Software Technology Conference Tutorial – Part II

VPKI Hits the Highway – Security and Privacy Models

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

NIST
Gaithersburg, MD
25 September 2017

Objectives of this Presentation

Testbeds and Pilot Programs

-- Overview of C-ITS and SCMS Field Operation Trials (FOT) – EU & US

-- EU PRESERVE Security Model

-- Introduction to US DOT Enterprise Security Architecture for Connected Car Pilots

--**Security and Privacy Threat Models for Connected Car / C-ITS**

-- Secure Vehicular Systems – categorizing the threats

-- Scope of Privacy Research for Connected Car

-- Privacy Threat Examples and Response (Privacy Impact Assessment)

Wireless Access for Vehicular Environments (IEEE 1609 Standard)

-- Overview of the technical standards (1609.0/2/3/4)

-- WAVE Topics in Connected Car Security and Privacy

SCMS Implementation Details

-- The research and operations reports

-- V2V Requirements from the NHTSA Notice of Proposed Rule

Security the Basic Safety Message

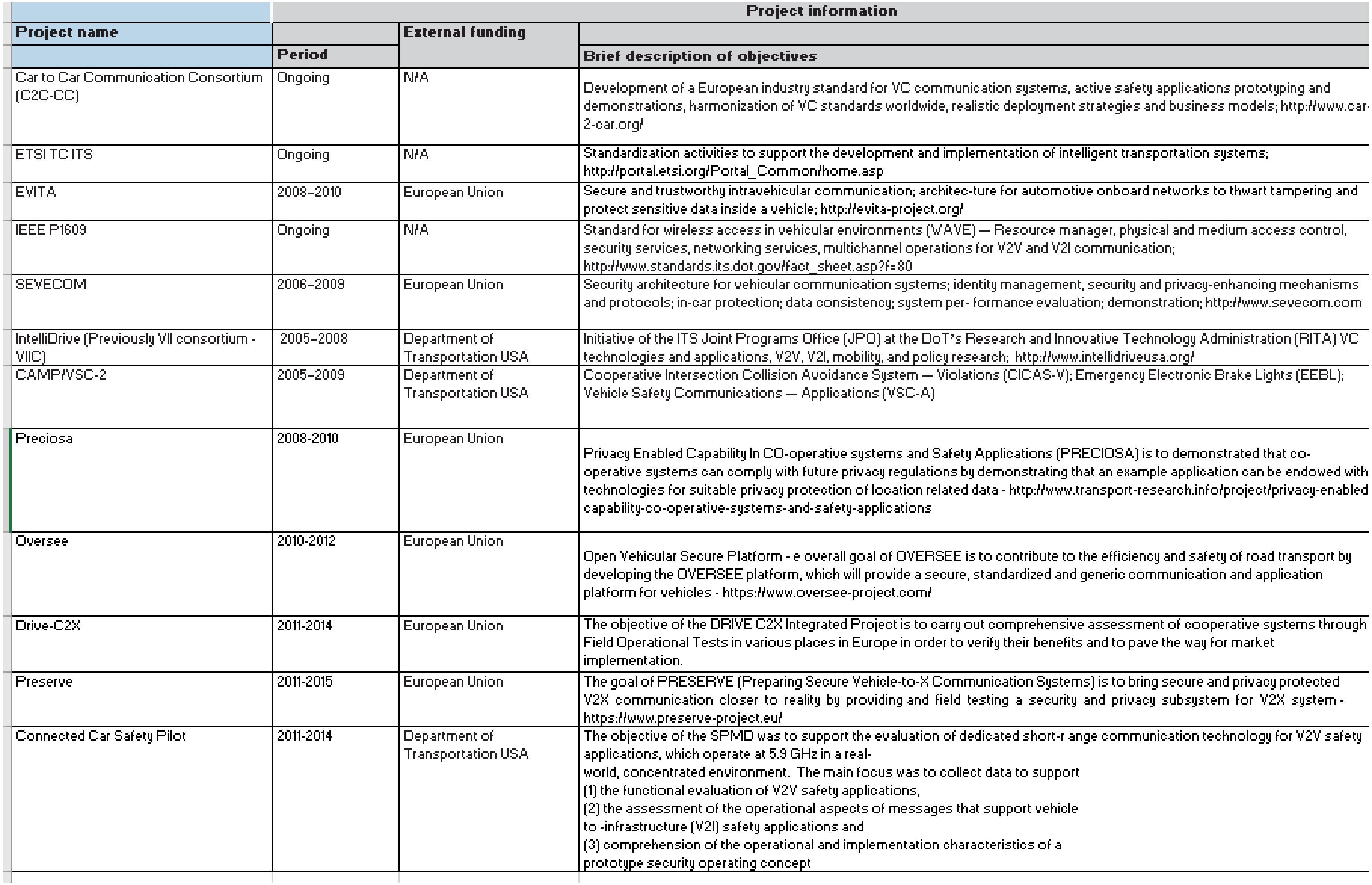
-- BSM Requirements Definition

-- BSM Security and Privacy Design and Analysis

Table of Contents

- Testbed and Pilot Programs (2004-2017)
- Evolving the Security and Privacy Model for Connected Car
- Wireless Access for Vehicular Environments (WAVE) Standard
- Secure Credential Management System (SCMS Implementation Details)
- Securing the Basic Safety Message (BSM)

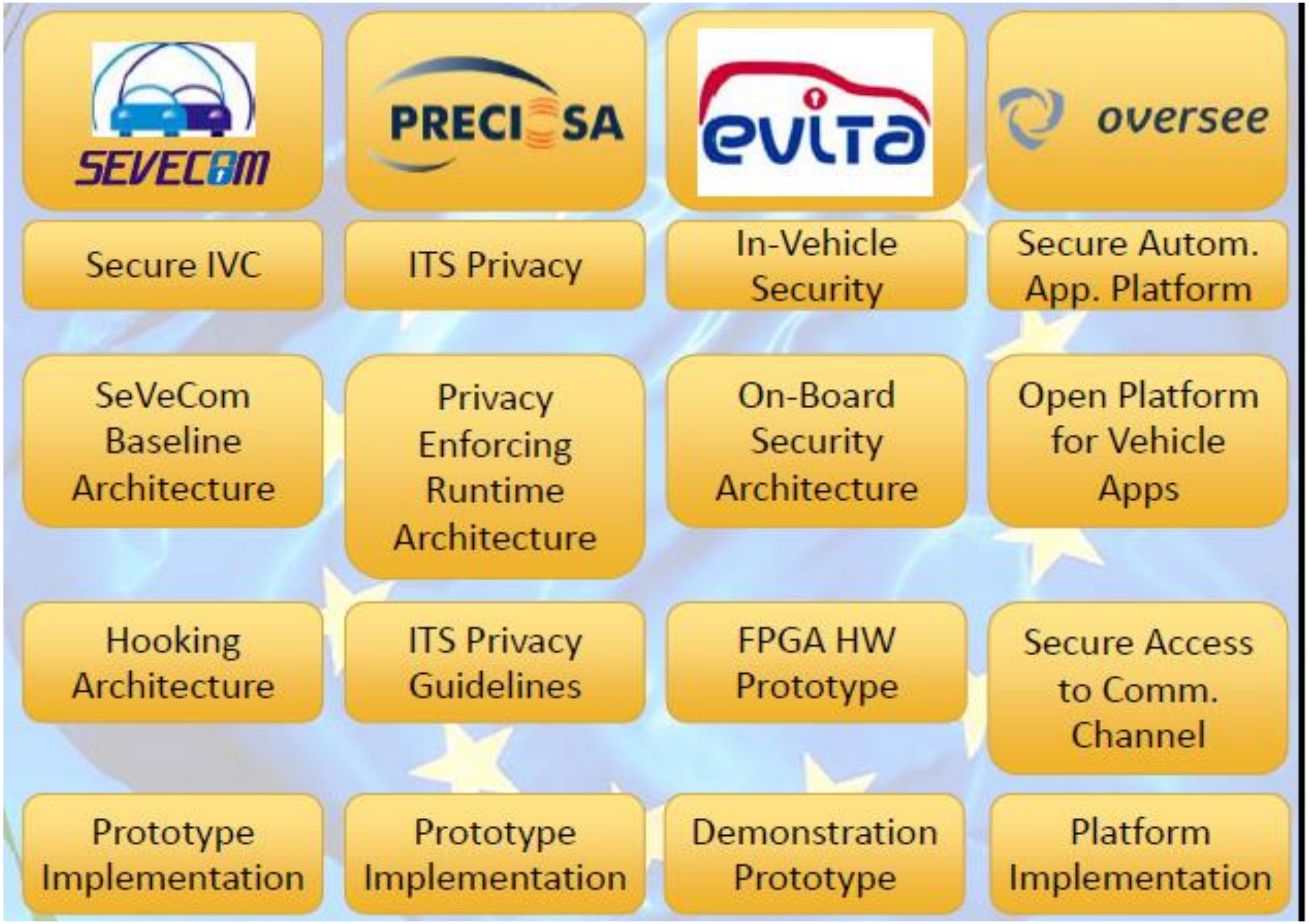
Representative VC projects, consortia, and working groups related to V-PKI



