U.S. Department of Transportation

SECURITY CREDENTIAL MANAGEMENT SYSTEM STATUS

SIS54 - Establishing a Large-Scale Security Credential Management System for V2X Communication

Ray Resendes

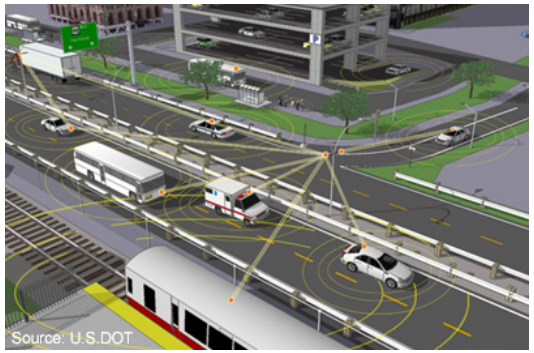
Volpe National Transportation Research Center

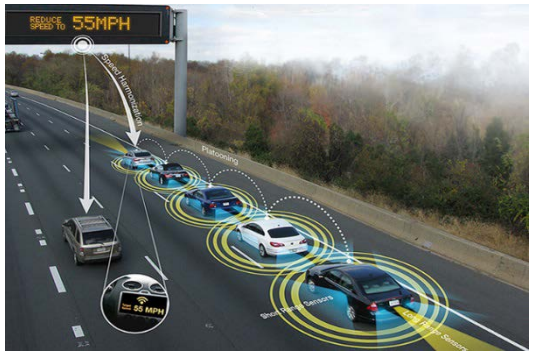
U.S. Department of Transportation

SEPTEMBER 19, 2018

Motivation for SCMS

Connected vehicles and infrastructure have the potential to transform the way Americans travel through the creation of a safe, interoperable wireless communications network.

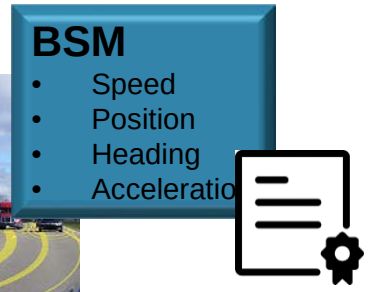




In order to realize the benefits of V2X applications, a **system must be in place that users can trust**.

Over-the-air messages must have:

- **Integrity**
- **Authenticity**
- **Privacy**



Where are we at with SCMS?

- **USDOT conducted early analysis and outreach efforts on how to deploy at scale**
- **Proof-of-Concept (PoC) was built and demonstrated**
- **Mostly done….but some missing technical elements**
  - Electors concept
  - Re-enrollment capability
  - Local and global misbehavior detection

- ***While the research was going on, commercial services have become available***

Why do we need a Full-Scale SCMS Model?

A full-scale SCMS is imperative to securing all types of communications for the V2X ecosystem

- To deploy and oversee the multifaceted SCMS, there must be a model or models to ensure effective governance and continued operations
- Without effective ownership and governance:

The SCMS could organically grow into a non-sustainable system with **varying levels of security and device enrollment** not meeting standard requirements

A lack of enforcement for policies and processes could create **varying security, privacy, and device standards across components.** This may result in **interoperability concerns, lack of confidence, and exploitable vulnerabilities**

There could be **inconsistent funding streams** that could lead to issues in availability and inconsistent services

Overall Project Approach

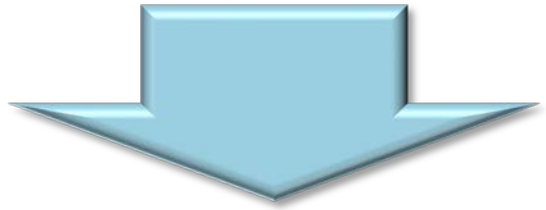
The Full-Scale SCMS Deployment Support project is intended to help identify and explore potential strategies for the establishment and governance of a broad SCMS ecosystem through stakeholder guidance and a feasibility assessment of these strategies

Ideally, outcomes will consist of next steps and milestones to implement the favored strategy or strategies

