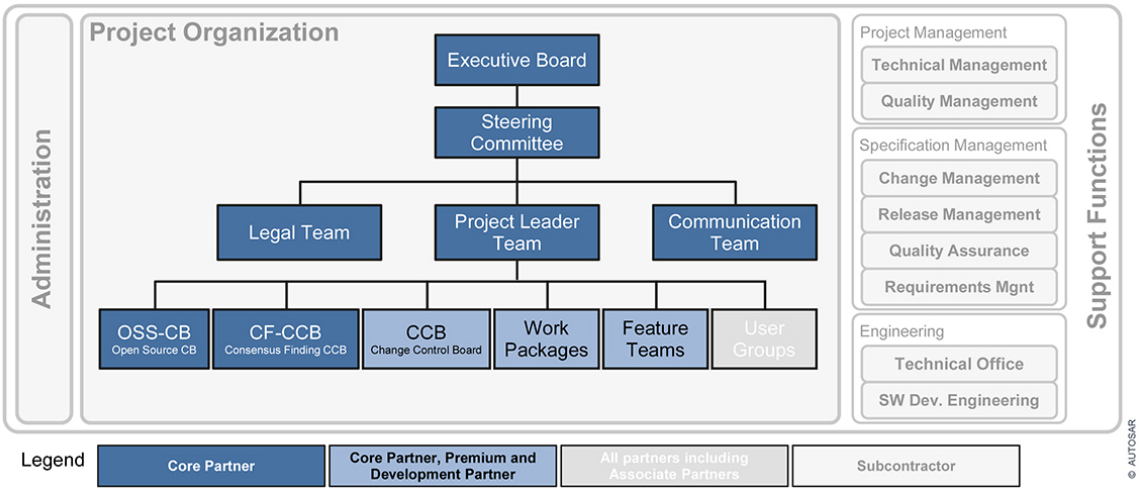

Figure 9. AUTOSAR Organizational Structure

The Executive Board focuses on the following:

- Decides on the overall strategy and roadmap of the AUTOSAR partnership
- Takes office of organizational and administrative control, such as the appointment and revocation of a Chairman, a Deputy Chairman, and a Project Leader Team Speaker of the AUTOSAR development cooperation
- Meets typically once a year
- Members are representatives of the Core Partners at executive management level.

The Steering Committee focuses on the following:

- Manages the admission of partners
- Manages the public relations
- Defines external information (e.g., web-release, clearance)
- Manages the strategy of AUTOSAR
- Recommends changes to the development agreement
- Recommends changes to the annual contributions to the partners
- Admits Premium Partners, Associate Partners, Development Partners, and Attendees
- Meets typically every six weeks.

The Legal Team focuses on the following:

- Legal issues regarding the AUTOSAR partnership such as the AUTOSAR development agreement.
- Meets on demand
- Members are representatives of the Core Partners.

The Project Leader Team focuses on the following:

- Projects plans, financial plans, and budgets within the budget framework
- Rules of procedures and establishment of working groups
- Gives technical information throughout the AUTOSAR development cooperation
- Decides on technical questions related to the AUTOSAR development
- Meets typically every six weeks
- Members are representatives of the Core Partners at project management level.

The Communication Team focuses on the following:

- Manages internal and external communications
- Is responsible for press releases
- Maintenance of the website
- AUTOSAR boilerplates
- Coordinates participation at congresses
- Manages the communication strategy
- Organizes AUTOSAR conferences.

Work Packages are working groups focusing on the following:

- Specify the AUTOSAR Runtime Environment to provide inter- and intra-electronic control unit communication across all nodes of a vehicle network
- Define standardized interfaces across the different vehicle domains
- Define requirements and analysis of existing solutions in the area of basic software modules and automotive operating systems
- Define methodology and data exchange formats for describing necessary elements of a vehicle's electrical/electronic system architecture
- Members are Core, Premium, and Development Partners as well as Attendees which represent the extensive knowledge and experience of the partnership from the various domains.

Feature Teams are working groups focusing on the following:

- Specify the AUTOSAR Runtime for Adaptive Applications
- Define the application programming interface and service interfaces of the functional cluster
- Develop, test, and integrate the AUTOSAR software implementation
- Core, Premium, and Development Partners as well as Attendees staff the Feature Teams. They represent the extensive knowledge and experience of the partnership from the various domains

AUTOSAR User Groups:

- Work on a particular topic based on already released AUTOSAR documents
- The topic is of general relevance for the AUTOSAR community

- Members are Core, Premium, Development, and Associate Partners as well as Attendees

External User Groups:

- The linked External User Groups consist of AUTOSAR partners only, but are not administered by AUTOSAR. They focus on the exploitation (e.g., penetration testing) of the AUTOSAR standard.

The Support Functions focus on the following:

- Organizational and administrative support of AUTOSAR
- Primary contact for all information requests from the public, partnership applications, etc.
- Technical support of all AUTOSAR standards
- Process support for technological, quality, specification, and engineering management.

The AUTOSAR Chairman is in charge of internal affairs and is supported by the Deputy Chairman. Both are members of the AUTOSAR Steering Committee. They are appointed for a nine-month term.

The AUTOSAR Spokesperson focuses exclusively on the external representation of the AUTOSAR development partnership (e.g., gives interviews for press and media, and promotes AUTOSAR on panels).

Oversight and Industry Governance: The consortium has four partnership levels. Core Partners include the founding partners, BMW, Bosch, Continental, Daimler AG, Ford, General Motors, PSA Peugeot Citroën, Toyota and Volkswagen. These companies are responsible for organization, administration, and control of the AUTOSAR development partnership. Within this core, the Executive Board defines the overall strategy and roadmap. There does not seem to be a deliberate certification or accreditation scheme. The consortium governs from within to ensure standards are properly disseminated. Suppliers must adhere to standards when providing services to the OEMs to continue to conduct business.

Policy Development and Approval: The industry standards are developed collectively as an alliance among all members with the core members having the executive authority.

Funding: It is funded by membership fees paid by various levels of members and the fees for AUTOSAR products, services, and support.

Best Practices and Takeaways: The four levels of membership and non-membership attendees ensured that the oversight and internal governance structures positively reinforce operational efficiency and a projectized internal organization structure. Each member is clear in its roles and responsibilities, each member chooses what level of authority they want to have in determining policies and standards based on their own business needs and interests.

4.2.3 GENIVI Alliance

Overview and Initial Deployment: The **GENIVI Alliance** is a non-profit automotive industry alliance to drive the broad adoption of open source In-Vehicle Infotainment (IVI) software and provides open

technology for the connected car. The GENIVI Alliance was founded on March 2, 2009, by BMW Group, Delphi, GM, Intel, Magneti-Marelli, PSA Peugeot Citroen, Visteon, and Wind River Systems.[34]

Having introduced Linux and open source software approaches to the automotive software ecosystem, GENIVI provides OEMs and their suppliers new and more efficient methods of producing car software. GENIVI focuses on delivering a GENIVI Development Platform (GDP) that equips both automotive and non-automotive developers to rapidly prototype new, innovative solutions in an automotive, embedded Linux context. Its software architecture consists of functional requirements and the software components that implement them. The software interfaces of GENIVI software components are defined using Franca IDL. Based on this formally-defined interface description language, integration with other platforms and standards can be established.[35] This allows the interoperability of GENIVI systems and non-GENIVI systems. (e.g., an integration with the AUTOSAR standard was developed in 2014). The GENIVI Alliance defines and maintains reference baselines. Those baselines are public open source software platforms listed as part of the GENIVI open source software projects.

Comparison to the SCMS: Comparison to the SCMS is also similar to that with AUTOSAR. The SCMS Manager governance could involve a broad spectrum of organizations in the connected vehicle space. An alliance or consortium type of governance is possible and may be expected by the stakeholders. After the initial set-up, the ongoing operational funding of the SCMS could also come, at least partially, from the fees of the products, services, and support that the SCMS Manager provides. The standards and policy development and approval mechanism within the SCMS Manager could be similar to the self-governed GENIVI Alliance and AUTOSAR, driven by the market and the participants of the consortium, although public interest may still need to be represented through the involvement of the Federal government.

Ecosystem Structure: The alliance has built a community where automotive experts and thought leaders from related industries (e.g., content providers, mobility) can collaborate to produce adoptable standards and open source code. These collaborations are based on industry trends that require collaborative development of solutions for increased functionality in automobiles. GENIVI has become a community where ecosystems outside of the automotive industry can meet and leverage the global automaker and supplier network in the GENIVI membership.

Internal Organizational Structure: GENIVI is similar to AUTOSAR. Both are non-profit private automotive-industry-led alliances consisting of members of various levels with respective authorities and membership fee requirements. **Both Alliances have a projectized organizational structures**. GENIVI has four levels of membership: funding charter, charter, core, and associate members.

The GENIVI structure contains the following:

- Board of directors (funding members, elected from core members)
- Project management office (PMO)
- System architecture team
- Expert groups
- GENIVI open source software project.

[34] https://www.genivi.org

[35] https://www.cnx-software.com/2011/08/19/what-is-genivi; https://www.crunchbase.com/organization/genivi-alliance

The board consists of founding charter and charter members, and a small number of elected core members. Each of the Expert Groups is led by an Automotive OEM and supported by a Tier 1 supplier.

Oversight and Industry Governance: It is a self-governing organization with authority concentrated on the Funding charter and Charter members. GENIVI manages a members-only GENIVI Compliance program based on the GENIVI Platform Compliance Specification, which is released twice annually to GENIVI members. The program offers OEMs a list of compliant offerings to simplify the vendor selection process. It also ensures products from suppliers meet GENIVI requirements for supply chain quality and adhere to standard application programming interfaces. GENIVI delivers an essential, efficient, and cost-saving development approach. This approach, grounded in open source software, has resulted in the rapid deployment of non-competitive IVI and connected car software for today's vehicles.

Policy Development and Approval: All members can submit policy changes or new policies. The board members meet twice a year and make the final decisions.

Funding: It is completely funded by the membership fees and fees for its products and services.

Best Practices and Takeaways: These are similar to AUTOSAR.

4.2.4 International Civil Aviation Organization (ICAO)

Overview and Initial Deployment: The International Civil Aviation Organization (ICAO) is a UN specialized agency, established by states in 1944 to manage the administration and governance of the Convention on International Civil Aviation (Chicago Convention). ICAO works with the Convention's 192 member states and industry groups to reach consensus on international civil aviation Standards and Recommended Practices (SARPs) and policies in support of a safe, efficient, secure, economically sustainable, and environmentally responsible civil aviation sector. These SARPs and policies are used by ICAO member states to ensure that their local civil aviation operations and regulations conform to global norms, which in turn permits more than 100,000 daily flights in aviation's global network to operate safely and reliably in every region of the world.

In addition to its core work resolving consensus-driven international SARPs and policies among its member states and industry, and among many other priorities and programs, ICAO also coordinates assistance and capacity building for states in support of numerous aviation development objectives; produces global plans to coordinate multilateral strategic progress for safety and air navigation; monitors and reports on numerous air transport sector performance metrics; and audits states' civil aviation oversight capabilities in the areas of safety and security.[36]

Comparison to the SCMS: The scope of the ICAO spans much wider than the SCMS. The ICAO is an international organization operating under the United Nations (UN) Specialized Agencies. Therefore, unlike the SCMS, the ICAO standards and polices extend to international stakeholders. The ICAO develops policies around safety, efficiency, security, economical sustainably, and environmental responsibility. The ICAO also focuses on policies to ensure local civil aviation operations and regulations conform to global norms, which permits flights in aviation's global network to operate safely and reliably in

[36] https://www.icao.int/Security/USAP/Pages/The-Creation-of-the-USAP.aspx

every region of the world. This is similar to the SCMS's goal of having an interoperable network with authentic and trusted messages.

