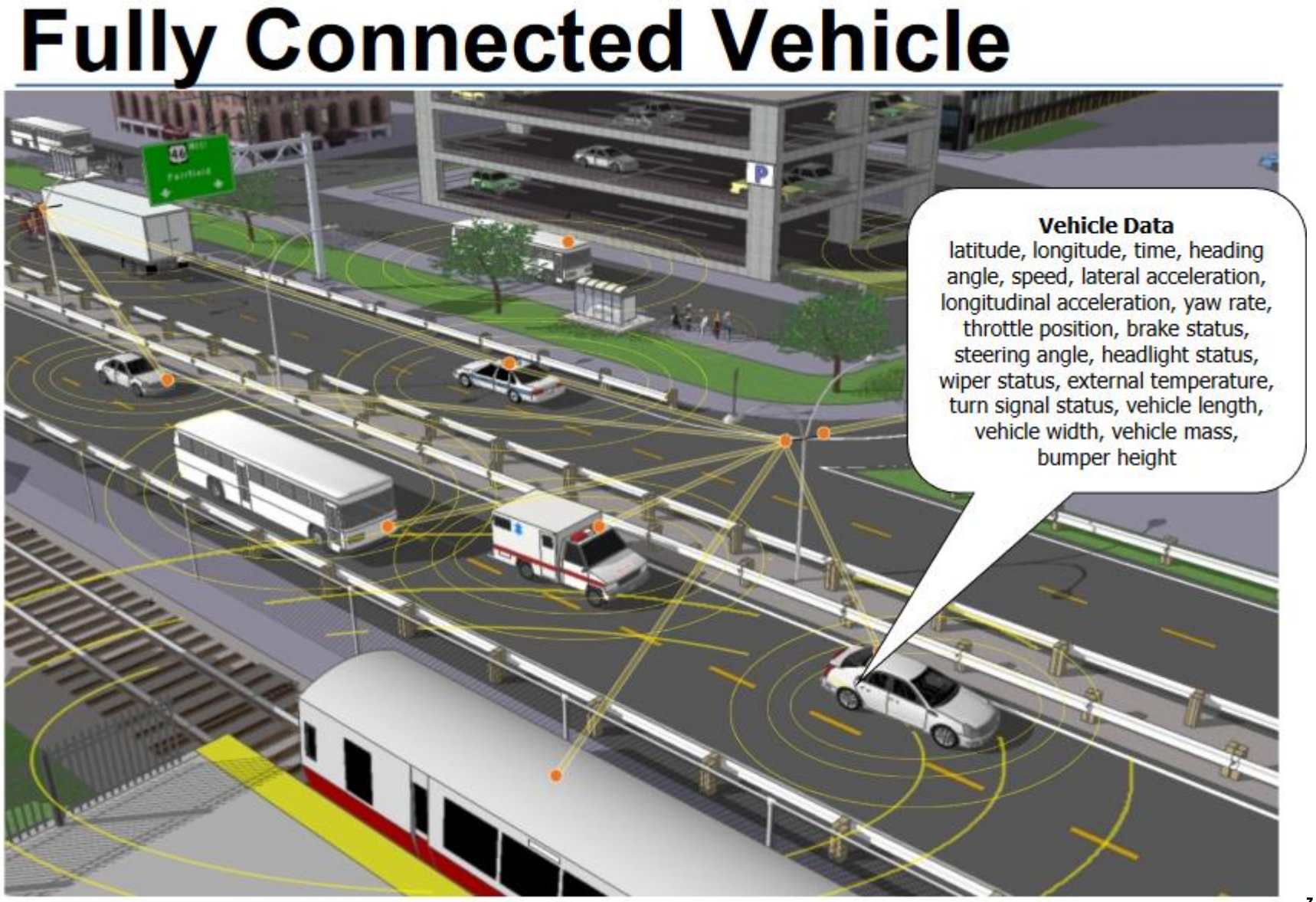
Software Technology Conference Tutorial – Part III

VPKI Hits the Highway – Evaluating the SCMS Deployment

Tim Weil – CISSP/CCSP, CISA, PMP
Alcohol Monitoring Systems
IEEE Senior Member
Member COMSOC, ITS Societies

NIST
Gaithersburg, MD
28 September 2017

US DOT Model


Fully Connected Vehicle
Vehicle Data
latitude, longitude, time, heading angle, speed, lateral acceleration, longitudinal acceleration, yaw rate, throttle position, brake status, steering angle, headlight status, wiper status, external temperature, turn signal status, vehicle length, vehicle width, vehicle mass, bumper height

Regulations.Gov – Industry Response to the FMVSS NPRM

https://www.regulations.gov/docketBrowser?rpp=50&so=DESC&sb=postedDate&po=50&s=SCMS&dct=PS&D=NHTSA-2016-0126

Sampling of Industry Response (1 of 5)