Review literature of other V2X trust models, and ownership & governance models

Solicit feedback and insights from stakeholders within the SCMS ecosystem

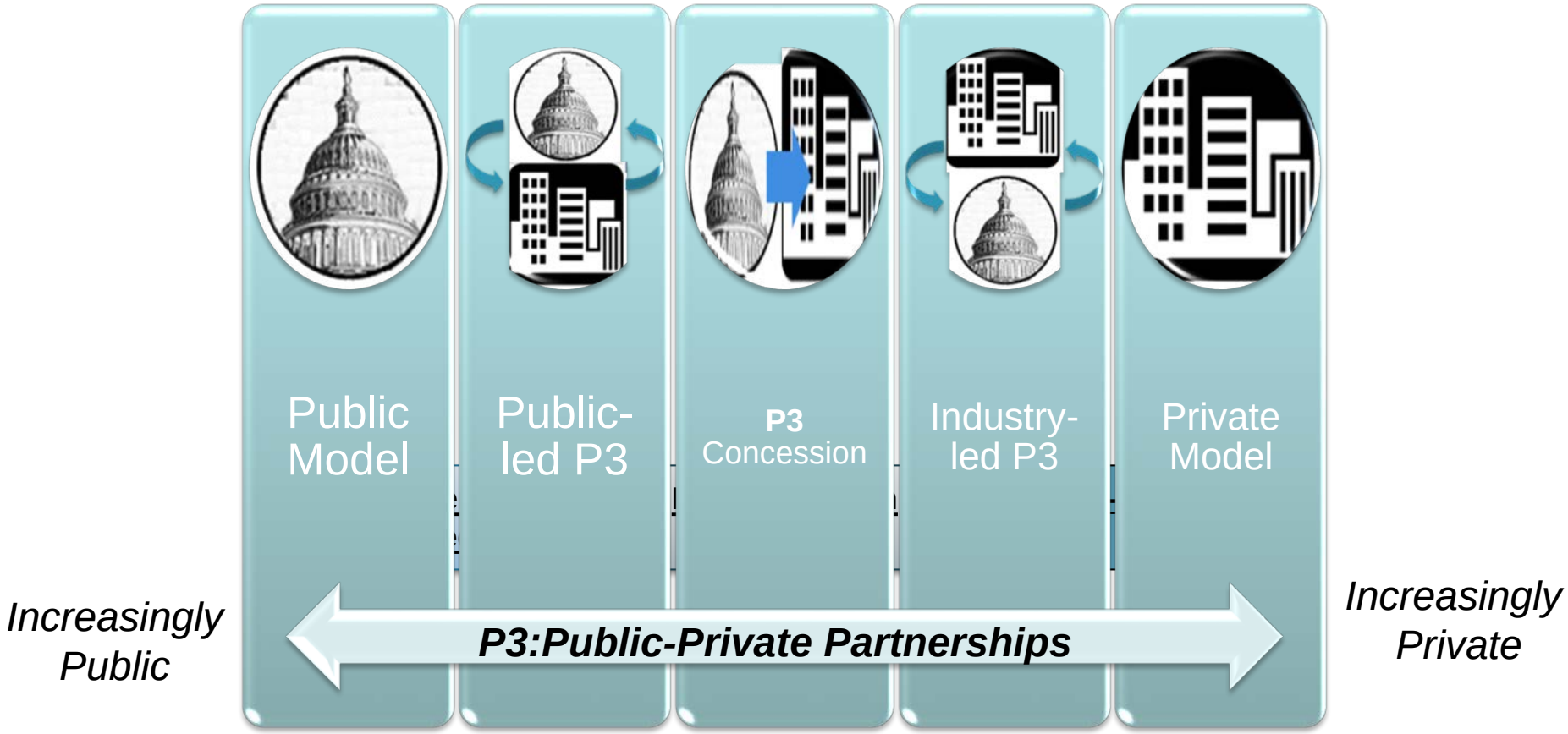
Conduct exercises to refine ownership & governance models and develop next steps



Suggest ownership and governance models, and next steps

Full-Scale SCMS Research

- USDOT needs to work with industry to facilitate the establishment of an organization that can lead the govern the national SCMS policies and procedures to provide secure and interoperable communications.



SCMS Model Ownership and Governance Attributes

SCMS Structure Attributes

- Initial Ownership
- Initial Funding
- SCMS Manager Sustainment Funding
- Technical Component Sustainment Funding
- Competition
- Legislation/Regulation

SCMS Manager Roles and Responsibilities Attributes

- Initial Policy Development
- Recurring Policy Development and Approval
- Oversight and Auditing
- Misbehavior Authority Management
- End Entity Certification
- Trust Anchor Management

Public Interest Objectives

Secure Communications – Privacy – Availability – Affordability – Performance – Stakeholder Representation

Stakeholder Groupings

SCMS IMPLEMENTERS INCLUDE:

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

SCMS USERS INCLUDE:

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

SCMS OTHER INTERESTED PARTIES INCLUDE:

- USDOT
- Academia
- Standards Organizations
- Advocacy Groups

Workshop Overview

- **Objectives**
  - Develop ownership and governance models
  - Understand stakeholder motivations, interests, concerns, and willingness to dedicate resources to deploy the National SCMS
  - Identify and describe additional challenges, risks, and opportunities to deploying and operating a functional and sustainable National SCMS

- **Research Results Published**
  - Literature Search
  - Ownership and Governance Models
  - Workshop Read Ahead Materials
  - Workshop Final Report

- **Logistics**
  - San Francisco, CA: September 11 – 12
  - McLean, VA: October 10 – 11