Ecosystem Structure: The ICAO has built a community where member states and industry organizations work together to develop international standards and policies for the aviation industry. They have established technical panels and committees to address specific standards areas and issues facing the industry. Furthermore, the ICAO has established regional offices to provide closer support and coordination for member states.

Internal Organizational Structure

Triennial Assembly

The Triennial Assembly, comprised of all member states of ICAO, meets no less than once every three years and is convened by the Council at a suitable time and place. The assembly has numerous powers and duties, among them to:

- Elect the member states to be represented on the Council
- Examine and take appropriate action on the reports of the Council and decide any matter reported to it by the Council
- Approve the budgets of the organization.

The assembly may refer, at its discretion, to the Council, to subsidiary commissions or to any other body any matter within its sphere of action. It can delegate to the Council the powers and authority necessary or desirable for the discharge of the duties of ICAO and revoke and modify the delegations of authority at any time; and deal with any matter within the sphere of action of ICAO not specifically assigned to the Council. It also reviews in detail the work of the organization in the technical, administrative, economic, legal, and technical cooperation fields. It has the power to approve amendments to the Convention on International Civil Aviation (Chicago, 1944), which are subject to ratification by member states.[37]

Governing Council

The Governing Council is a permanent body of the organization responsible to the Triennial Assembly. It is composed of 36 member states elected by the assembly for a three-year term. In the election, adequate representation is given to states of chief importance in air transport, states not otherwise included, but which make the largest contribution to the provision of facilities for international civil air navigation, and states not otherwise included whose designation will ensure that all major geographic areas of the world are represented on the Council. The Council convenes the Triennial Assembly. The Council has numerous functions, notable among which are:

- To submit annual reports to the Triennial Assembly
- Carry out the directions of the Triennial Assembly
- Discharge the duties and obligations which are laid on it by the Convention on International Civil Aviation (Chicago, 1944)

[37] https://www.icao.int/about-icao/assembly/Pages/default.aspx

- Administers the finances of ICAO
- Appoints and defines the duties of the Air Transport Committee, as well as the Committee on Joint Support of Air Navigation Services, the Finance Committee, the Committee on Unlawful Interference, the Technical Co-operation Committee, and the Human Resources Committee
- Appoints the Air Navigation Commission members and elects the Edward Warner Award Committee members.

Another key function of the Council is to appoint the Secretary General.

As one of the two governing bodies of ICAO, the Council gives continuing direction to the work of ICAO. In this regard, one of its major duties is to adopt international SARPs and to incorporate these as Annexes to the Chicago Convention. The Council may also amend existing Annexes as necessary.

On occasion, the Council may act as an arbiter between member states on matters concerning aviation and the implementation of the provisions of the Convention; it may investigate any situation that presents avoidable obstacles to the development of international air navigation; and, in general, it may take necessary steps to maintain the safety and regularity of international air transport.[38]

Air Navigation Commission

The Air Navigation Commission (ANC) considers and recommends SARPs and Procedures for Air Navigation Services (PANS) for adoption or approval by the ICAO Council. The Commission is composed of nineteen members. Qualifications are outlined in the Convention on International Civil Aviation (Chicago Convention). Although ANC Commissioners are nominated by specific ICAO member states, and appointed by the Council, they do not represent the interest of any particular state or region. They act independently and utilize their expertise in the interest of the entire international civil aviation community. Additionally, a number of persons from states and industry participate in the ANC as observers.

The ANC is tasked by the Council to manage the technical work program of ICAO. Under the approval of the Council, the ANC typically convenes for three sessions each year to address matters within its work program. Each session typically lasts nine weeks, including a three-week recess. The key challenges faced by the ANC include maintaining and improving aviation safety and air navigation efficiency while integrating increased traffic into the current aviation infrastructure, and introducing advanced systems, as well as proactively identifying risks and devising mitigation measures in accordance with the ICAO Global Aviation Safety Plan (GASP) and the Global Air Navigation Plan (GANP).[39]

Secretariat of the ICAO

The Secretariat of the ICAO is headed by the Secretary General. The Secretariat consists of five bureaus: the Air Navigation Bureau, the Air Transport Bureau, the Technical Co-operation Bureau, the Legal Affairs and External Relations Bureau, and the Bureau of Administration and Services. The five Bureau Directors, and the senior officers in charge of Finance, Evaluation and Internal Audit, Communications, and ICAO's seven Regional Offices all report directly to the Secretary General.

[38] https://www.icao.int/about-icao/Council/Pages/council.aspx

[39] https://www.icao.int/about-icao/AirNavigationCommission/Pages/default.aspx

Oversight and Industry Governance: ICAO's Universal Security Audit Program (USAP) conducts audits for member states. The USAP Continuous Monitoring Approach (CMA) will be incorporating a variety of audit and monitoring activities tailored to each member state's aviation security situation. Accordingly, the USAP-CMA will include a range of activities including, but not limited to the activities described below.

Documentation-based audits are used for those states with the most developed aviation security and oversight systems. They primarily measure a state's capability to provide effective oversight over its aviation security system. It is important to note that states identified for documentation-based audits will still receive on-site audits from time to time, as appropriate.

Oversight-focused audits are conducted by means of on-site audits and are used for those states with oversight and quality control systems already in place, but not sufficiently developed to effectively and sustainably address aviation security risks in compliance with relevant Annex provisions. The scope of such audits can be full, covering all audit areas, or partial, covering one or more audit areas.

Compliance-focused audits are conducted by means of on-site audits and focus on states with no or very limited quality control activities. In these cases, the audits include more observations of the implementation of security measures to assess compliance with relevant standards.

Other audit and monitoring activities:

- USAP-CMA cost-recovery audits may be conducted at the request of a member state. The methodology for USAP-CMA cost-recovery audits is the same as for compliance-focused audits or oversight-focused audits. However, ICAO identifies the need for compliance-focused or oversight-focused audits and determines their scope, whereas the type, scope and scheduling of any USAP CMA cost-recovery audit will require agreement between ICAO and the state, and will be assessed by ICAO on a case-by-case basis. The results of USAP-CMA cost-recovery audits will be treated in the same manner as the results from regularly-scheduled USAP-CMA activities, including the possibility of invoking the Significant Security Concern (SSeC) mechanism.
- It is recognized that a number of states are not in a position to derive full benefit from an audit. These states would instead be considered for aviation security assistance and referred to the organization's assistance programs offered through the Implementation Support and Development - Security (ISD-SEC) Section and the Technical Cooperation Program, for the determination and provision of appropriate and timely assistance. These states will be identified in the USAP-CMA secure website. Once assistance is provided to a state, ICAO will determine the appropriate timing for a USAP-CMA audit-related activity to be conducted for such state.[40]

All activities relating to a specific audit are conducted in a transparent manner involving the full participation of the state throughout the audit process, beginning four to six months prior to the starting date of the audit when the states that are scheduled for an audit are officially notified of the audit dates and are requested to submit a signed copy of the USAP-CMA Memorandum of Understanding (MoU), if this has not already been accomplished. At the same time:

[40] https://www.icao.int/Security/USAP/Pages/USAP-CMA-Activities.aspx

- States are requested to submit a completed State Aviation Security Activity Questionnaire (SASAQ), completed compliance checklists, and copies of relevant documents to assist in creating an audit plan
- Audit-related documents and other essential information are forwarded to the state to be audited to enable it to appropriately prepare for the forthcoming audit.

In the case of on-site audits, one or more airports will be selected to be visited by the audit team. During the course of the audit, the auditor(s) will gather evidence and provide the state with ongoing feedback regarding the conduct of the activity.

At the conclusion of the audit, a detailed debriefing is provided to the state and copies of any preliminary findings and recommendations are submitted. A confidential audit report is forwarded to the audited state within 60 calendar days of the completion of the audit and, under the terms of the MoU signed with ICAO, the state is expected to submit a Corrective Action Plan (CAP) within 60 calendar days following receipt of the report. At the same time, states are asked to complete and submit a state audit feedback form commenting on all aspects of the audit process. This feedback is used, whenever feasible, to improve the audit process.

The ICAO audit reports, coupled with the state CAP, provide the starting point for initiating corrective actions taken by a state. Depending upon the nature of the deficiencies identified in an audited state, immediate and direct assistance may be available through the ICAO Implementation Support and Development – Security Section (ISD-SEC), and longer-term assistance projects may be coordinated through the Technical Co-operation Program.[41]

Policy Development and Approval: The ICAO establishes and maintains the international Standards and Recommended Practices (SARPs), as well as Procedures for Air Navigation (PANS), that are fundamental tenets of the Convention on International Civil Aviation (Chicago Convention). SARPs and PANS are critical to ICAO member states and other stakeholders, given that they provide the fundamental basis for harmonized global aviation safety and efficiency in the air and on the ground, the worldwide standardization of functional and performance requirements of air navigation facilities and services, and the orderly development of air transport.

The development of SARPs and PANS follows a structured, transparent, and multi-staged process – often known as the ICAO “amendment process” or “standards-making process.” It involves many technical and non-technical bodies that are either within the organization or closely associated with ICAO. Typically, it takes approximately two years for an initial proposal for a new or improved standard, recommended practice, or procedure to be formally adopted or approved for inclusion in an Annex or a PANS. Occasionally, this timescale can be expanded or compressed depending on the nature and priority of the proposal under consideration.[42]

Funding: The ICAO is a UN Specialized Agency. Those agencies are funded partly through assessments from the UN and voluntary contributions.[43]

[41] https://www.icao.int/Security/USAP/Pages/The-Audit-Process.aspx

[42] https://www.icao.int/about-icao/AirNavigationCommission/Pages/how-icao-develops-standards.aspx

[43] http://www.un.org/en/sections/about-un/funds-programmes-specialized-agencies-and-others/

Best Practices and Takeaways: The ICAO and SCMS both have a diverse group of stakeholders comprising of governments agencies as well as industry. The ICAO uses their stakeholder base to enact working groups and committees to research and develop the standards and policies they implement. A similar process could be developed for the SCMS.

4.2.5 NAV CANADA

Overview and Initial Deployment: NAV CANADA owns and operates Canada's civil air navigation service (ANS), providing services including air traffic control, airport advisory and flight information, and aeronautical information to commercial and general aviation from facilities throughout Canada. The Company was incorporated as a non-share capital corporation funded solely through publicly traded debt and service fees. It manages 12 million aircraft movements a year for 40,000 customers in over 18 million square kilometers – the world's second-largest air navigation service provider by traffic volume.

It is also the world's first fully privatized civil air navigation service provider, created in 1996 through the combined efforts of **four stakeholders: commercial air carriers, general aviation, the Government of Canada, as well as the employees and their unions**.