	Project information		
Project name		External funding	
	Period		Brief description of objectives
Car to Car Communication Consortium (C2C-CC)	Ongoing	N/A	Development of a European industry standard for VC communication systems, active safety applications prototyping and demonstrations, harmonization of VC standards worldwide, realistic deployment strategies and business models; http://www.car-2-car.org/
ETSI TC ITS	Ongoing	N/A	Standardization activities to support the development and implementation of intelligent transportation systems; http://portal.etsi.org/Portal_Common/home.asp
EVITA	2008–2010	European Union	Secure and trustworthy intravehicular communication; architec-ture for automotive onboard networks to thwart tampering and protect sensitive data inside a vehicle; http://evita-project.org/
IEEE P1609	Ongoing	N/A	Standard for wireless access in vehicular environments (WAVE) — Resource manager, physical and medium access control, security services, networking services, multichannel operations for V2V and V2I communication; http://www.standards.its.dot.gov/fact_sheet.asp?f=80
SEVECOM	2006–2009	European Union	Security architecture for vehicular communication systems; identity management, security and privacy-enhancing mechanisms and protocols; in-car protection; data consistency; system per- formance evaluation; demonstration; http://www.sevecom.com
IntelliDrive (Previously VII consortium - VIIC)	2005–2008	Department of Transportation USA	Initiative of the ITS Joint Programs Office (JPO) at the DoT's Research and Innovative Technology Administration (RITA) VC technologies and applications, V2V, V2I, mobility, and policy research; http://www.intellidriveusa.org/
CAMP/VSC-2	2005–2009	Department of Transportation USA	Cooperative Intersection Collision Avoidance System — Violations (CICAS-V); Emergency Electronic Brake Lights (EEBL); Vehicle Safety Communications — Applications (VSC-A)
Preciosa	2008-2010	European Union	Privacy Enabled Capability In CO-operative systems and Safety Applications (PRECIOSA) is to demonstrated that co-operative systems can comply with future privacy regulations by demonstrating that an example application can be endowed with technologies for suitable privacy protection of location related data - http://www.transport-research.info/project/privacy-enabled capability-co-operative-systems-and-safety-applications
Oversee	2010-2012	European Union	Open Vehicular Secure Platform - e overall goal of OVERSEE is to contribute to the efficiency and safety of road transport by developing the OVERSEE platform, which will provide a secure, standardized and generic communication and application platform for vehicles - https://www.oversee-project.com/
Drive-C2X	2011-2014	European Union	The objective of the DRIVE C2X Integrated Project is to carry out comprehensive assessment of cooperative systems through Field Operational Tests in various places in Europe in order to verify their benefits and to pave the way for market implementation.
Preserve	2011-2015	European Union	The goal of PRESERVE (Preparing Secure Vehicle-to-X Communication Systems) is to bring secure and privacy protected V2X communication closer to reality by providing and field testing a security and privacy subsystem for V2X system - https://www.preserve-project.eu/
Connected Car Safety Pilot	2011-2014	Department of Transportation USA	The objective of the SPMD was to support the evaluation of dedicated short-r ange communication technology for V2V safety applications, which operate at 5.9 GHz in a real-world, concentrated environment. The main focus was to collect data to support (1) the functional evaluation of V2V safety applications, (2) the assessment of the operational aspects of messages that support vehicle to -infrastructure (V2I) safety applications and (3) comprehension of the operational and implementation characteristics of a prototype security operating concept

1). P Papadimitratos, et al , “Vehicular communication systems: Enabling Technologies, Applications, IEEE Communications Magazine, Nov 2009 ,