#	Responder	Organization Section	NPRM Opinion	Issues	Comments
					55 Comments specific to SCMS
NHTSA-2016-0126-0478	UL (Underwriters Laboratory)	Safety Certification Lab	Evaluate CMVP for ECDSA	Cryptography (FIPS 140-2)	NIST Guidance for ECIES/ECDSA/Tamper Proof Devices http://csrc.nist.gov/groups/STM/cmvp/
NHTSA-2016-0126-0477	R Street Institute	Government Lobbyist	Cost of DSRC Mandate	DSRC Spectrum Sharing	Emerging 5G standards benefits Neutral NHTSA Technology Position
NHTSA-2016-0126-0473	Lobby for Highway and Auto Safety	Consumer Advocacy	Support of FMVSS Mandate	Executive Order 13771	https://en.wikipedia.org/wiki/Executive_Order_13771
NHTSA-2016-0126-0468	LG Electronics	Manufacturer	Support of FMVSS Mandate	Align SCMS / BSM with NIST Guidance	Supports DSRC/LTE Hybrid Solution for BSM Crypto Alternatives to ECDSA for BSM Signing
NHTSA-2016-0126-0366	Omniair	DSRC / WAVE Certification Lab	Support of FMVSS Mandate	Require V2V Interoperability Certification	Deploy V2V DSRC Recommendation
NHTSA-2016-0126-0331	Qualcomm	Telecomm Manufacturer	Delay mandate subject to V2V technolgy evaluation	DSRC Spectrum Sharing Hybrid Wireless Solutions	Emerging 5G standards benefits Neutral NHTSA Technology Position
NHTSA-2016-0126-0340	Utah DOT	State Agency	Support of FMVSS Mandate	Expand BSM data elements Maintain federal oversight of SCMS	Expand V2V Guidance to freight and commercial vehicles
NHTSA-2016-0126-0448	Cisco	Telecom Industry	Support of FMVSS Mandate	Specify alternative message authentication requirements. CRL Management issues. Rotating pseudonym certs does not guarantee anonymity.	SCMS across multiple jurisdictions to be managed Certification process for SCMS VPKI Misbehavior detection and managing 'false positives'

Sampling of Industry Response (2 of 5)

#	Responder	Organization Section	NPRM Opinion	Issues	Comments
					55 Comments specific to SCMS
NHTSA-2016-0126-0446	Infineon Techologies Americas	Semiconductor Manufacturer	Consider alternative SCMS technologies to reduce complexity	Deviations from FIPS 140 standards (ECDSA signature vs CAVP). 1609.2 not on CAVP list. ECIES encryption not on CAVP list.	Security needs to be capable of withstanding twenty plus years of evolving attacks, and that resiliency will be dependent upon strong initial trust relationships established at vehicle production and issuance (sale).
NHTSA-2016-0126-0387	5G Americas	Trade Association	Delay mandate subject to V2V technolgy evaluation	DSRC technical limitations Hybrid Wireless Solutions	Cellular technologies (3GPP / LTE / 5G) better suited for V2X SCMS has managed to strike a good balance between these apparently conflicting requirements DSRC primarily focused on safety applications
HTSA-2016-0126-0314	Bosch	Automotive Manufacturer	Support of FMVSS	Message authentication load on OBU is prohibitive. Zeroization of secrets is required whenever the OBD detects that it enters a state where the secrets are likely to be more easily exposed.	Restricting the safety critical messages to a single channel would not provide sufficient bandwidth for the system's needs for in the future. However, misbehavior detection /integration is not complete in the SCMS system and a thorough risk assessment of the SCMS system
NHTSA-2016-0126-0412	General Motors	Automotive Manufacturer	Support of FMVSS. PKI specified in the proposed rules, with an enterprise chain of trust, is the best authentication method for BSM messages	Maintain federal oversight of SCMS Reduce SCMS elements to be stored in secured memory	Does not support a mandate of specific safety applications at this time. Issuing new certificates, providing updates, misbehavior reporting and managing certificate revocation lists (CRLs) together have the potential to represent a significant portion of V2V costs

Sampling of Industry Response (3 of 5)

#	Responder	Organization Section	NPRM Opinion	Issues	Comments
					55 Comments specific to SCMS
NHTSA-2016-0126-0363	Delphi	Automotive Manufacturer	Support of FMVSS SCMS Privacy protection is sufficient	No other known alternatives exists that meet the V2v safety critical performance requirements, OEM rapid deployment needs, nor NHTSA's US deployment readiness milestones	Clarification requested - Initialization time A DSRC device must begin transmitting the BSM within 2 seconds
NHTSA-2016-0126-0322	American Association for Justice	Trial Lawyer advocacy and lobbying association	Delay mandate subject to consumer acceptance and definable SCMS Liability issues	We urge NHTSA to reject any liability-limiting options and instead to preserve common law causes of action and the civil jury system, which is the only appropriate forum for sorting out any causation issues associated with V2V-related collisions	The agency fails to address potential victims in V2V-related accidents. If such liability-limiting options were pursued, NHTSA would be prioritizing simplicity in process over the concerns and safety of individuals
NHTSA-2016-0126-0367	Security Innovations	Aerolink Software Manufacturer	Support of FMVSS	Multiple technical deficiencies cited in the FMVSS NPRM (eg FMVSS does not adequately specify system interoperability (communication stack)	Security Innovation recommends that the regulation provides specific security requirements and makes it clear that formal FIPS certification is not necessary. Security Innovation staff have been the editor of IEEE 1609.2 and have contributed to SCMS design projects. Our software ran on over half of the vehicles in the Safety Pilot Model Deployment. We have been tracking the development of this technology since 2003 and believe that the time is right to mandate its deployment