Comparison to the SCMS: NAV CANADA provides technology-facilitated air navigation services to commercial and general customers as the National SCMS will provide credential management services in V2X environment (supporting safer vehicle operations). Both the National SCMS and NAV CANADA's eco-systems involve a broad spectrum of organizations, associations, and entities interested in their respective services. Both are initiated from their respective country's government. When NAV CANADA was fully owned and operated by the Canadian government as the service provider, the regulator and inspector had a conflict of interest. The National SCMS and SCMS Manager, if solely run by the Federal government as the service provider, could also have similar conflicts of interest for regulations, operations, and inspections and auditing.

NAV CANADA's governance structure and policy development and approval mechanism requires consideration and representation of all stakeholders (including all customers groups) to ensure safety, technological advancement, competitiveness, fairness, and sustained profitability. The National SCMS and SCMS Manager's governance structure and policy development and approval mechanism will would likely have similar requirements and goals.

Ecosystem Structure: NAV CANADA is governed by Board of Directors elected from four stakeholders: commercial air carriers, general aviation, the Government of Canada, as well as the employees and their unions. The 20-member Advisory Committee functions as the deputy of the Board on all matters related to ANS. Eleven nominating (professional and trade) associations, representing a broad spectrum of organizations interested in ANS, elect these 20 members each year. It provides air navigation services to over 40,000 commercial and general aviation customers. Customers are represented in the company's governance and policy-making structure.

Internal Organizational Structure: Internally, the organizational structure is typical of a private corporation. Under the leadership of its Chief Executive Officer (CEO), there are three Executive Vice Presidents: Service Delivery, Finance and Chief Financial Officer, and Human Resources. The General Counsel and Corporate Secretary at a Vice President level report directly to the CEO. The Executive Vice President of Service and Delivery oversees safety and quality, technical operations, IT, and engineering – each of which is led by a vice president. The Executive Vice President of Finance and Chief Financial

Officer oversees pension investments and treasury among other financial matters. The Executive Vice President of Human Resources oversees communications and public affairs, labor relations, etc.

Board of Directors:

As a non-share capital corporation, NAV CANADA has no shareholders. The company is governed by a 15-member board of directors representing the four stakeholder groups that founded NAV CANADA. The four stakeholders elect 10 members as follows:

Table 4. NAV CANADA Board of Directors

Stakeholders	Seats
Air carriers	4
General and business aviation	1
Federal government	3
Bargaining agents (unions)	2

These 10 directors then elect four independent directors, with no ties to the stakeholder groups. Those 14 directors then appoint the president and chief executive officer who becomes the 15th board member.

This structure ensures that the interests of individual stakeholders do not dominate and no member group could exert undue influence over the remainder of the board.

Advisory Committee:

NAV CANADA has an Advisory Committee, comprised of 20 members, which conducts activities on behalf of the Board of Directors on matters relating to the ANS. The 20-member Committee represents a broad spectrum of organizations with an interest in the ANS. Committee members are elected at the Annual General Meeting.

Eleven nominating associations (as they are defined in the Company's by-laws) appoint 19 members to the Committee, and there is one member-at-large.

Oversight and Industry Governance: It is governed by the board of directors. Since it is a non-profit, non-share private organization and its business has much to do with public citizens' safety and national aviation/transportation, the Canadian government is represented on the governing board. As the business operation was owned and operated by the government for years, the current policies and regulations are not recreated, modifications or new policies are brought up by the advisory committees and voted by the Board. Audits are provided internally by an Audit and Finance Committee composed of directors who are independent from the business and non-voting members, and externally by third parties.

The Aeronautics Act and the Canadian Aviation Regulations (CARs) are enforced both internally and externally. Judiciary and administrative penalties would result in the case of offences.

Policy Development and Approval: Policy development is market driven, collaboratively developed and enforced via the Advisory Committee, the Board of Directors, and the executive management team considering key stakeholders, customers, market and economic trends, and the company's sustained profitability.

Funding: It was fully funded by the Canadian government prior to 1996. After 1996 privatization, the business entity paid the government $CAN 1.5 billion and has been only funded by publicly traded debt and service charges to aircraft operators.

Best Practices and Takeaways: NAV CANADA is a good benchmark that the National SCMS could potentially emulate in later stages, but not in the stand-up or start-up stage. Canada used to have a government Federal Communications Commission-like organization to run the civil aviation communication system. Canada later moved the whole operation to the private and non-profit organization, NAV CANADA. In effect, this entity was fully funded by the government in the beginning, then when the operation had been fully established and was running efficiently, it was turned into a private, non-profit, self-sufficient entity.

Potentially, SCMS ownership and governance could also evolve from a governmental-heavy funded structure to a fully private self-sufficient (non-profit or for profit) entity. During the initial National SCMS deployment, it may need government funds and authority to ensure public interest objectives are met.

4.2.6 Responsible Business Alliance

Overview and Initial Deployment: The Responsible Business Alliance (RBA), formerly the Electronic Industry Citizenship Coalition (EICC) is a non-profit organization committed to helping 100+ international members understand and improve the social and environmental challenges and opportunities in the global electronics supply chain.

Through facilitating collaboration among the RBA, the members, and external stakeholders, RBA works with its members and their Tier 1 suppliers to develop supply chain capabilities to assess and address social and environmental risks as they relate to its Code of Conduct. RBA members commit and are held accountable to a common Code of Conduct and utilize a range of training and assessment tools to support continuous improvement.

The RBA is comprised of more than 110 electronics, retail, auto, and toy companies with combined annual revenue greater than $4.75 trillion, directly employing over 6 million people. In addition to RBA members, thousands of companies that are Tier 1 suppliers to those members are required to implement the RBA Code of Conduct. More than 3.5 million people from over 120 countries contribute to the manufacture of RBA members' products.

Comparison to the SCMS: The organization's mission is to maintain a healthy business ecosystem so that every electronics-related business can benefit from lower cost sustainably and socially responsible supply chains. Members conduct business with each other and if one member does not conform to the code its business will suffer eventually. In this regard, SCMS governance could be designed that there is an imbedded self-control and self-regulation mechanism. However, the RBA is a voluntary program for electronics related companies with a simple purpose (lower cost sustainably) and governance. It does not require much funding as it is primarily operated by volunteers. The SCMS requires high degrees of trust, security, privacy, and involves diverse stakeholders from many industries and government entities. It will require substantial funding and a much more sophisticated and complex governance structure.

Ecosystem Structure: The RBA and members develop the Code of Conduct, are held accountable in implementing and conforming to the code by a set of training programs, working groups, task forces, and a self-auditing mechanism in which the Factory Lead Certification program plays a key role. The RBA

collaborates with its stakeholders, achieving a socially responsible, sustainable, fair and healthy business environment and free market economy, ultimately benefiting everyone in the RBA.

RBA members are companies that manufacture or contract the manufacture of electronics, and companies with products in which electronics are essential to the primary functionality of the product. The members include electronics auto, toy, aviation, and wearable technology companies.

All RBA members are required to commit publicly to the RBA Code of Conduct and actively pursue conformance to the code and its standards. RBA members must regard the code as a total supply chain initiative, meaning that members must at a minimum require their next tier suppliers to acknowledge and implement the code.

The RBA's stakeholders include the unions, various trade associations, governments, and NGOs.

Internal Organizational Structure: The RBA is led by a Board of Directors, a secretariat comprised of an Executive Director and a full-time staff, and staff from member companies who participate in a variety of working groups (long term) and task forces (short term) on specific issues. RBA leadership is also advised by a Senior Executive Advisory Council, comprised of executives from member companies.

Oversight and Industry Governance: The RBA is a voluntary coalition aimed at lowering or sustainably controlling the cost of producing electronics or electronic components products for everyone in the alliance. By voluntarily conforming to a set code of conduct, members ensure fair market competition, and sustainable business ecosystems and continuity. The RBA only recently added a paid staff member with all other staff being volunteers from member companies. It certifies a Factory Lead to be responsible for implementing and enforcing adherence of the Code of Conduct. It conducts training, auditing, and assessments to hold its members accountable.

RBA members are held accountable to their Code of Conduct commitment via a range of mandatory accountability and assessment means, including self-assessment questionnaires, audits, and corrective actions where necessary. RBA applicant members have two years from the date they join the RBA to conform to the membership requirements.

The RBA Factory Lead Certification Program is a training and certification program for factory staff. This certification is intended for the individual at a factory responsible for implementing RBA requirements. It is a professional designation to help RBA members, their supply chain partners, and other interested parties ensure understanding of common standards and supply chain issues. The core curriculum can be taken online in the RBA Learning Academy.

Policy Development and Approval: The Code of Conduct, which is the core of the RBA, is developed by a process approved by the full members.

Full members submit policy and code of conduct amendments, revisions, additions, or other changes with standard forms. Submissions are organized and put on a ballot. The Board of Directors reviews and approves the revisions. The full members vote on the Board approved revisions. The Board further revises the code after the round of votes from the members. After some iterations of this process, the code is socialized with the external stakeholders that may recommend further amendments. Finally, the code will be ratified and put out to be implemented by all members and their Tier 1 suppliers.

The Code of Conduct is reviewed every three years, which typically takes one year in duration and follows an extensive consultation process with members and stakeholders.

The policy development process has a relatively low level of effort. The working groups and task forces usually propose policy creations and amendments, while the Board reviews and approves them. All working groups and task forces are comprised of voluntary staff from member companies.

Funding: The RBA members pay an annual fee and the RBA Factory Lead collects a fee from each certification applicant. The organization is run by volunteers from member companies and has only one paid staff member.

Best Practices and Takeaways: The RBA has a very long-term perspective (decades) for the organization's vision and mission. It sets out to address preventatively social, environmental, and other larger long-lasting effects on sustainability issues that the industry may face in the future. Even though the alliance is industry initiated and the policies are self-imposed, RBA has established comprehensive multiple top-down and bottom-up policy/standard implementation/enforcing mechanisms and systems. Rules/policies/standards are clearly defined and disseminated. Implementation of policies and standards is strictly ensured, and ongoing daily auditing and enforcing are carried out globally at the very bottom level of the supply chains. This strategy and practice ensures that all players in the alliance operate in ways that are best for the whole and itself. Such a favorable business environment draws more players to join the alliance; hence, RBA is more and more influential and impactful with time.

4.2.7 SEMATECH[44]

Overview and Initial Deployment: SEMATECH (from Semiconductor Manufacturing Technology) is a non-profit consortium that performs research and development to advance chip manufacturing. SEMATECH has broad engagement with various sectors of the research and development community, including chipmakers, equipment and material suppliers, universities, research institutes, and government partners. SEMATECH conducts research on the technical challenges and costs associated with developing new materials, processes, and equipment for semiconductor manufacturing.

Comparison to the SCMS: SEMATECH was created as a partnership between the United States Government and 14 US-based semiconductor manufacturers to solve common manufacturing problems and regain competitiveness for the US semiconductor industry, which had been surpassed by Japanese industry in the mid-1980s. The semiconductor industry in the late 1970s and early 1980s was a cutting-edge, high-tech industry, similar to V2X communications, involving many other sectors such as materials and equipment. It impacted US national security and strategic competitive positions requiring the US government's involvement and support. The SCMS is critical in V2X deployment, and countries around the world have all been actively working to achieve national deployment to benefit from increased vehicle safety and mobility. V2X deployment could potentially be accelerated and ensure the public interest with government legislation and collaboration, with potential initial government funding. As the V2X ecosystem establishes equilibrium and matures in this case, the SCMS Manager may gradually reduce government funding, and different funding sources may emerge as in the SEMATECH case. SEMATECH was

[44] https://web.archive.org/web/20130702191328/; http://www.sematech.org/corporate/history.htm

established as a research organization and later added manufacturing capacity. It does not directly create policies or standards.