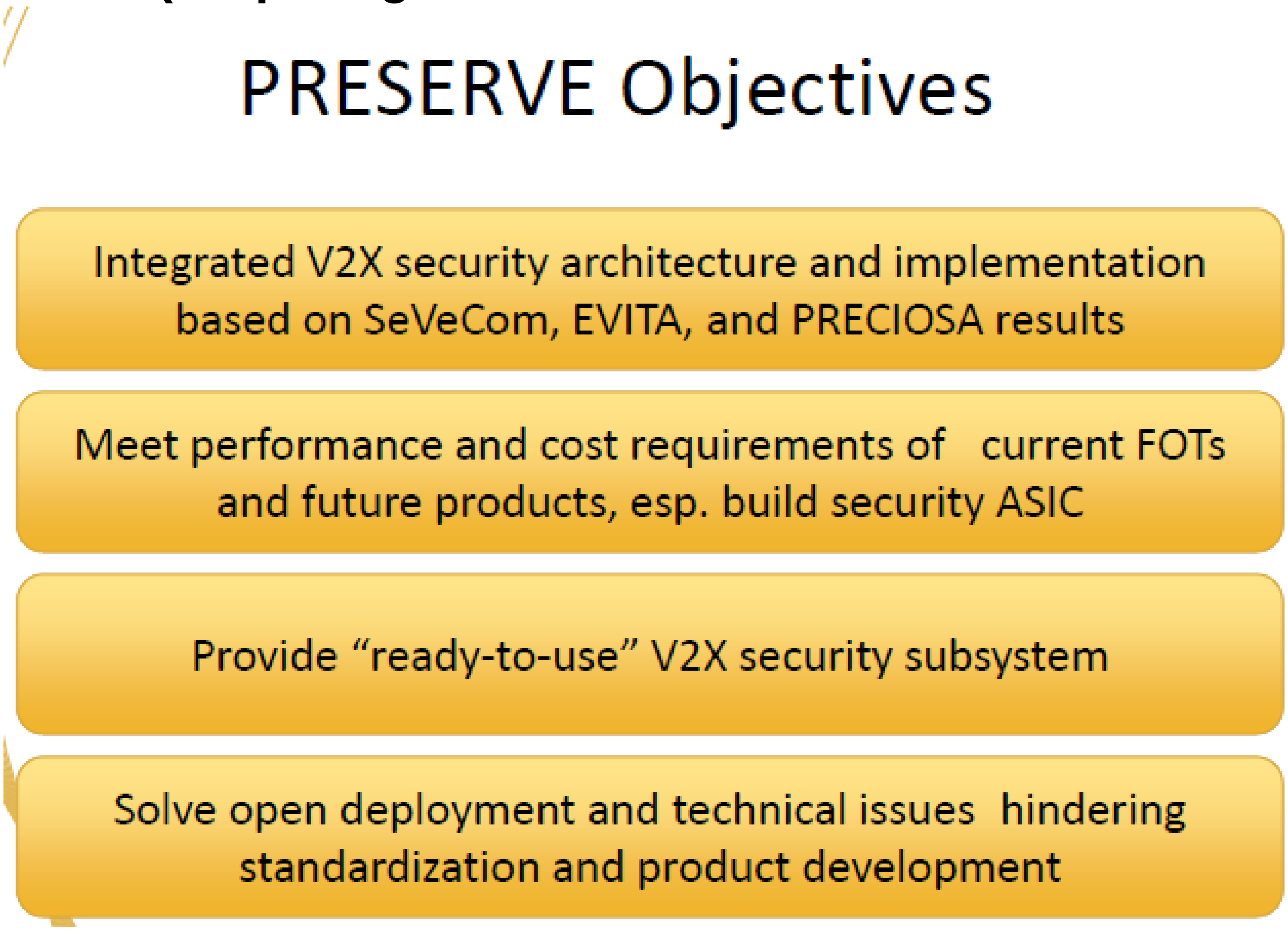
Recent EU ITS Security and Privacy Related Projects



SEVECOM	PRECIOSA	evita	oversee
Secure IVC	ITS Privacy	In-Vehicle Security	Secure Autom. App. Platform
SeVeCom Baseline Architecture	Privacy Enforcing Runtime Architecture	On-Board Security Architecture	Open Platform for Vehicle Apps
Hooking Architecture	ITS Privacy Guidelines	FPGA HW Prototype	Secure Access to Comm. Channel
Prototype Implementation	Prototype Implementation	Demonstration Prototype	Platform Implementation

1) P. Papadimitratos, PRESERVE Overview, WC3 Meeting, Jan 2011 - https://www.w3.org/wiki/images/1/11/PRESERVE-Overview.pdf

PRESERVE (Preparing Secure Vehicle-to-X Communication Systems)



PRESERVE Objectives

Integrated V2X security architecture and implementation based on SeVeCom, EVITA, and PRECIOSA results