- **Participants**

Stakeholder Group	Stakeholder Sub-group
Implementers	Certification Services
	IT/Tech Companies
	OEMs
	PKI Security Services
	Telecommunications Companies
	Cybersecurity Firms
Other Interested Parties	Academia
	International
	Other PKI and Governance Organizations
	Trade Organizations
	Federal Government
Users	State/Local DOTs
	System Integrators
	V2X Equipment and Application Suppliers
Total	

Stay Connected

For more information, contact…

Ray Resendes

Volpe National Transportation Center
U.S. Department of Transportation
Raymond.Resendes@dot.gov

Kevin Gay

ITS Joint Program Office
U.S. Department of Transportation
Kevin.Gay@dot.gov

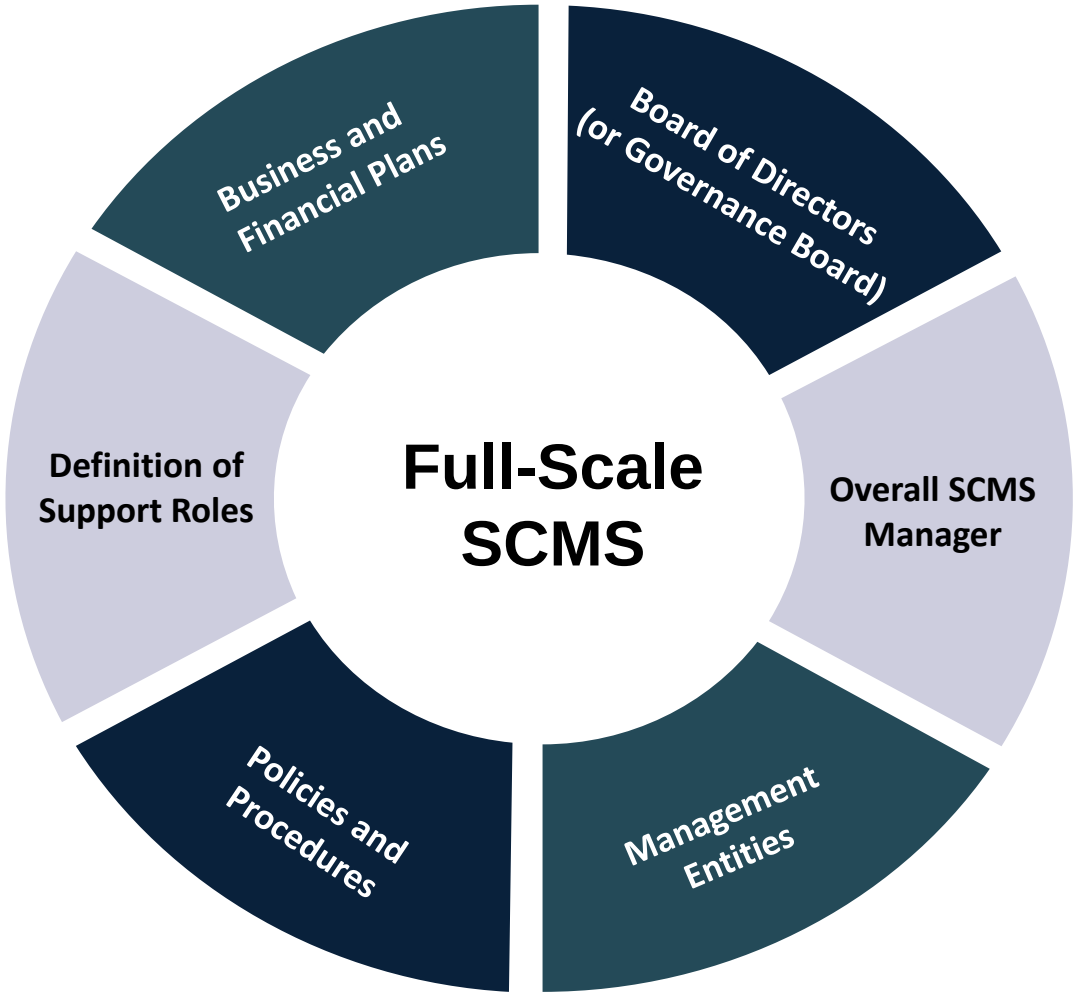
Robert Kreeb

National Highway Traffic Safety Administration
U.S. Department of Transportation
Robert.Kreeb@dot.gov

Website: http://www.its.dot.gov

Backup slides

Elements of a Full-Scale SCMS



Potential SCMS Manager Purpose and Responsibilities

The SCMS Manager is likely a centralized body responsible for setting certain standards and policies, and providing guidance and oversight to promote consistency and adherence to needed standards and practices throughout the V2X certificate management industry

- Develop industry-wide policies and standards that assure interoperability of technology and maintain security and privacy in Certificate Management Entity (CME) operations
- Set performance requirements for all V2X industry participants
- Enforce compliance with requirements, standards, and policies throughout the SCMS
- Assure open, informative, and consistent dissemination of information to all stakeholders
- Set rules and guidelines about ownership and operations of the CMEs, and how those owners/operators will interact with private companies that are part of the V2X industry