Ecosystem Structure: Before 1996, SEMATECH was headquartered and operated in Austin, TX with its own research and manufacturing facilities. The new chip technologies were created and implemented by the leading semiconductor players at the time including the leading chip makers, materials, and equipment suppliers. The US semiconductor industry's competitiveness began to surpass that of Japan, and the consortium successfully completed its original mission by 1996 with support from the Defense Advanced Research Projects Agency (DARPA). The industry went through a period of consolidation and the consortium turned to international companies and organizations to join. The focus was shifted to research, development, and commercialization of a completely new generation of semiconductor technologies without the US government's involvement.

In 2003, SEMATECH and the University at Albany – State University of New York (SUNY) – established a major partnership to commercialize advanced semiconductor, nanotechnology, and other emerging technologies. Through its government-university-industry partnership with the SUNY Poly Institute, SEMATECH started conducting programs in lithography and metrology at University's Albany NanoTech Complex.

In 2010, SEMATECH was lured by a $300 million investment from the State of New York to move its headquarters and become completely absorbed into SUNY Poly Institute. SEMATECH employees became the Institute's employees.

Internal Organizational Structure: Prior to 2000, the organization was governed by the board of directors from its member companies. The organization ran as a chip manufacturer with heavy emphasis on research and development of new generation chips. From 2010 to present, the organization has been absorbed into SUNY Poly Institute and focuses on researching, developing, and commercializing cutting-edge new technologies.

Oversight and Industry Governance: DARPA invested heavily in the consortium and had oversight authority until it started tapering funding to the consortium. Oversight gradually shifted to the Board of Directors.

Policy Development and Approval: The original consortium did not explicitly set industry-wide polices, but by adapting products and technologies developed in the consortium's facilities, the industry has been gradually developing and adopting a set of product and technology standards. Originally, the mission was straightforward: surpass Japan in chip technology as soon as possible. Now, the leadership council and board direct the organization on semiconductor research, development, and production priorities to further the global industry.

Funding: SEMATECH was funded over a period of five years by public subsidies coming from the US Department of Defense (via DARPA) for a total of $500 million. By 1994, the US semiconductor industry regained strength and market share. SEMATECH shifted its focus to developing and commercializing advanced technologies, such as lithography, front end processes, green energy, power electronics, and biotechnology. The Board decided to gradually eliminate matching funds from the US government, opening memberships to international companies via a subsidiary, International SEMATECH. In 2000, SEMATECH completed its first year of operations as a unified global consortium, with members from

Asia, Europe, and the United States. Its members represent about half of the worldwide chip market. Since 2000, SEMATECH has been solely funded by member dues.

Best Practices and Takeaways: With government leadership and funding, businesses and the industry were quickly motivated to pool resources and talents together to efficiently tackle a defined problem. The purposes, resources, roles, responsibilities, and goals/mission/vision were clearly defined. The establishment and the operation of the consortium were well executed.

4.2.8 Payment Card Industry Security Standards Council (PCI SSC)

Overview and Initial Deployment: The Payment Card Industry Security Standards Council (PCI SSC) was originally formed by American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc. on September 7, 2006. The goal of the PCI SSC is to manage the ongoing evolution of the Payment Card Industry (PCI) Data Security Standard (DSS). The council itself claims to be independent of the various card vendors that make up the council.

Comparison to the SCMS: Like the future SCMS, payment card brands operate massive data systems that bring together different parties (e.g., acquiring banks and issuing banks) to exchange information and sensitive data.

Ecosystem Structure: The PCI SSC was instrumental in the development of security standards intended to benefit cardholders and everyone else involved in payment card transactions. The standards, most notably PCI DSS, are widely applicable because money collection through payment card transactions touches such a vast array of industries. The structure of the PCI SSC and the reasons why its voluntary standards are widely practiced (e.g., the requirement for compliance by the five leading payment card brands) are useful case studies for owners and operators of the certificate management industry.

Internal Organizational Structure: The PCI SSC is led by a policy-setting Executive Committee, composed of representatives from the five founding global payment brands and Strategic Members. A Board of Advisors, drawn from participating organizations, provides input to the organization and feedback on the evolution of the PCI Standards. The Management Committees (i.e., Standards Committee, Operations Committee, and Marketing Committee) drives activity across various work domains. The committee is comprised of participants from the founding and Strategic Membership and employees of the Council. The Management Committee is responsible for maintaining PCI standards and all other Council technical work products, and developing and managing new working groups, special interest groups, and task forces on technical matters. The Management Committee also manages the Council's day-to-day operational functions and provides recommendations, suggestions, and guidance to the Executive Committee regarding corporate and operational matters.

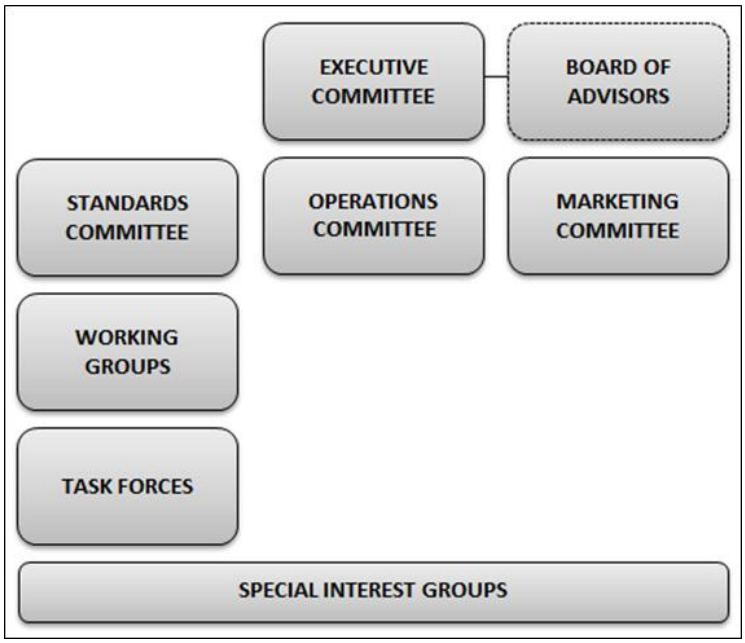

Figure 10. PCI SSC Organizational Structure

Oversight and Industry Governance: The PCI SSC has established three standards pertaining to different areas of payment card security. These standards are directed at three distinct audiences: institutions that process cardholder data; manufacturers of payment card transaction equipment; and developers of payment card transaction software.

- **PCI DSS**: PCI DSS has evolved from a set of largely voluntary guidelines in 2006 to an industry standard with which merchants must comply if they wish to accept payment cards bearing the logos of the five aforementioned leading brands. The standard lists 12 requirements related to safe practices for how cardholder data must be stored, processed, and transmitted in the systems of merchants and service providers (e.g., business entities separate from merchants that can access cardholder data). PCI DSS also specifies auditing requirements to ensure compliance (see the "Security Assurance" section below for additional information).
- **PIN Transaction Security (PTS) Requirements:** This standard specifies a set of security requirements for the equipment used in payment card transaction processing. The requirements are intended for "manufacturers to follow in the design, manufacture, and transport of a device to the entity that implements it."[45] Those who process payment cards (e.g., merchants, financial institutions) are encouraged to use devices that are approved by PCI SSC through these requirements to protect cardholder data and PIN information.
- **Payment Application Data Security Standard (PA-DSS):** PA-DSS applies to the software programs that perform payment applications for storage, processing, or transmittal of cardholder data that takes

[45] PCI SSC, *PCI DSS Quick Reference Guide, v3.1*, https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf.

place during authorization or settlement.[46] This applies to commercial off-the-shelf products that merchants purchase to manage their financial transactions, but only to the applications in the software that involve cardholder data. Vendors of financial software must consider PA-DSS when designing products.

The role of the PCI SSC is limited to setting industry-wide security standards through collaboration and consensus among members, and providing education and training to the larger industry. The Council maintains and updates the standards, while also monitoring emerging threats to cardholder data security. However, enforcement of the standards through compliance programs, and imposing of non-compliance penalties such as fines, is the responsibility of individual payment card brands.[47] Penalties for non-compliance with any required standards would be dictated by the voluntary agreement between the payment card brands and the merchants and service providers under contract. External law enforcement officials would not be involved unless a lack of compliance led to misbehavior in the form of criminal activity, such as identity theft or credit card fraud.

The PCI SSC develops and operates programs to train, test, and qualify organizations and individuals to assess and validate adherence to the various PCI Security Standards and to be re-certified each year. These programs are designed for industry professionals who seek to assist organizations (whether their own or a client's organization) with standards implementation and compliance. The five founding members of the Council recognize those certified by the PCI Security Standards Council as being qualified to assess compliance to the PCI DSS.

Policy Development and Approval: Organizations that are part of the PCI SSC have different roles for standards development depending of their membership type. Participating Organizations within the PCI SSC have access to community meetings, exclusive Council communications, such as advance review of drafts of standards and supporting materials, and regular dialogue with key stakeholders. More than 700 organizations around the world have signed up. The Council's Board of Advisors is another membership within the PCI SSC. It consists of representatives from Participating Organizations. This cross-industry group ensures that all global stakeholder voices are heard in the ongoing development of PCI Security Standards. The Strategic Class Membership provides the opportunity to play a directive role in Council activities, including the ability to nominate PCI officers, as well as serve on the Council's Executive Committee. The Affiliate Class Membership is open to regional and national organizations that define standards and influence adoption by their constituents who process, store, or transmit cardholder data. This category offers the opportunity to serve on PCI working groups and play an active role in the standards development process. The Special Interest Groups (SIGs) are created to analyze specific payment card industry challenges to securing cardholder data. Each SIG is formed to address a specific industry or technological challenge, and recommend changes, clarifications, or improvements to corresponding PCI standards and supporting PCI programs. SIGs are elected by the participating organization members and leverage the business and technical experience of assessors and participating organizations in their respective areas of focus.

[46] PCI SSC, *PCI Payment Application Data Security Standard: Requirements and Security Assessment Procedures, v3.0*, https://www.pcisecuritystandards.org/minisite/en/docs/PA-DSS_v3.pdf.

[47] PCI SSC, *For Merchants*, https://www.pcisecuritystandards.org/merchants/index.php.

Funding: PCI SSC is funded by the payment card brands as well as membership annual dues for participating organizations ($3,750).[48]

Best Practices and Takeaways: Private organizations with the payment card industry have come together to set strict privacy and security standards to ensure protection against malicious use of sensitive data under the PCI SSC. The SCMS could take a similar approach providing a minimum set of security and/or privacy thresholds that the industry must meet set by government, with additional shared practices, procedures, compliance auditing, and further evolution of standards to meet a wider set of consumer (and possible government) concerns or needs. A governing body provides a chance for representatives from all interested parties to have a say in the development of these standards and policies, ensuring stakeholder perspectives are well represented.

4.2.9 Internet Corporation for Assigned Names and Numbers (ICANN)

Overview and Initial Deployment: The Internet Corporation for Assigned Names and Numbers (ICANN) is a nonprofit organization responsible for coordinating the maintenance and procedures of several databases related to the namespaces of the Internet, ensuring the network's stable and secure operation.