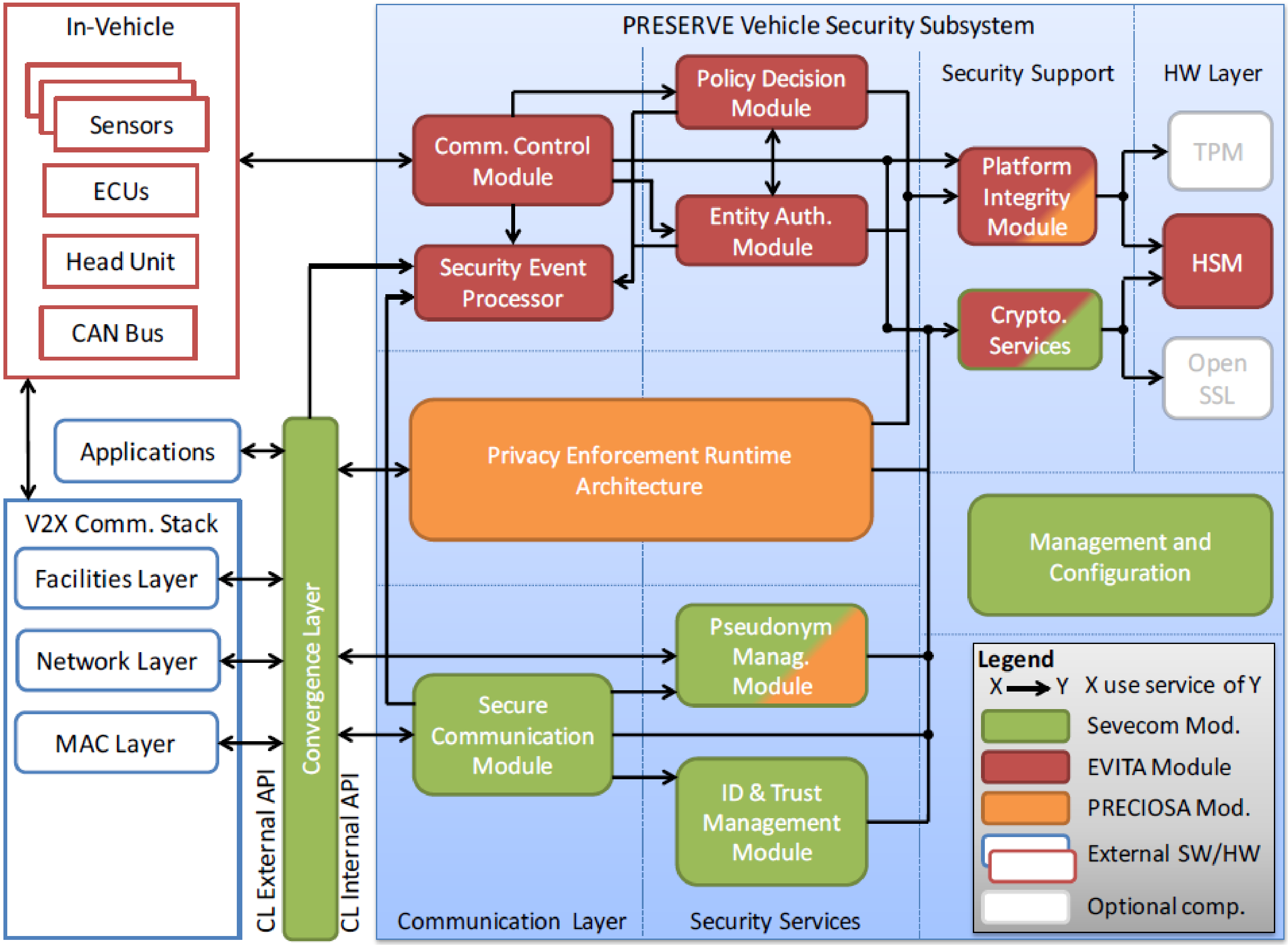
Meet performance and cost requirements of current FOTs and future products, esp. build security ASIC

Provide “ready-to-use” V2X security subsystem

Solve open deployment and technical issues hindering standardization and product development