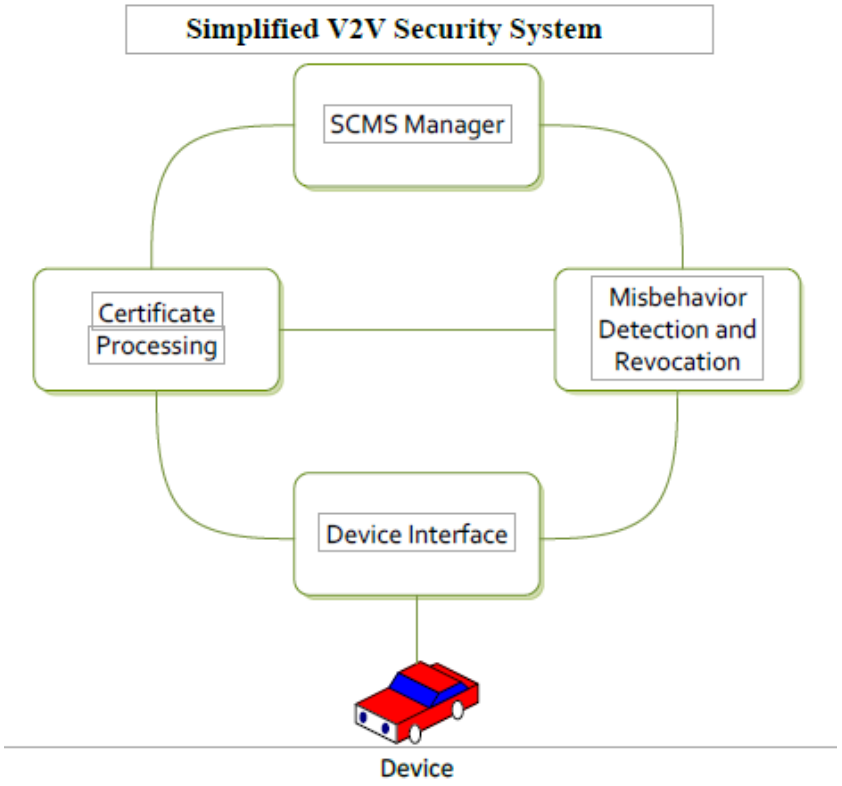
Sampling of Industry Response (4 of 5)