The inception of ICANN was a result of the global expansion of the Internet. On January 30, 1998, the National Telecommunications and Information Administration (NTIA) issued for comments on proposed rulemaking, “A Proposal to Improve the Technical Management of Internet Names and Addresses." The proposed rulemaking suggested certain actions designed to privatize the management of Internet names and addresses that allows for the development of competition and facilitates global participation in Internet management. The rulemaking also proposed discussing a variety of issues relating to Domain Name System (DNS) management, including private sector creation of a new nonprofit corporation managed by a globally and functionally-representative board of directors. ICANN was formed in response to this policy. ICANN managed the Internet Assigned Numbers Authority (IANA) under contract to the Department of Commerce (DOC), and pursuant to an agreement with the Internet Engineering Task Force (IETF).

On September 30, 2009, NTIA, reached agreement with ICANN on an Affirmation of Commitments that completed the transition of the technical coordination of the DNS to a multi-stakeholder, private-sector led model, and contains provisions to ensure accountability and transparency in ICANN's decision-making with the goal of protecting the interests of global Internet users, as well as mechanisms to address the security, stability, and resiliency of the Internet DNS.

Comparison to the SCMS: The ICANN was established to help regulate and secure the global expansion of the Internet. The ICANN was initially tasked with taking on the responsibility of the Internet Assigned Numbers Authority (IANA). This is similar to the future National SCMS. The current SCMS proof of concept, which primarily supports government-funded connected vehicle related efforts, could possibly be incorporated into the national SCMS to support the nationwide deployment of connected vehicles. ICANN however, transitioned private-sector led model, while the National SCMS’s model is still to be determined. Both the ICANN and the SCMS have a diverse stakeholder group. ICANN relies on stakeholders ranging from international governments, commercial and no-commercial entities, the public

[48] http://www.posdata.com/documents/Principles_of_PCI_Compliance.pdf

and so on to help develop their policies. Similar to the ICANN, the diverse stakeholders of the SCMS ecosystem could help shape the development and implementation of future policies.

Ecosystem Structure: ICANN performs the technical maintenance work of the Central Internet Address pools and DNS root zone registries pursuant to the Internet Assigned Numbers Authority (IANA) function contract. A majority of ICANN's work revolves around the Internet's global DNS, including policy development for internationalization of the DNS system, introduction of new generic top-level domains (TLDs), and the operation of root name servers. ICANN manages the Internet Protocol (IP) address spaces for IPv4 and IPv6, and assignment of address blocks to regional Internet registries, as well as maintaining registries of IP identifiers.

Internal Organizational Structure: ICANN has been formally organized as a nonprofit corporation "for charitable and public purposes" under the California Nonprofit Public Benefit Corporation Law. It is managed by a 16-member Board of Directors composed of eight members selected by a nominating committee, on which all the constituencies of ICANN are represented; six representatives of its supporting organizations, sub-groups that deal with specific sections of the policies under ICANN's purview; an at-large seat filled by an at-large organization; and the President/CEO, appointed by the Board.

There are currently three Supporting Organizations (SO) to support ICANN's policy making. The Generic Names Supporting Organization (GNSO) deals with policy making on generic top-level domains (gTLDs); the Country Code Names Supporting Organization (ccNSO) deals with policy making on country-code top-level domains (ccTLDs); the Address Supporting Organization (ASO) deals with policy making on IP addresses.

ICANN also relies on some Advisory Committees (AC) and other advisory mechanisms to receive advice on the interests and needs of stakeholders that do not directly participate in the supporting organizations. These include the Governmental Advisory Committee (GAC), which is composed of representatives of a large number of national governments from all over the world; the At-Large Advisory Committee (ALAC), which is composed of individual Internet users from around the world selected by each of the Regional At-Large Organizations (RALO), and Nominating Committees, a team of community volunteers responsible for the selection of eight ICANN Board members, and portions of the At-Large Advisory Committee, the ccNSO and the GNSO. The Root Server System Advisory Committee provides advice on the operation of the DNS root server system; the Security and Stability Advisory Committee (SSAC), which is composed of Internet experts who study security issues pertaining to ICANN's mandate; and the Technical Liaison Group (TLG), which is composed of representatives of other international technical organizations that focus, at least in part, on the Internet.

The ICANN Ombudsman is an independent, impartial, and neutral person contracted to ICANN, with jurisdiction over problems and complaints made about decisions, actions, or inactions by ICANN or the Board of Directors; or unfair treatment of a community member by ICANN Staff, Board, or a constituency body.

Oversight and Industry Governance: ICANN is made up of a number of different groups, each of which represent a different interest on the Internet and all of which contribute to any final decisions that ICANN's makes. The three supporting organizations, mentioned above, oversee their respective areas (domain names, country code top-level domains, IP addresses). The four advisory committees provide ICANN with advice and recommendations. These represent:

- Governments and international treaty organizations
- Root server operators
- Those concerned with the Internet's security
- The "at large" community, meaning average Internet users.

ICANN's final decisions are made by a Board of Directors. Fifteen board members have voting rights and six are non-voting liaisons. Eight of the voting members are chosen by an independent nominating committee and the remainder are nominated members from supporting organizations. ICANN has a President and CEO who is also a Board member and directs the work of ICANN staff, who are based across the globe and help coordinate, manage, and implement all the different discussions and decisions made by the supporting organizations and advisory committees. An ICANN Ombudsman acts as an independent reviewer of the work of the ICANN staff and Board.

Policy Development and Approval:[49] ICANN's policy-making uses a multi-stakeholder model, which is a decentralized governance model that places citizens, industry, and government on an equal level. Unlike more traditional top-down governance models where governments make policy decisions, the multi-stakeholder approach allows for bottom-up, consensus-driven policy-making. Policy recommendations are developed and refined by the ICANN community through its supporting organizations and influenced by advisory committees, all of which are composed of volunteers from across the world. Each supporting organization has its own specific policy development process.

The Generic Names Supporting Organization (GNSO). If there is a policy change or update, the GNSO requests a primary issue report, which is created by the ICANN staff and is open to public comment. Following public comment review, a Final Issue Report is submitted for GNSO Council consideration. The GNSO Council considers the Final Issue Report and decides whether to initiate the policy development process (PDP). If yes, the GNSO Council develops and adopts a charter for the PDP working group and the council calls for volunteers. The working group works with stakeholders to develop a report of the policy changes, which is submitted to the council. The GNSO Council reviews the Final Report and considers adoption. If adoption is considered, the GNSO Council submits a Final Report to ICANN Board. The ICANN Board consults with stakeholders and the GAC, then the ICANN Board votes on the Final Report recommendations.

Country Code Names Supporting Organization (ccNSO). If a policy is changed, the ccNSO Council, the ICANN Board, the Regional ccTLD organizations, the Supporting Organizations (SO)/Advisory Committees (AC), or at least 10 members of the ccNSO may request an Issue Report. The ccNSO Council appoints an issue manager, and determines if the issue is within the scope of ccNSO, which is defined by the bylaws. If the issue is in scope and the ccNSO Council approves the Issue Report, the PDP begins. The ccNSO Council gives public notice and opens a public comment period. The ccNSO Council appoints a working group to develop the policy and issue an Initial Report, which is open to public comment. The working group produces a Final Report and the ccNSO Council requests GAC input. The ccNSO Council deliberates the Final Report and, if adopted, makes recommendations to its members. If members approve, the ccNSO Council submits the Final Report to the ICANN Board. The ICANN Board votes on Final Report recommendations, but national laws remain paramount.

[49] https://www.icann.org/en/system/files/files/multistakeholder-policy-development-31jan17-en.pdf

Address Supporting Organization (ASO). Any individual may submit a global policy proposal to the ASO Address Council or Regional Internet Registries (RIR). The RIR PDP generates a global policy proposal, which the ICANN Board may also request. The ASO Address Council appoints a Policy Proposal Facilitator Team (PPFT). The ASO Address Council or PPFT determine if a global policy proposal requires specific IANA functions, actions, or outcomes. Also, the ASO Address Council oversees the global PDP. Five RIRs review the global policy proposal, and must approve the identical global policy proposal and submit the approved global policy proposal to the ASO Address Council for review. The ASO Address Council then submits a ratified global policy proposal to the ICANN Board. The ICANN Board may accept, reject, request changes, or take no action.

Funding:[50] ICANN's primary sources of revenue are generated from domain name registration activities and DNS service as follows:

Registry Fees. Registry fees are described in the respective registry agreements. Based on those agreements, registries pay to ICANN fees via a fixed fee, transaction-based fee, or both.

Registrar Fees. ICANN accredits registrars in accordance with the Registrar Accreditation Agreement (RAA). The RAA provides for the following types of fees:

- Application fees are paid one time by prospective registrars at the time of the application.
- Annual accreditation fees are fees that all registrars are required to pay annually to maintain accreditation.
- Per-registrar variable fees
- Transaction-based fees based on each add, transfer, or renewal domain name registration.
- Add Grace Period (AGP) deletion fees are charged to registrars that delete added names within the grace period in excess of a threshold.

Address Registry Fees. ICANN coordinates with the Regional Internet Registries (RIRs), which are responsible for the assignment and administration of Internet addresses. RIRs contribute annually to ICANN.

Application Fees. Paid by applicants seeking to become an ICANN accredited domain name registrar. New generic Top-Level Domain (gTLD) - The application fees are paid during the application window by applicants seeking to become a new gTLD registry operator for a particular top-level domain. Application fees are refundable at a decreasing rate according to the processing phase in which the request for refund occurs. Note that once a new gTLD registry agreement is signed with an applicant, that party becomes a registry operator that is subject to registry fees in accordance with the terms of the registry agreement.

Auction Proceeds. Contention sets are groups of applications containing identical or confusingly similar applied for gTLDs. Contention sets must be resolved prior to the execution of a registry agreement for an applied-for gTLD. If ICANN facilitates the resolution of a contention set through an auction, it serves as the method of last resort for determining which applicant may operate a gTLD when several entities have

[50] https://www.icann.org/en/system/files/files/financial-report-fye-30jun17-en.pdf

applied for the same or confusingly similar gTLD. The auction is concluded when the remaining application is not in contention as a result of competing applicants having exited the auction. The auction fee received by ICANN is the prevailing price and is paid by the final bidder.

Country Code Top Level Domain (ccTLD) Contribution and Fees. ICANN receives contributions from ccTLD operators on a voluntary basis. The ccNSO maintains guidelines offered to ccTLD operators that decide to contribute financially to ICANN. These guidelines suggest amounts of voluntary contributions based on the number of domain names under management.

Contributions and Other Income. ICANN receives sponsorships from parties for the ICANN meetings in return for providing exhibition space and advertisements at the meetings.

Best Practices and Takeaways: ICANN's transition from public to private is a unique example. NTIA issued a proposed rulemaking to privatize the management of Internet names and addresses that allows for the development of competition and facilitates global participation in Internet management as well as addresses a variety of issues relating to DNS management. The proposed rulemaking allowed stakeholders to provide feedback on the development of the ICANN, like the organizational structure.