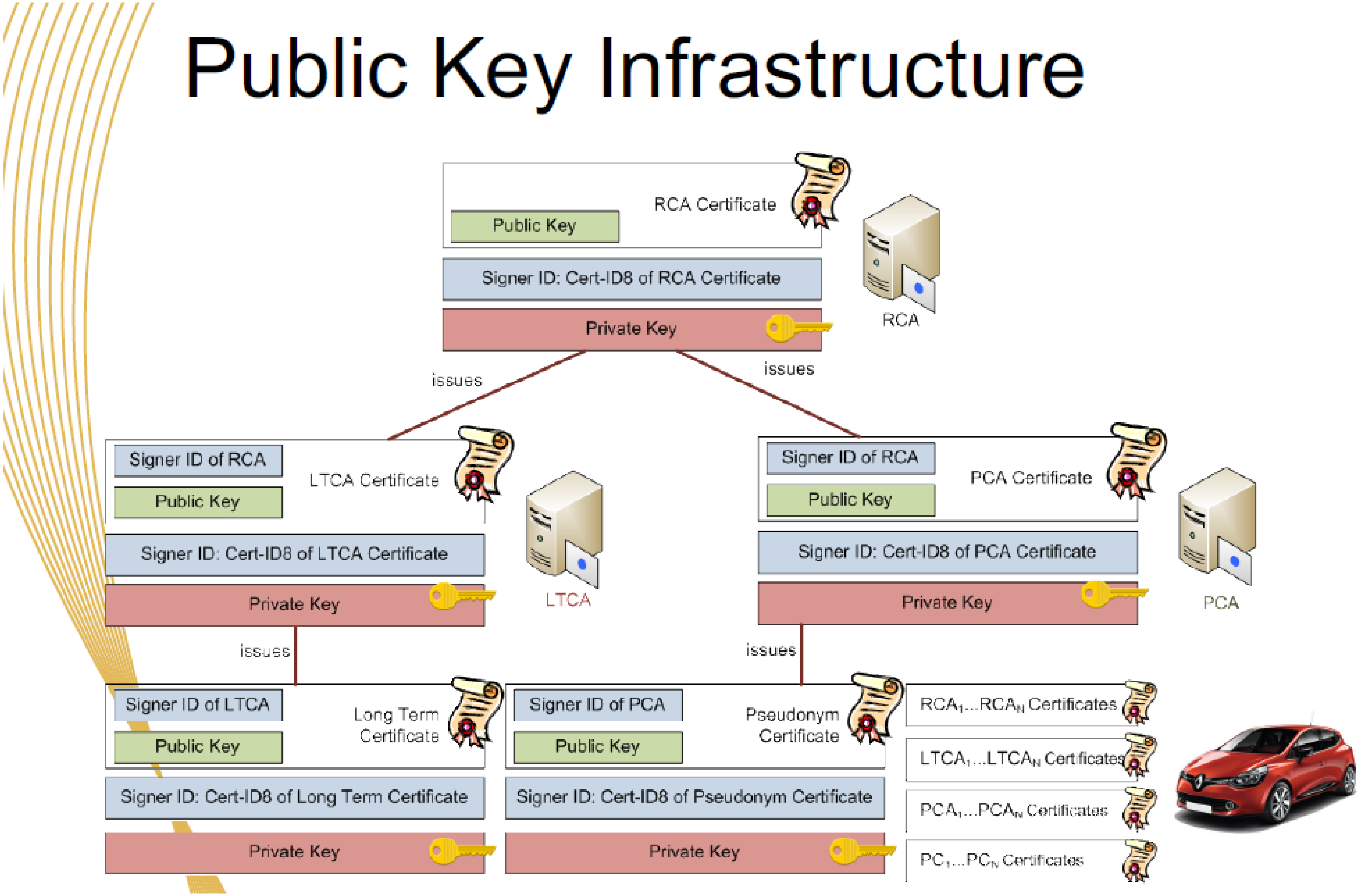
1) P. Papadimitratos, PRESERVE Overview, WC3 Meeting, Jan 2011 - https://www.w3.org/wiki/images/1/11/PRESERVE-Overview-.pdf

PRESERVE Vehicle Security Subsystems (EU)



1) Security Architecture PRESERVE Project - https://www.preserve-project.eu/sites/preserve-project.eu/files/preserve-ws-02-security-architecture.pdf

PRESERVE V-PKI Infrastructure (EU)