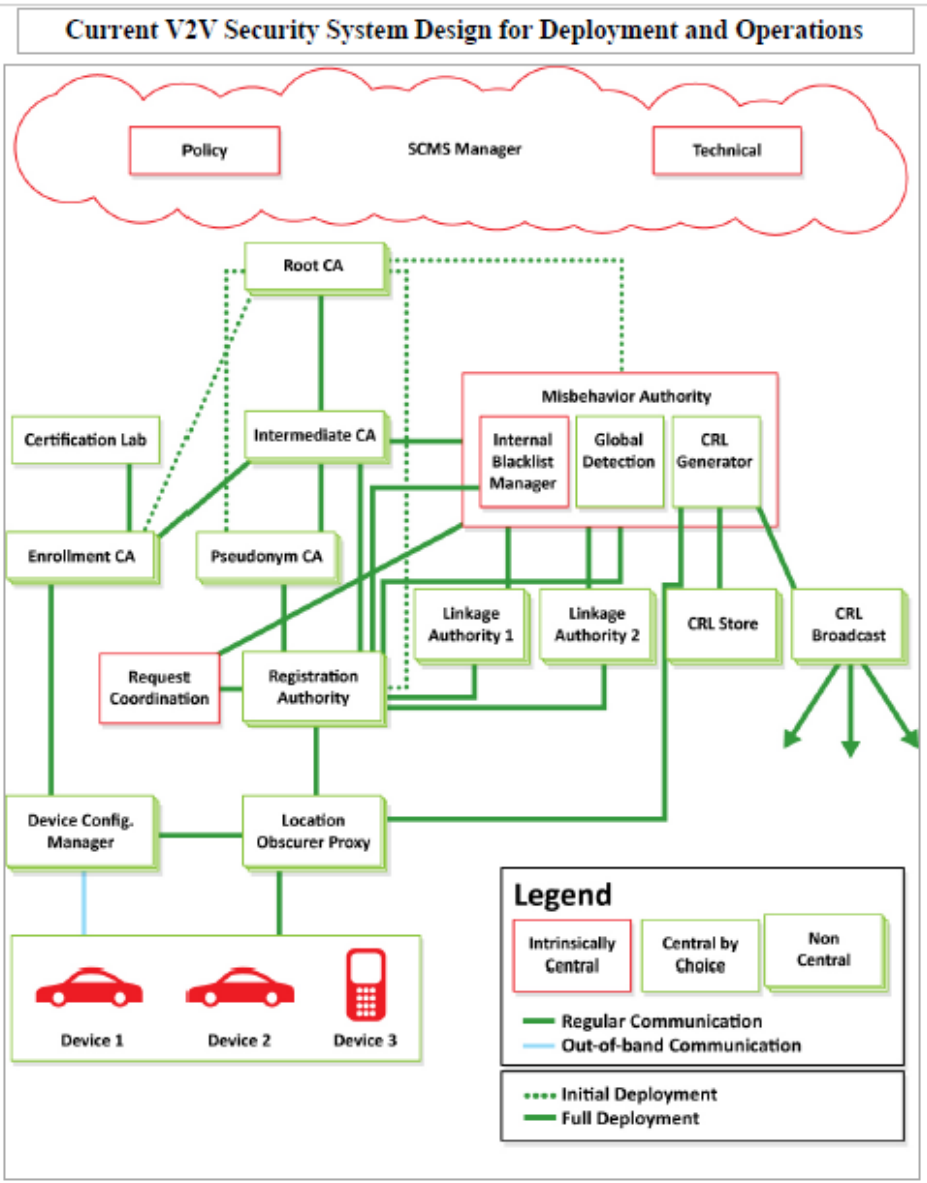
#	Responder	Organization Section	NPRM Opinion	Issues	Comments
					55 Comments specific to SCMS
NHTSA-2016-0126-0117	Secure|Set Academy	Cybersecurity Education and Training	Consider alternative SCMS technologies to mitigate threats and vulnerabilities	DSRC / WAVE Threat model introduces vulnerabilities in vehicle systems posing unnecessary privacy, security, and safety risks to the public at large.	Recommends that NHTSA require the establishment of an industry-developed automotive security standard or compliance framework. GSMA, IOActive, Bosch, Lab Mouse Security, I Am The Cavalry have provided frameworks that can be adopted to mitigate vulnerabilities and protect consumers
NHTSA-2016-0126-0338	AT&T	Telecommunications Services	Support of FMVSS	Demonstrated interoperability with Delphi, Ford and Consumer Electronics Show (CES) SCMS governance, technical, and administrative functions can and should be performed by private sector actors, in coordination with NHTSA and other appropriate government stakeholders	SCMS contemplated by NHTSA is supportable and deployable, and NHTSA's SMCS Proof-of-Concept (SCMS PoC) will provide a good mechanism for exploring and developing acceptable solutions to the remaining implementation challenges
NHTSA-2016-0126-0355	IEEE 1609 Working Group	Standards Body	Support of FMVSS	SCMS is out of scope for this reply.	NPRM should directly address IEEE 802.11, IEEE 1609, SAE DSRC standards in these specification area - Interoperability and standards, Alternative technologies, Security and Other Benefits
State of Dedicated Short Range Radio Communications Report	25 respondents to the NHTSA FMVSS NPRM	Multiple stakeholder	Comments mostly derived from DSRC vs hybrid cellular solutions	Summary comments given as examples	CTIA encourages NHTSA to leverage authentication technology from commercial wireless services to secure the SCMS Alliance of Automobile Manufacturers in its comments also calls for federal leadership in creating and managing the SCMS for connected cars

Sampling of Industry Response (4 of 5)

#	Responder	Organization Section	NPRM Opinion	Issues	Comments
					55 Comments specific to SCMS
NHTSA-2016-0126-0384	Electronic Frontier Foundation	Consumer Advocacy Lobby	Opposes FMVSS		(1) The proposal tries unsuccessfully to mitigate the privacy risk presented by V2V and will not prevent vehicle tracking; (2) The proposed application of a Public Key Infrastructure (PKI) is unduly complicated and will create potentially dangerous misconceptions regarding whether the contents of basic safety messages (BSMs) are "safe" and to be trusted; (3) The proposal fails to address the serious security concerns presented by V2V— leaving drivers and passengers at potentially grave risk; and (4) The proposal is inefficient from a common sense, cost-benefit perspective; the technology is expensive and, if implemented, will be outpaced by other communications technology by the time it is fully deployed.