ICANN's policy-making process uses a multi-stakeholder model that places citizens, industry, and government on an equal level. Unlike more traditional top-down governance models, where governments make policy decisions, the multi-stakeholder approach allows for bottom-up, consensus-driven policy-making. Policy recommendations are developed and refined by the ICANN community through its supporting organizations and influenced by advisory committees, all of which are composed of volunteers from across the world.

4.2.10 The Joint Commission

Overview and Initial Deployment: The Joint Commission is a United States-based, nonprofit, tax-exempt 501(c) organization that accredits more than 21,000 US health care organizations and programs. The international branch accredits medical services from around the world. A majority of state governments recognize Joint Commission accreditation as a condition of licensure for the receipt of Medicaid and Medicare reimbursements. It is not the only accreditation organization and no other organizations certify the Joint Commission. It is sometimes criticized as accrediting organizations as long as they pay. It is a simple accreditation organization and it is not necessarily applicable to the SCMS Manager governance case; although, there are lessons learned that could be applied for accreditation of certification test labs.

Comparison to the SCMS: It sets up a standard and audits healthcare organizations against the standard for a substantial fee. It certifies them if they pass the audit. The healthcare organizations usually get between six months to one year of advanced notice for them to prepare for the audit. Since it charges a fee ranging from $1,400 to $46,000 per on-site survey and provides advanced notice before audit, many healthcare providers pass the audits even though they would not normally meet the standard. The Joint Commission governance model is not applicable to SCMS; except for understanding accreditation processes.

Ecosystem Structure: The Joint Commission is part of the accreditation organizations in the healthcare industry. The term "accreditation" refers to the voluntary evaluation that a hospital can undergo to confirm that it is compliant with the Medicare Conditions of Participation (CoPs) specified by Centers for Medicare

& Medicaid Services (CMS). Any hospital seeking to be certified as a provider to patients who qualify for Medicare (health insurance for the elderly) and Medicaid (health insurance for low-income individuals) must meet the Medicare CoPs. Hospitals can be evaluated by the relevant CMS State Survey Agency for compliance with the CoPs, or they can seek accreditation from a CMS-approved accreditation organization. It should be noted that accreditation is separate from licensure. Hospitals usually must apply for a license (or licenses) to operate from the relevant state government prior to providing services and seeking Medicare certification. The Joint Commission provides accreditation that allows hospitals to meet Medicare CoP and achieve other benefits. Many state governments have recognized the value of the Joint Commission accreditation and incorporated it into their requirements for state licensure.

Internal Organizational Structure: A Board of Commissioners, made up of 32 industry representatives, governs the Joint Commission. The Board includes physicians, administrators, nurses, a labor representative, and others, along with corporate members – such as representatives from relevant trade groups (e.g., American Hospital Association and American Medical Association). The Board is led by a President and features eight standing committees with various task forces for current initiatives.[51]

Oversight and Industry Governance: Accreditation by the Joint Commission allows a hospital to display the Gold Seal of Approval®,[52] which can give the organization a competitive edge in the marketplace. Many of the results of the Joint Commission surveys are made available online to consumers, which increases the transparency of the accreditation process and helps potential patients make informed decisions about where to seek treatment.

Policy Development and Approval: The Joint Commission standards are developed with input from health care professionals, providers, subject matter experts, consumers, and government agencies (including the Centers for Medicare & Medicaid Services). They are informed by scientific literature and expert consensus and reviewed by the Board of Commissioners. New standards are added only if they relate to patient safety or quality of care, have a positive impact on health outcomes, meet or surpass law and regulation, and can be accurately and readily measured**.** The standards development process includes the following steps:

1) Emerging quality and safety issues suggesting the need for additional or modified requirements are identified through the scientific literature or discussions with the Joint Commission's standing committees and advisory groups, accredited organizations, professional associations, consumer groups, or others.
2) The Joint Commission prepares draft standards using input from technical advisory panels, focus groups, experts, and other stakeholders.
3) The draft standards are distributed nationally for review and made available for comment on the Standards Field Review page of the Joint Commission website.
4) After any necessary revisions, standards are reviewed and approved by executive leadership.
5) The survey process is enhanced, as needed, to address the new standards requirements, and pilot testing of the survey process is conducted.

[51] The Joint Commission, *Facts about the Board of Commissioners*, http://www.jointcommission.org/about_us/who_we_are.aspx.

[52] The Gold Seal of Approval® is a registered trademark of The Joint Commission.

6) Surveyors are educated about how to assess compliance with the new standards.
7) The approved standards are published for use by the field.
8) Once a standard is in effect, ongoing feedback is sought for the purpose of continuous improvement.

Funding: A large portion of the Joint Commission's funds come from annual accreditation subscription fees and on-site survey fees. The Joint Commission is also funded from their consultative technical assistance, educational programs, and publications. Since the Joint Commission is a nonprofit organization, they also accept donations.[53]

Best Practices and Takeaways: Developing, approving, and populating industry standards through a combined effort by doctors, nurses, technicians, administrators, and other healthcare professionals ensure the standards are in line with the best practices of the industry. It seems that hospitals basically pay for accreditation with a substantial fee. Accreditation should be realistically affordable and ensure that those accredited organizations follow set standards.

[53] The Joint Commission on Accreditation of Healthcare Organizations and Affiliates. Financial Statements and Supplemental Schedules. (December 2013)

Chapter 5. Best Practices, Lessons Learned, and Takeaways Applied to a National SCMS

While the National SCMS is a unique, large-scale, distributed PKI system, deployers can apply concepts and lessons learned from other policy development and governance organizations (PKI-related or not). Themes and commonalities start to emerge as one reads through the descriptions of the international V2X development and deployment efforts, public and private PKI systems, and other industry policy and governance organizations. Many of the same concepts can be implemented within the National SCMS and the SCMS Manager to increase the internal organizational efficiency and ability of the SCMS Manager to provide effective industry governance and enforcement to fulfill public interest objectives.

This chapter aggregates the best practices from Chapters 2 through 4 and explains how concepts can be applied to deploying the eventual National SCMS ownership, governance, operational, and deployment models. The content will continue to evolve, and be restructured and reused within later project tasks based on additional discussion on how to apply specific concepts to the National SCMS ownership, governance, and operational models. These best practices, lessons learned, and takeaways feed directly into the development of draft ownership and governance models within Task 4 of this project.

Table 5 aligns the high-level ownership and governance models the team developed in Task 4 to a representative governance organization or system explored within this report. The table also discusses why that type of model was used for that specific organization and applies relevant considerations in using that model, or a similar model, to deploy the National SCMS.

Tables 6 through 9 identify best practices, lessons learned, and takeaways:

- Regardless of the ownership and governance model used to deploy the National SCMS
- If the National SCMS and SCMS Manager are public organizations and owned by the US Government
- If the National SCMS and SCMS Manager are deployed as some version of a P3, which can range from highly public to highly private
- If the National SCMS and SCMS Manager are deployed through a completely private consortium.

Table 5. Potential High-Level National SCMS Deployment Models Aligned to Existing Industry Organizations

High-Level Deployment Models	Example Organization	Reasons for the Deployment Model for the Example Organization	Considerations in Using the Deployment Model for the National SCMS
Completely Public	Federal Aviation Administration (FAA) (and initially the Canadian air navigation system which became NAV CANADA)	Policies and rules impact a vast number of public citizen's safety and daily life. Any deviation from the standards/policies/rules could result in significant harm to many public citizens. Enforcement is essential.	It may be difficult to function effectively as both a regulator and operator. It may become unnecessarily bureaucratic and inefficient. Continued funding may not be available or unstable for political reasons.
Government-led P3	SEMATECH	The primary goal (semiconductor technology advancement) was critical to the US defense system, and the country's military competitive advantage. There was an urgency to achieve the desired goal and it required large initial capital funding.	In the initial stage, a government-led model may be most conducive in establishing the operation: developing policies, regulations, standards, and exerting authority and leadership
Balanced P3	VICS (Japan)	Japan is a small and homogeneous country. Trust and cooperation are deeply entrenched in its culture and business environment. There is a need and great benefit for the citizens in highly populated cities to navigate safely and efficiently. It is beneficial for the government, businesses, and the public. The government set up operations and policies with input from industry. Industries cooperatively run operations, abiding by a set of unwritten rules and expectations.	This requires high levels of trust and cooperation between the government and industry, and trust among all the stakeholders from various industries. With numerous business cultures, a huge population, and different business environments and state laws, this necessary level of trust and cooperation may be difficult to achieve.
Industry-led P3	NAV CANADA (private air navigation service)	Originally, the Canadian air navigation was run as a completely public organization. However, the decision was made to privatize services for increased efficiency. Since it is critical to everyday citizens' life and safety, government representation is still essential.	Once the SCMS Manager has been well established, the industry-led P3 model may be better suited to maintain and improve the operations as it is likely to be more efficient, less bureaucratic, and more market driven than a government-led model.
Completely Private	RBA, AUTOSAR, GENIVI Alliance	For RBA, the goal was to keep every player in check so that no rogue actor would disrupt the industry. It's for the industry players' own good that no one acts outside of the self-imposed policies and rules. However, any deviation from the policies and rules/standards would not cause immediate harm to the public in general. As	National SCMS operations would affect many public citizens' safety and daily life. Any small deviation from compliance to the regulations and policies could cause immediate harm to the public. Federal government authority and oversight could be necessary to strictly

High-Level Deployment Models	Example Organization	Reasons for the Deployment Model for the Example Organization	Considerations in Using the Deployment Model for the National SCMS
		for AUTOSAR and GENIVI and other completely private industry alliances, they were formed by their industry's leaders to develop and populate a specified, narrowly focused small number of standards for a specific part of an industry (such as automotive electronic control systems manufacturing). It is for the industry's own good to adhere to such standards as this will benefit the suppliers and the car manufacturers at the same time. However, if any actor deviates from the policies and standards it would not cause immediate and large-scale harm to public.	enforce adherence to the policies, rules, and standards.