Public Key Infrastructure

RCA Certificate

Public Key

Signer ID: Cert-ID8 of RCA Certificate

Private Key

RCA

issues

issues

Signer ID of RCA

Public Key

LTCA Certificate

Signer ID: Cert-ID8 of LTCA Certificate

Private Key

LTCA

Signer ID of RCA

Public Key

PCA Certificate

Signer ID: Cert-ID8 of PCA Certificate

Private Key

PCA

issues

issues

Signer ID of LTCA

Public Key

Long Term Certificate

Signer ID: Cert-ID8 of Long Term Certificate

Private Key

Signer ID of PCA

Public Key

Pseudonym Certificate

Signer ID: Cert-ID8 of Pseudonym Certificate

Private Key

RCA_1...RCA_N Certificates

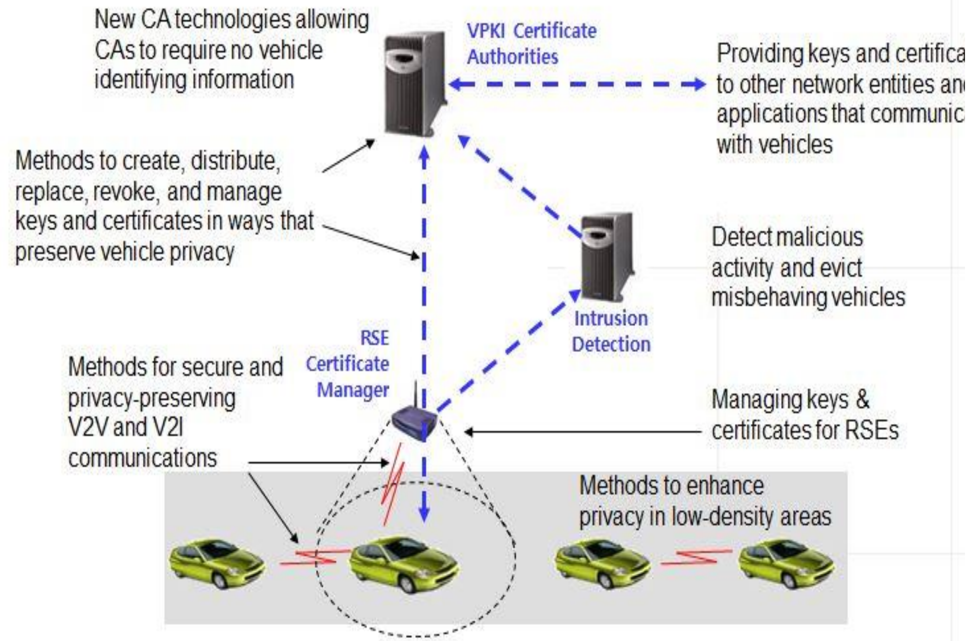
$LTCA_1$...$LTCA_N$ Certificates

PCA_1...PCA_N Certificates

PC_1...PC_N Certificates

1) V-PKI Model PRESERVE Project - https://www.preserve-project.eu/sites/preserve-project.eu/files/preserve-ws-02-security-architecture.pdf

A quick look at VPKI for US DOT Pilots (10 year span)



New CA technologies allowing CAs to require no vehicle identifying information

Methods to create, distribute, replace, revoke, and manage keys and certificates in ways that preserve vehicle privacy

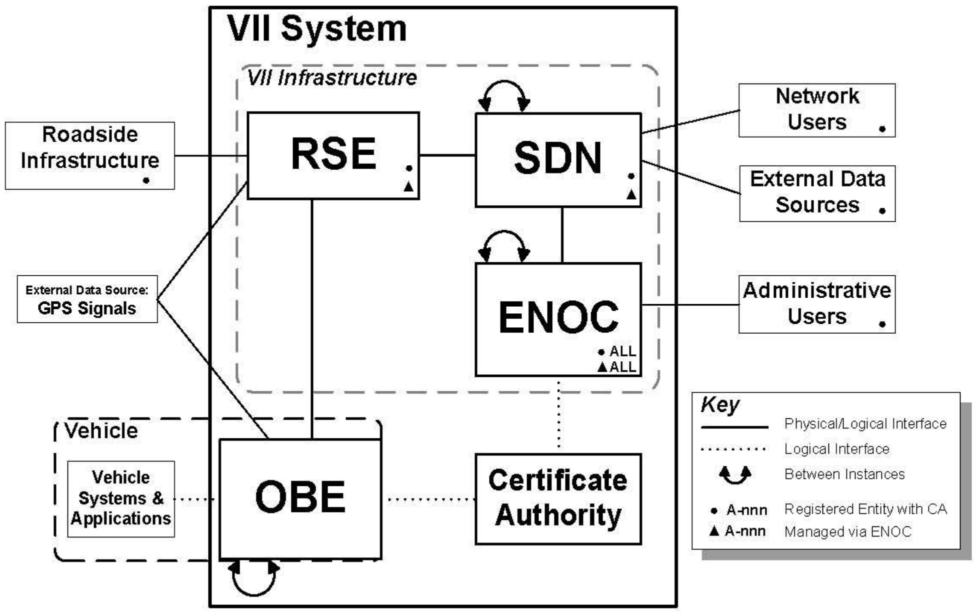
Methods for secure and privacy-preserving V2V and V2I communications