Introducing the Security Credential Management Systems (VPKI)





This image presents both an initial deployment model as well as a full deployment model. Note that this diagram shows the initial deployment model where there is no Intermediate CA and the Root CA talks to the MA, PCA, and ECA (dotted lines). In the full deployment model, these entities communicate with the Intermediate CA instead of the Root CA to protect the Root CA from unnecessary exposure (solid line)

[1] W. Whyte, A. Weimerskirch et al, Crash Avoidance Metrics Partnership, Technical Design of the Security Credential Management System (Final Report),

SCMS Component Functions –

A security credential management system for V2V communications, William Whyte (et al)

Concepts	Purpose
Pseudonym Functions / Certificate	A short-term digital certificates used by a vehicle's on-board equipment to authenticate and validate sent and received basic safety messages that form the foundation for V2V safety technologies. These short-term certificates contain no information about users to protect privacy, but serve as credentials that permit users to participate in the V2V
Intermediate CA	Authorize other Certificate Management Entities (CMEs) (or possibly an Enrollment Certificate Authority [ECA]) using authority from the Root CA, but does not hold the same authority as the Root CA in that it cannot self-sign a certificate.
Linkage Authority	The linkage values provide the PCA with a means to calculate a certificate ID and a mechanism to connect all short-term certificates from a specific device for ease of revocation in the event of misbehavior
Location Obscure Proxy (LOP)	Obscures the location of OBE seeking to communicate with the SCMS functions, so that the functions are not aware of the geographic location of a specific vehicle. All communications from the OBE to the SCMS components must pass through the LOP.
Misbehavior Authority	The MA acts as the central function to process misbehavior reports and produce and publish the certificate revocation list. It works with the PCA, RA, and LAs to acquire necessary information about a certificate to create entries to the CRL through the CRL Generator.
Pseudonym Certificate Authority	PCA Issues the short-term certificates used to ensure trust in the system. In earlier designs their lifetime was fixed at five minutes. The validity period of certificates is still on the order of "minutes" but is now a variable length of time, making them less predictable and thus harder to track.
Registration Authority	The RA performs the necessary key expansions before the PCA performs the final key expansion functions. It receives certificate requests from the OBE (by way of the LOP), requests and receives linkage values from the LAs, and sends certificate requests to the PCA
Root Certificate Authority	The ROOT CA - master root for all other CAs; it is the "center of trust" of the system. It issues certificates to subordinate CAs in a hierarchical fashion, providing their authentication within the system so all other users and functions know they can be trusted. The Root CA produces a self-signed certificate (verifying its own trustworthiness) using out-of-band communications
SCMS Manager	Management and Control functions that will provide the policy and technical standards for the entire connected vehicle industry. Just as any large-scale industry ensures consistency and standardization of technical specifications, standard operating procedures, and other industry-wide practices such as auditing

What If – SCMS Functional Requirements for all use cases are met?

https://wiki.campllc.org/display/SCP/Requirements+by+Use+Case

To support implemented from an end entities (EE) perspective to fulfill a major feature of the SCMS. A use case might comprehend multiple steps from a system's architecture perspective that can be run without interference with each other to return a partial result of the overall use case. In general, steps need to be executed in the given order to fulfill the use case. For example, Use Case 3: OBE Pseudonym Certificates Provisioning describes all necessary processes to equip an OBE with pseudonym certificates. It comprehends five steps that are coherent but self-contained:

Step 3.1: Request for Pseudonym Certificates
Step 3.2: Pseudonym Certificate Generation
Step 3.3: Initial Download of Pseudonym Certificates
Step 3.4: Schedule Generation of Subsequent Batch of Pseudonym Certificates
Step 3.5: Top-off Pseudonym Certificates

OBE Use Cases
The following chapters are about OBE requirements. These are the main use cases for OBEs, but there are requirements throughout all chapters for 11. Backend Management are requirements about what an OBE needs to do if a root CA is revoked or a new root CA is introduced to the system.
Use Case 2: OBE Bootstrapping (Manual)
Use Case 3: OBE Pseudonym Certificates Provisioning
Use Case 8: OBE Pseudonym Certificate Revocation
Use Case 19: OBE Identification Certificate Provisioning

RSE Use Cases
The following chapters are about RSE requirements. These are the main use cases for RSEs, but there are requirements throughout all chapters for 11. Backend Management are requirements about what an RSE needs to do if a root CA is revoked or a new root CA is introduced to the system.
Use Case 12: RSE Bootstrapping (Manual)
Use Case 13: RSE Application Certificate Provisioning
Use Case 16: RSE Application and OBE Identification Certificate Revocation