Table 6. Best Practices, Lessons Learned, and Takeaways for the National SCMS and SCMS Manager Regardless of the Ownership and Governance Model

Objective and/or Attribute	Best Practice, Lesson Learned, or Takeaway (with aligned organization)	Applicability to the National SCMS and/or SCMS Manager
Oversight and Governance/ Policy Development and Approval	A formal charter that details an organization's purpose, membership requirements, policy change process, and voting process (CA/B Forum).	The SCMS Manager should have a formal charter describing its mission, goals, membership requirements, authority, and responsibilities. The PKI policy change process and voting process should also be formalized; although, these processes may not be specifically outlined within the charter.
Internal Organizational Structure	A combination of function and project oriented internal organizational structure (Multiple organizations such AUTOSAR, VICS, RBA).	The SCMS Manager could have a matrixed internal organizational structure to manage standard functions as well as lead projects or tasks, e.g., new policy or process development. However, this structure will likely vary slightly based on the ownership and governance model. Example: There is an operations department/office/group to monitor that the National SCMS is performing to a certain standard as designed, but there are also ad hoc working groups and task forces that conduct primary development of

Objective and/or Attribute	Best Practice, Lesson Learned, or Takeaway (with aligned organization)	Applicability to the National SCMS and/or SCMS Manager
		policies (e.g., certificate policy update working group or task force) and other processes as necessary.
Stakeholder Representation	Transparency of policies, as long as there is no privacy or security concern in sharing those policies (Multiple organizations, such as the CA/B Forum).	To promote transparency and trust among the general public, industry, and government, the SCMS Manager should require all National SCMS policies be publicly available unless there is a specific privacy or security need to restrict access.
Availability/ Performance/ Trust Anchor Management	If there are multiple root CAs operated by separate entities using multiple certificate policies, certificate policies should be mapped to the overarching CP (Federal Bridge Certificate Authority).	Mapping of certificate policies to an overarching CP is standard for systems involving multiple root CAs. These types of requirements would be specified within the overarching CP developed by the SCMS Manager. The SCMS Manager would require periodic submission of audit reports from each separate policy management authority attesting to the compliance of that portion of the SCMS with the respective policy.
Availability/ Performance/ Trust Anchor Management	If the SCMS will have a single root CA operated under a single CP, the Federal PKI method of performing compliance analysis would serve as an appropriate model.	The SCMS Manager would serve as the single policy management authority, reviewing and approving the Certification Practice Statements of each component to ensure compliance with the single policy. The SCMS Manager would require periodic submission of audit reports from each operating organization attesting to the compliance if that portion of the SCMS with the policy and approved practice statement.
Security/ Privacy/ Availability	Requirements for members to provide real time information concerning security incidents and status/resolution of those incidents (Federal PKI).	Each component of the SCMS should be conducting continuous monitoring to provide visibility into information and infrastructure assets, awareness of threats and vulnerabilities, and visibility into the effectiveness of security controls. Each owner-operator should immediately report incidents and the status of those incidents to the SCMS Manager so that the manager can determine the overall risk to the system and employ the necessary mitigation strategies. These processes would be specified within the CP.

Objective and/or Attribute	Best Practice, Lesson Learned, or Takeaway (with aligned organization)	Applicability to the National SCMS and/or SCMS Manager
Oversight and Auditing/ Policy Development and Approval	Requirements for PKI components to undergo annual independent compliance audits and provide an annual update which includes changes to policies and practices and results of the annual audits (Federal PKI).	Annual independent compliance audits are standard practice in PKI systems. The SCMS Manager would specify audit processes, practices, and procedures within the CP.
Adaptability and Resiliency/ Performance	Periodic testing of all member PKI artifacts (certificates, revocation lists, etc.) to ensure interoperability and conformance to standards and monitor public facing repositories for both currency of information and availability (Federal PKI).	Similar justification and applicability as the annual auditing best practice above. The SCMS Manager will specify these processes and requirements within the CP.
Trust Anchor Management	The use of cross certificates has proven to be a brittle trust mechanism (Federal PKI).	Although technically feasible, cross certificates would not be a viable method for ensuring trust across multiple PKIs within the SCMS.
End Entity Certification Method/ Affordability	Accreditation should be realistically affordable and follow a public standard (The Joint Commission).	The SCMS Manager could set and publish its certification lab accreditation policy and process. A private company or other organization may then set up the required test lab facilities and request accreditation from the SCMS Manager. The test lab completes the published accreditation process and, if it meets the stated criteria, receives accreditation. This grants the test lab the ability to certify devices and to refer to itself as accredited. The fee to accredit should support the continued operation of the accreditation program. Depending on the funding model for sustainment, this may apply to supporting other aspects of the SCMS Manager. However, the accreditation fees should not be one of the main sources of funding for the SCMS Manager.

Table 7. Best Practices, Lessons Learned, and Takeaways for a Publicly Owned and Governed National SCMS and SCMS Manager

Objective and/or Attribute	Best Practice, Lesson Learned, or Takeaway (with aligned organization)	Applicability to the National SCMS and/or SCMS Manager
Ownership	Publicly owned and operated PKIs such as the Federal PKI and the EU Digital Signature Infrastructure primarily support government organizations or the public's direct interaction with the government (e.g., payment of a fee).	The Federal government will likely not be able to own and operate all PKI components of the National SCMS for reasons of maintaining privacy and ensuring efficient scalability. The system is primarily for use within the transportation system used by all, not government activities.
Oversight and Governance	The Federal PKI consists of the Policy Authority (PA) and the Management Authority (MA) and operates under a charter approved by the US Government Federal Chief Information Officer Council.	The SCMS Manager charter should be approved by the select government organization or official bestowed with the applicable authority. The SCMS Manager could be organized in a similar way to separate the policy and management of operations functions.
Funding	The Federal PKI is funded by a combination of appropriated funds for Federal Agencies and Federal Agency cost reimbursement to the General Services Administration (GSA) which provides the Policy Authority secretariat support and operates the Management Authority.	National SCMS component and Manager funding could be a combination of appropriated funds for the Federal Agency in charge and fees for service.
Ownership/ Funding	Members owning and operating their own PKIs directly fund their own operations (Federal PKI).	Because there are already companies offering V2X certificate services, there is a high likelihood that the National SCMS will be a multi-root environment. In this case, those entities could fund their own operations without government support.
Stakeholder Representation / Policy Development and Approval	While the Federal PKI provides significant opportunity for participants to have their voices heard on proposed policy changes and the decision to approve it for implementation, participants are members and this information is not publicly available. This is mainly because it does not affect the many people outside of the Federal government.	Because the National SCMS will impact most Americans, a public model should still include transparency and public discussion, which the Federal PKI lacks.

Table 8. Best Practices, Lessons Learned, and Takeaways for a Public – Private Partnership (P3) Owned and Governed National SCMS and SCMS Manager

Objective and/or Attribute	Best Practice, Lesson Learned, or Takeaway (with aligned organization)	Applicability to the National SCMS and/or SCMS Manager
Ownership/ Funding	The European Commission will implement the common EU root CA and TLM based on the common rules to ensure EU wide interoperability and trust in a four year fully funded pilot phase, open to all stakeholders and pilots.	The Federal government could take a similar approach to initiate the early deployment of the National SCMS and periodically reassess plans to auction off components or grant concessions at the end of a set time period.
Sustainment Funding	The European Commission has developed potential high-level funding models for each role within the trust model, as well as a registration fee structure to sustain the TLM and CPOC.	The National SCMS and SCMS Manager could be funded by a registration fee. However, it is more realistic to fund the SCMS through a one-time fee associated with the purchase of a vehicle. Depending on the actual ownership and governance model, that fee may be segmented and distributed to different entities.
Oversight and Governance/ Policy Development and Approval	Based on current plans, the TLM will be run by the European Commission.	The Federal government could maintain control of the SCMS Manager for policy development, oversight, and enforcement, while leaving actual technical operations to industry.
Ownership/ Oversight and Governance	The VICS governance model is facilitated by trust and cooperation between the government and industry. Japan being a small country with homogenous culture and deeply subscribed believe to collectively contribute and even sacrifice for the benefit of the society likely played a role in the success of this governance model.	In a P3 National SCMS model, the Federal government must ensure its roles, responsibilities, and authority are clearly stated within the SCMS Manager charter and relative to the Federal funding and support provided. At least for initial deployment, the government cannot expect industry to sacrifice for the benefit of society which is a common philosophy in Japan.
Oversight and Governance/ Policy Development	ICANN uses a multi-stakeholder model when updating policies, which places citizens, industry and government on an equal level. Policy recommendations are developed and refined by the ICANN community through its supporting	Since there is a diverse group of stakeholders within the National SCMS, this approach could level the playing field when deciding upon polices. Also, a similar approach could be taken depending on the decided level of involvement of the

Objective and/or Attribute	Best Practice, Lesson Learned, or Takeaway (with aligned organization)	Applicability to the National SCMS and/or SCMS Manager
and Approval/ Stakeholder Representation	organizations and influenced by advisory committees, all of which are composed of volunteers from across the world. ICANN's final policy decisions are made by a Board of Directors. The US Government, along with other nations' governments do not have the voting rights when developing policies, however they do serve as an advisory committee and provide advice and recommendations to the ICANN board.	Federal government. Having the Federal government as an advisory role in the National SCMS could help ensure public interest objectives are met without overseeing the SCMS Manager.
Ownership/ Funding	Canada used to have a government FAA-like organization to manage air traffic control operations. Canada privatized its air traffic control operations which became a non-profit organization, NAV CANADA.	The National SCMS could potentially emulate this transition from fully public to fully private in later stages. SCMS ownership and governance could evolve from a heavily government funded structure to a fully private self-sufficient entity (for profit or non-profit). During the initial National SCMS deployment, it may need government funds and authority to ensure public interest objectives are met.
Ownership/ Funding	With the government leadership and funding, businesses and the industry were quickly motivated to pool resources and talent to create SEMATECH to quickly advance US company semi-conductor capabilities and technologies.	For quicker initial SCMS deployment in line with the Federal government's established goals and objectives for V2V communication, the Federal government may need to provide the initial heavy lifting in terms of funding and leadership.

Table 9. Best Practices, Lessons Learned, and Takeaways for a Privately Owned and Governed National SCMS and SCMS Manager

Objective and/or Attribute	Best Practice, Lesson Learned, or Takeaway (with aligned organization)	Applicability to the National SCMS and/or SCMS Manager
Security/ Privacy/ Stakeholder Representation	In the case of most organizations that originated based on a government mandate or a government related objective was the purpose of the organization, the government was involved in the initial funding, deployment, and operation of the organization (EU V2V deployment, SEMATECH, ICANN, ICAO, NAV CANADA, US Government Federal PKI, EU Digital Signature Infrastructure).	If the USDOT continues forward with the V2V NPRM, it may need to have some involvement within the National SCMS deployment to ensure public interest objectives and requirements are met. A completely private approach will not provide an adequate lever for government influence and the ability to ensure public interest objectives, specifically privacy.
Policy Development and Approval	The CA/B Forum policy development process is well thought-out and provides an appropriate level of transparency to ensure that the policies properly balance security and cost. Policy is developed using a publicly accessible web site and discussed through a public mailing list. The forum maintains a private web site and private mailing list for sensitive items where discussion on the public mail list could reasonably be detrimental to the implementation of security measures by members.	The SCMS Manager could implement a similar strategy for policy development to balance openness, security, and cost. Although, this process should likely be employed no matter the ownership and governance model.
Oversight and Governance	While the distributed oversight and governance model simplifies the CA/B Forum's roles and responsibilities, it also presents the potential for certificates from compliant PKIs to fail because they did not meet a specific vendor requirement that may not be a requirement of other product vendor.	This level of distributed oversight and lack of an enforcement capability is not feasible for the National SCMS. The SCMS Manager will need to have authority to enforce policy and requirements to ensure a completely functional system.
Oversight and Governance	Within AUTOSAR and the GENIVI Alliance, suppliers basically need to meet the standards to do business with the OEMs. This serves as the enforcement mechanism for standards and policies.	If the National SCMS was completely private, the SCMS Manager could use a similar mechanism. If the entity does not meet the standard set in the CP or fails audits, they simply would not be authorized to provide services within the National SCMS.