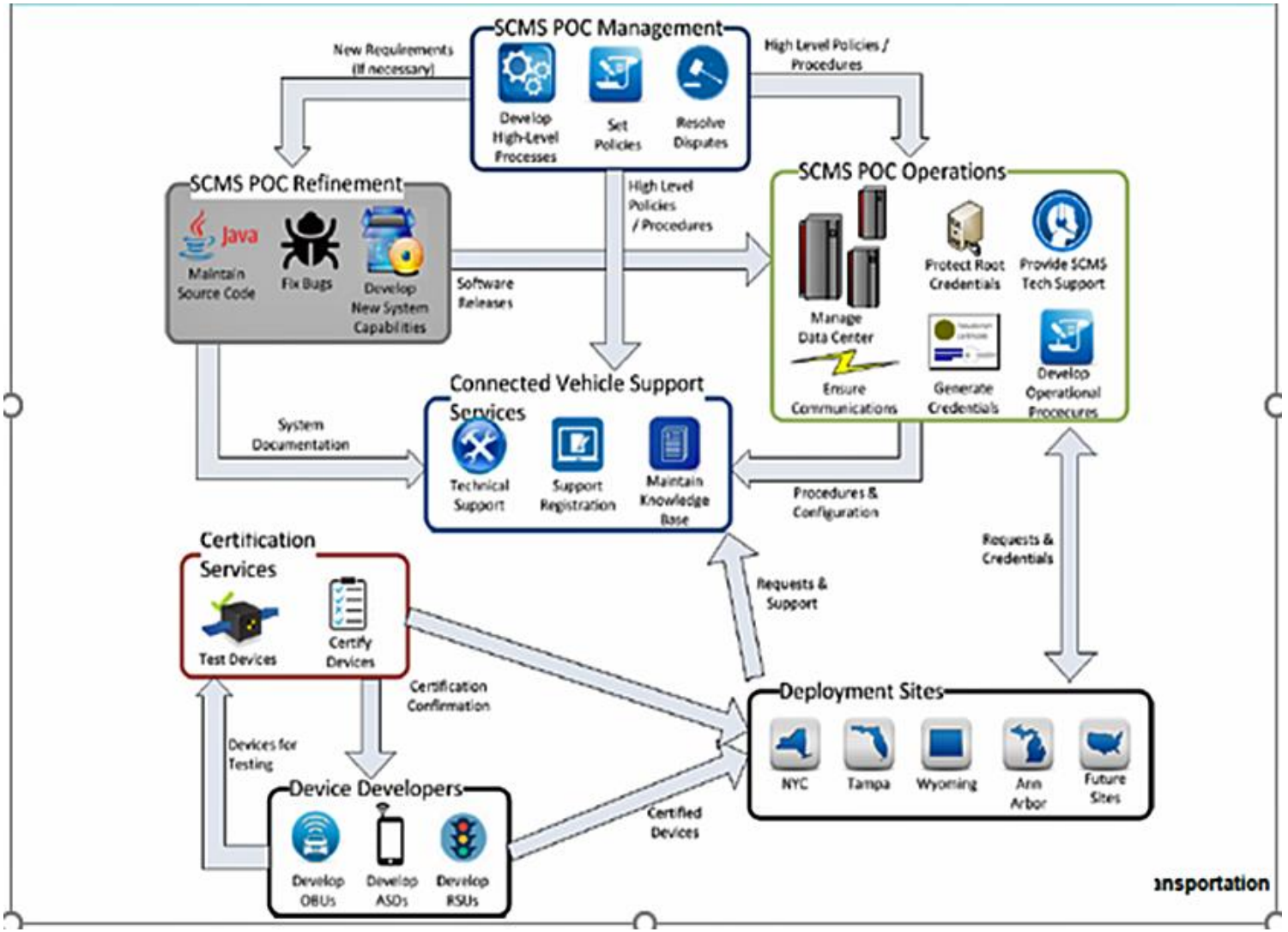
Common EE Use Casesth EE types should implement the following chapters:
Use Case 5: Misbehavior Reporting
Use Case 6: CRL Download
Use Case 11: Backend Management (CA compromise recover strategy)

Use Case 18: Provide and Enforce Technical Policies
Use Case 20: EE Re-Enrollment

What do SCMS Management and Operations Look Like?

https://www.its.dot.gov/pilots/pdf/TechAssistWebinar_Template_SCMSIIv4.pdf

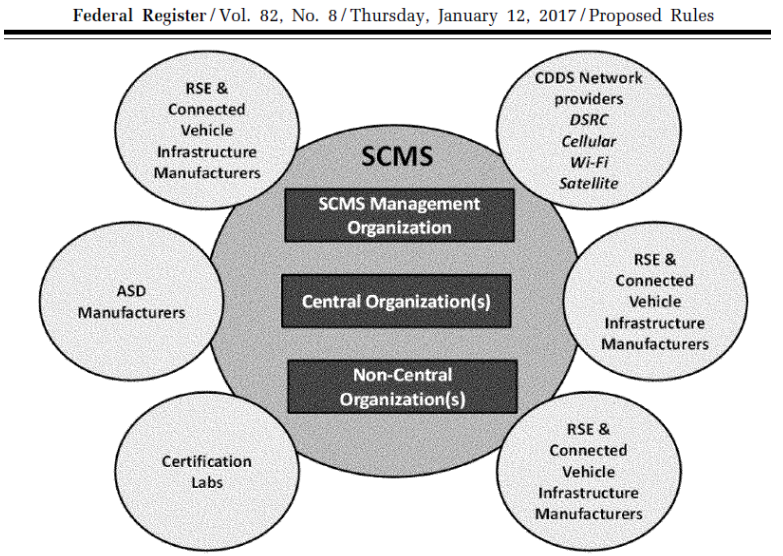
.



What If – Models for Industry Self Regulation (Risk Models)?