Objective and/or Attribute	Best Practice, Lesson Learned, or Takeaway (with aligned organization)	Applicability to the National SCMS and/or SCMS Manager
Funding/ Stakeholder Representation / Policy Development and Approval	Within multiple completely private entities (e.g., AUTOSAR, GENIVI Alliance, RBA), there are multiple membership tiers which are linked to a specific fee paid to the governance organization. These tiers are organized based on the type of stakeholder and allowed involvement within the governance organization.	In a completely private model, a tiered membership model would be key to ensuring that the appropriate and interested stakeholders had the greatest involvement in activities such as policy development while supplementing funds for the operation of the SCMS Manager. The lowest level of membership could be free for interested stakeholders to have access to policies and appropriate levels of SCMS performance data.
Oversight and Governance	Private organizations with the payment card industry have come together to set strict privacy and security standards to ensure protection against malicious use of sensitive data under the PCI SSC. However, enforcement of the standards through compliance programs, and imposing of non-compliance penalties such as fines, is the responsibility of individual payment card brands. Penalties for non-compliance with any required standards would be dictated by the voluntary agreement between the payment card brands and the merchants and service providers under contract.	The SCMS Manager could take a similar approach providing a minimum set of security and/or privacy thresholds that the industry must meet, with additional shared practices, procedures, compliance auditing, and further evolution of standards to meet a wider set of consumer (and possible government) concerns or needs. Penalties for non-compliance could be written into the CP.

Acronyms

Table 10. Acronyms

Acronym	Definition
AA	Authorization Authority
AC	Advisory Committees
AGP	Add Grace Period
ALAC	At-Large Advisory Committee
AMTICS	Advanced Mobile Traffic Information & Communication System
ANC	Air Navigation Commission
ANPRM	Advanced Notice of Proposed Rule Making
ANS	Air Navigation Service
ARA	AUTOSAR Runtime for Adaptive Applications
ASO	Address Supporting Organization
AUTOSAR	AUTomotive Open System ARchitecture
CA	Certificate Authority
CA/B	CA/Browser
CAP	Corrective Action Plan
C-ARS	Cooperative Automated Driving Roadway System
CCMS	Central Configuration and Management System
C-ITS	Cooperative Intelligent Transport Systems
CMS	Centers for Medicare & Medicaid Services
CP	Certificate Policy
CPOC	C-ITS Point of Contact
CPS	Certificate Practice Statement
CV	Connected Vehicle
DARPA	Defense Advanced Research Projects Agency
DNS	Domain Name System
DOC	Department of Commerce
DSS	Data Security Standard
EA	Enrollment Authority
EC	European Commission

Acronym	Definition
ECTL	European Certificate Trust List
EDSD	Electronic Digital Signature Directive
EFTA	European Free Trade Association
EICC	Electronic Industry Citizenship Coalition
ESI	Electronic Signatures and Infrastructure
ESO	European Standards Organization
ETSI	European Telecommunications Standards Institute
FBCA	Federal Bridge Certificate Authority
FHWA	Federal Highway Administration
FPKI	Federal Public Key Infrastructure
GAC	Governmental Advisory Committee
GANP	Global Air Navigation Plan
GASP	Global Aviation Safety Plan
GDP	GENIVI Development Platform
GNSO	Generic Names Supporting Organization
GSA	General Services Administration
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ICAO	International Civil Aviation Organization
ICT	Information and Communications Technologies
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISD-SEC	Implementation Support and Development – Security Section
ITS	Intelligent Transportation Systems
ITS-S	ITS-Station
IVI	In-Vehicle Infotainment
KISA	Korea Internet Security Agency
MA	Management Authority
MIAC	Ministry of Internal Affairs and Communications
MIC	Ministry of Internal Affairs and Communications
MLIT	Ministry of Land, Infrastructure and Transport
MOC	Ministry of Construction
MPT	Ministry of Posts and Telecommunication
NHTSA	National Highway Traffic Safety Administration

Acronym	Definition
NPA	National Police Association
NPE	Non-Person Entities
NPRM	Notice of Proposed Rule Making
NSO	National Standards Organizations
NTIA	National Telecommunications and Information Administration
OEM	Original Equipment Manufacturer
PA	Policy Authority
PA-DSS	Payment Application Data Security Standard
PANS	Procedures for Air Navigation Services
PCI	Payment Card Industry
PDP	Policy Development Process
PE	Public Enquiry
PIN	Personal Identification Number
PIV	Personal Identity Validation
PKI	Public Key Infrastructure
PMO	Project Management Office
PPFT	Proposal Facilitator Team
PTS	PIN Transaction Security
RA	Registration Authority
RAA	Registrar Accreditation Agreement
RACS	Road/Automobile Communication System
RALO	Regional At-Large Organizations
RBA	Responsible Business Alliance
RIR	Registries
SASAQ	State Aviation Security Activity Questionnaire
SCMS	Security Credential Management System
SIG	Special Interest Groups
SO	Supporting Organization
SSAC	Security and Stability Advisory Committee
SSC	Security Standards Council
SSL	Secure Sockets Layer
TCA	Transport Certification Australia
TLG	Technical Liaison Group
TLM	Trust List Manager

Acronym	Definition
TLS	Transport Layer Security
TSP	Trusted Service Providers
UN	United Nations
USAP	Universal Security Audit Program
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
VERTIS	Vehicle, Road, and Traffic Intelligence Society
VICS	Vehicle Information and Communication System
VIIC	Vehicle Infrastructure Integration Consortium
WG	Working Group

References

European Commission. (December 2017). Security Policy & Governance Framework for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS). Release 1. DG Move, European Commission.

European Commission. (January 2016). C-ITS Platform. Final Report. DG Move, European Commission.

European Commission. (June 2017). Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS). Release 1. DG Move, European Commission.

European Commission. (September 2017). C-ITS Platform Phase II Working Group Security. Final Report. DG Move, European Commission.

Australian Government Digital Transformation Office. (December 2015). Gatekeeper Public Key Infrastructure Framework. V 3.1, p. 10. Australian Government, Department of Finance.

Austroads. (March 2015). Research Report AP-R479-15, "Concept of Operations for Core C-ITS Functions", March 2015. Association of Australasian Road Transport and Traffic Agencies, Australian Government.

Transport Certification Australia (TCA). (Accessed January 2018) https://tca.gov.au/tca. TCA, Australian Government.

AUTOSAR. (Accessed March 2018) https://www.autosar.org.

AUTOSAR. (Accessed March 2018) https://www.engineersgarage.com/articles/autosar-automotive-open-systems-architecture.

CA/Browser Forum. (effective as of July 6, 2017). By Laws of the CA/Browser Forum. Version 1.7. CA/Browser Forum.

CA/Browser Forum. Member List. (As of 2017). https://cabforum.org/members/. CA/Browser Forum.

Federal Public Key Infrastructure (FPKI). FPKI Website. (Accessed December 2017). https://fpki.idmanagement.gov/. FPKI, General Services Administration (GSA).

Federal Public Key Infrastructure (FPKI). (January 2015). Federal Public Key Infrastructure Policy Authority Charter, Bylaws, and Operational Procedures. Version 1.0. FPKI, General Services Administration (GSA).

European Telecommunications Standards Institute (ETSI). Overview of Electronic Signatures Law in the EU. (Accessed December 2017). https://acrobat.adobe.com/content/dam/doc-cloud/en/pdfs/overview-of-electronic-signature-law-in-the-EU.pdf. ETSI, European Commission.

ETSI. Funding ETSI. (Accessed December 2017). http://www.etsi.org/about/what-we-are/funding. ETSI, European Commission.

ETSI. Approval Process. (Accessed December 2017). http://www.etsi.org/standards/how-does-etsi-make-standards/approval-processes. ETSI, European Commission.

IEEE. (October 1996). The Strategy and Deployment Plan for VICS. By Shinsaku Yamada. Vehicle Information and Communication System Center, Published in the IEEE Communications Magazine.

GENIVI. (Accessed March 2018). https://www.genivi.org.

GENIVI. (Accessed March 2018). https://www.cnx-software.com/2011/08/19/what-is-genivi.

GENIVI. (Accessed March 2018). https://www.crunchbase.com/organization/genivi-alliance.

Vehicle Information and Communication System (VICS) Center. (2013). VICS Pamphlet, VICS Center, Ministry of Land, Infrastructure and Transport, Government of Japan.

Ministry of Land, Infrastructure and Transport. (October 2007). ITS Policy in Japan and Smartway. By Mitsuo Arino. ITS Policy and Program Office, Road Bureau, Ministry of Land, Infrastructure and Transport, Government of Japan.

Akira Mizutani, Mai Kawamura, Eriko Ando, and Toru Owada, Security Operation Management Initiatives in Cooperative Vehicle-Infrastructure Systems for Safe Driving, *Hitachi Review*, Vol. 65 (2016), No. 1. Pp. 747-751.

IEEE. (1993). Toward Realization of VICS – Vehicle Information and Communications. By Kaoru Tamura, Makoto Hirayama. VICS Promotion Council, IEEE - IEEE Vehicle Navigation & Information Systems Conference, Ottawa - VNIS ©

USDOT. (1996). Intelligent Transportation Systems in Japan By Hideo Tokuyama. FHWA Public Roads, Issue No: Vol. 60 No. 2, Fall 1996. Federal Highway Administration (FHWA), USDOT.

USDOT. (October 23, 2013). Organizational and Operational Models for the Security Credentials Management System (SCMS), Industry Governance Models, Privacy Analysis, and Cost Updates. Draft Revision Report. Federal Highway Administration (FHWA), USDOT.

SEMATECH. SEMATECH History. (Accessed January 2018). https://web.archive.org/web/20130702191328/http://www.sematech.org/corporate/history.htm. SEMATECH

Payment Card Industry Security Standards Council (PCI SSC). (May 2015). PCI DSS Quick Reference Guide, v3.1, https://www.pcisecuritystandards.org/documents/PCIDSS_QRGv3_1.pdf

PCI SSC. (November 2013). PCI Payment Application Data Security Standard: Requirements and Security Assessment Procedures, v3.0. https://www.pcisecuritystandards.org/minisite/en/docs/PA-DSS_v3.pdf.

PCI SSC. For Merchants, https://www.pcisecuritystandards.org/merchants/index.php.

International Civil Aviation Organization (ICAO). The Assembly. (Accessed January 2018). https://www.icao.int/about-icao/assembly/Pages/default.aspx

ICAO. The Creation of the USAP. (Accessed January 2018). https://www.icao.int/Security/USAP/Pages/The-Creation-of-the-USAP.aspx. ICAO

ICAO. The ICAO Council. (Accessed January 2018). https://www.icao.int/about-icao/Council/Pages/council.aspx. ICAO

ICAO. The Air Navigation Commission. (Accessed January 2018). https://www.icao.int/about icao/AirNavigationCommission/Pages/default.aspx. ICAO

ICAO. USAP-CMA Activities. (Accessed January 2018). https://www.icao.int/Security/USAP/Pages/USAP-CMA-Activities.aspx. ICAO

ICAO. The USAP-CMA Audit Process. (Accessed January 2018). https://www.icao.int/Security/USAP/Pages/The-Audit-Process.aspx. ICAO

ICAO. How ICAO Develops Standards. (Accessed January 2018). https://www.icao.int/about-icao/AirNavigationCommission/Pages/how-icao-develops-standards.aspx. ICAO

ICAO. Funds, Programmes, Specialized Agencies and Others. (Accessed January 2018). http://www.un.org/en/sections/about-un/funds-programmes-specialized-agencies-and-others/. United Nations.

The Joint Commission, Facts about the Board of Commissioners, http://www.jointcommission.org/about_us/who_we_are.aspx.

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

Toll-Free “Help Line” 866-367-7487

www.its.dot.gov

FHWA-JPO-18-687

U.S. Department of Transportation