In analyzing SCMS governance options, NHTSA and its research partners have investigated a variety of industries with characteristics similar to those seen as critical for a V2V SCMS governance model, including security, privacy protection, stability, sustainability, multi-stakeholder representation and technical complexity. How risk was managed in the context these models. Some of the industries researched included:

- Internet Corporation for Assigned Names and Numbers (ICANN)
- DTE Energy Company
- Aeronautical Radio Incorporated (ARINC)
- End of Life Vehicle Solutions Corporation (ELVS)
- The FAA's Next Gen Air Transportation System
- The FRA's Positive Train Control
- Smart Grid
- The Rail/Transit Train Control Systems (ATC and CBTC)
- Medical Devices failure and liability
- Security in nuclear industry and liability
- Warning/Signal Failures
- UAVs
- HIPAA/Health Care industry/
- Electronic Health Records (EHRs)
- CONNECT system

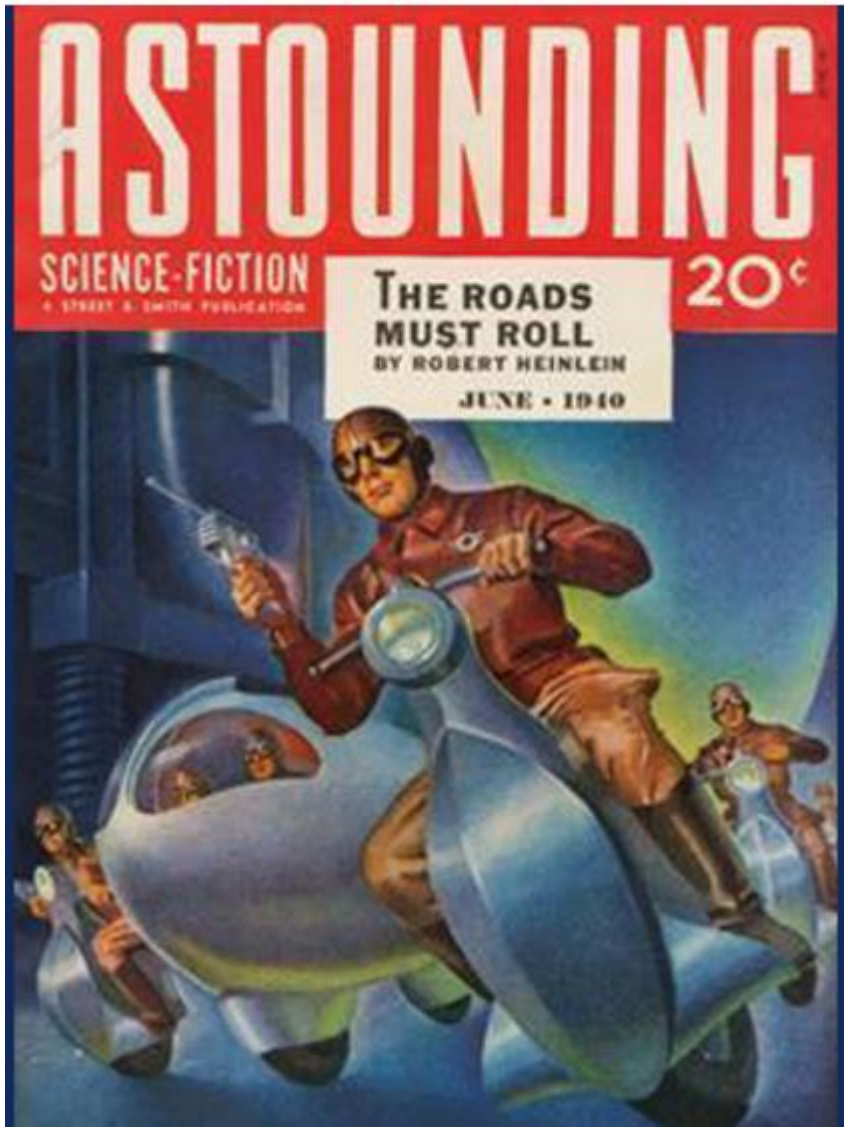


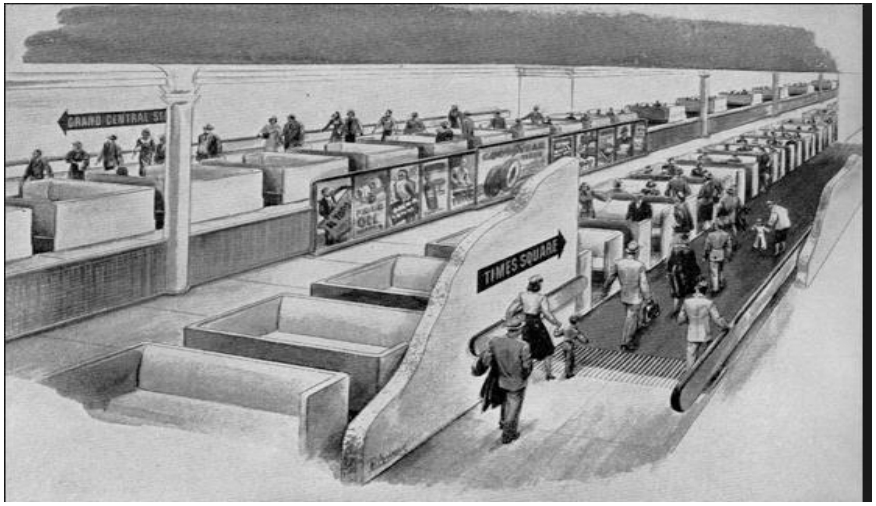
** National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT) Notice of Proposed Rulemaking, '*Federal Motor Vehicle Safety Standard (FMVSS), No. 150, to mandate vehicle-to-vehicle (V2V) communications for new light vehicles and to standardize the message and format of V2V transmissions*', Federal Register Vol 82, No 87, Jan 12, 2017,

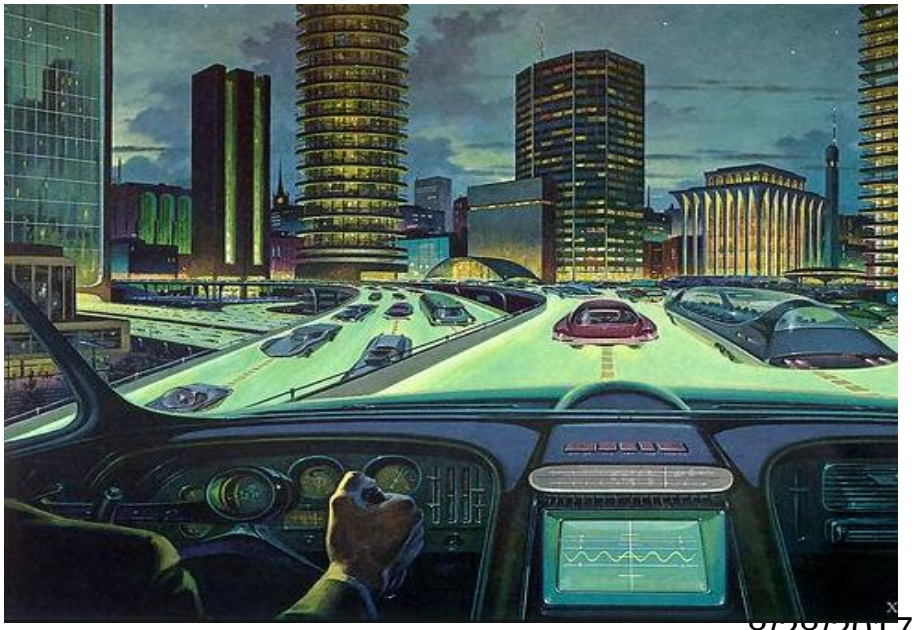
Thank you for joining us!

Security for Vehicular Networks Website - http://securityfeeds.com/dwd.html

The Roads Must Roll – Robert Heinlein







References Used in This Presentation

- T.Weil, VPKI Hits the Highway: Security Communication for the Connected Vehicle Program, IT Professional Magazine, Volume 19, Issue 1, January 2017
- National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT) Notice of Proposed Rulemaking, '*Federal Motor Vehicle Safety Standard (FMVSS), No. 150, to mandate vehicle-to-vehicle (V2V) communications for new light vehicles and to standardize the message and format of V2V transmissions*', Federal Register Vol 82, No 87, Jan 12, 2017, online available at - https://www.federalregister.gov/documents/2017/01/12/2016-31059/federal-motor-vehicle-safety-standards-v2v-communications
- W. Whyte, A. Weimerskirch et al, Crash Avoidance Metrics Partnership, Technical Design of the Security Credential Management System (Final Report), Cooperative Agreement Number DTFH61-05-H-01277, July 31, 2014 online available at - https://www.regulations.gov/contentStreamer?documentId=NHTSA-2015-0060-0004&attachmentNumber=2&contentType=pdf
- Harding, J., Powell, G., R., Yoon, R., Fikentscher, J., Doyle, C., Sade, D., Lukuc, M., Simons, J., & Wang, J. (2014, August). *Vehicle-to-vehicle communications: Readiness of V2V technology for application.* (Report No. DOT HS 812 014). Washington, DC: National Highway Traffic Safety Administration, online available - https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/readiness-of-v2v-technology-for-application-812014.pdf
- W. Whyte et al., "A Security Credential Management System for V2V Communications," Proc. IEEE Vehicular Networking Conf. (VNC), 2013 https://www.researchgate.net/publication/271554151_A_security_credential_management_system_for_V2V_communications
- Security Credential Management System (SCMS) Connected Vehicle Pilot Documentation, Crash Avoidance Metrics Partnership (CAMP) Wiki - https://wiki.campllc.org/display/SCP
- Regulations.Gov – Industry Response to the FMVSS NPRM https://www.regulations.gov/docketBrowser?rpp=50&so=DESC&sb=postedDate&po=50&s=SCMS&dct=PS&D=NHTSA-2016-0126