Providing keys and certifica to other network entities an applications that communic with vehicles

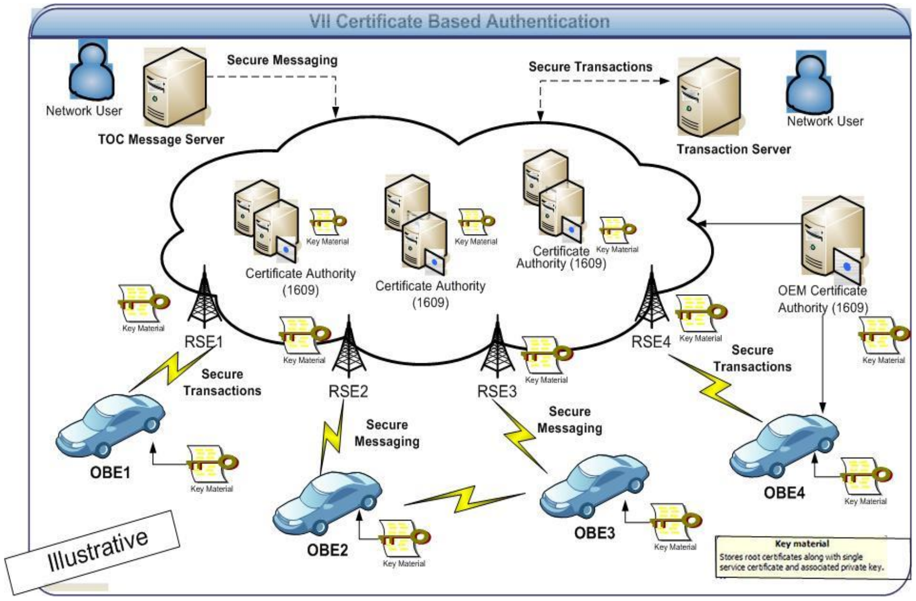
Detect malicious activity and evict misbehaving vehicles

Managing keys & certificates for RSEs

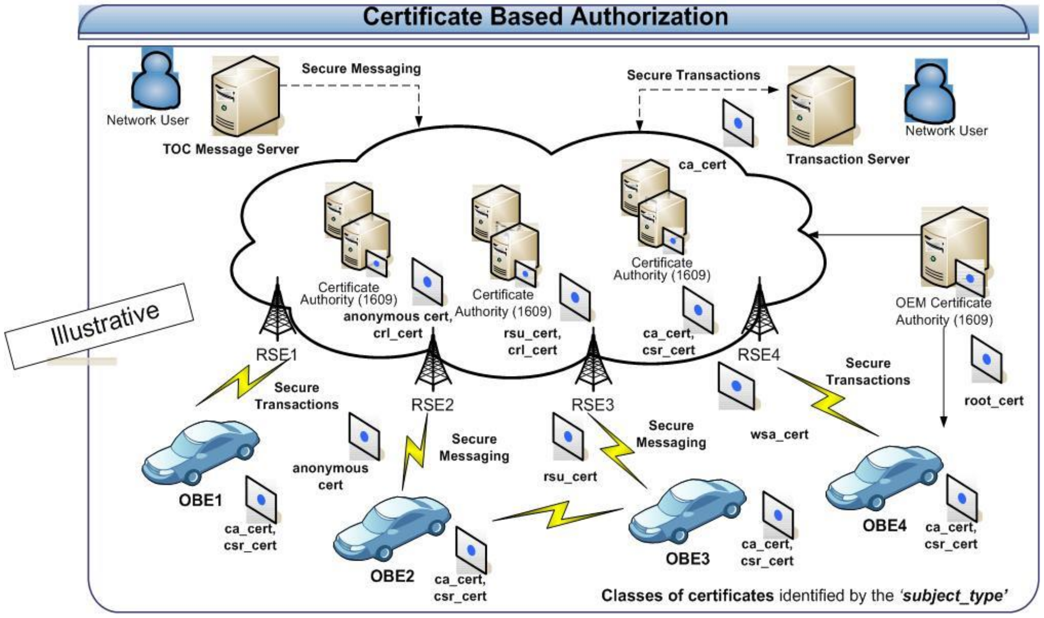
Methods to enhance privacy in low-density areas



Key	
───	Physical/Logical Interface
········	Logical Interface
↶↷	Between Instances
● A-nnn	Registered Entity with CA
▲ A-nnn	Managed via ENOC



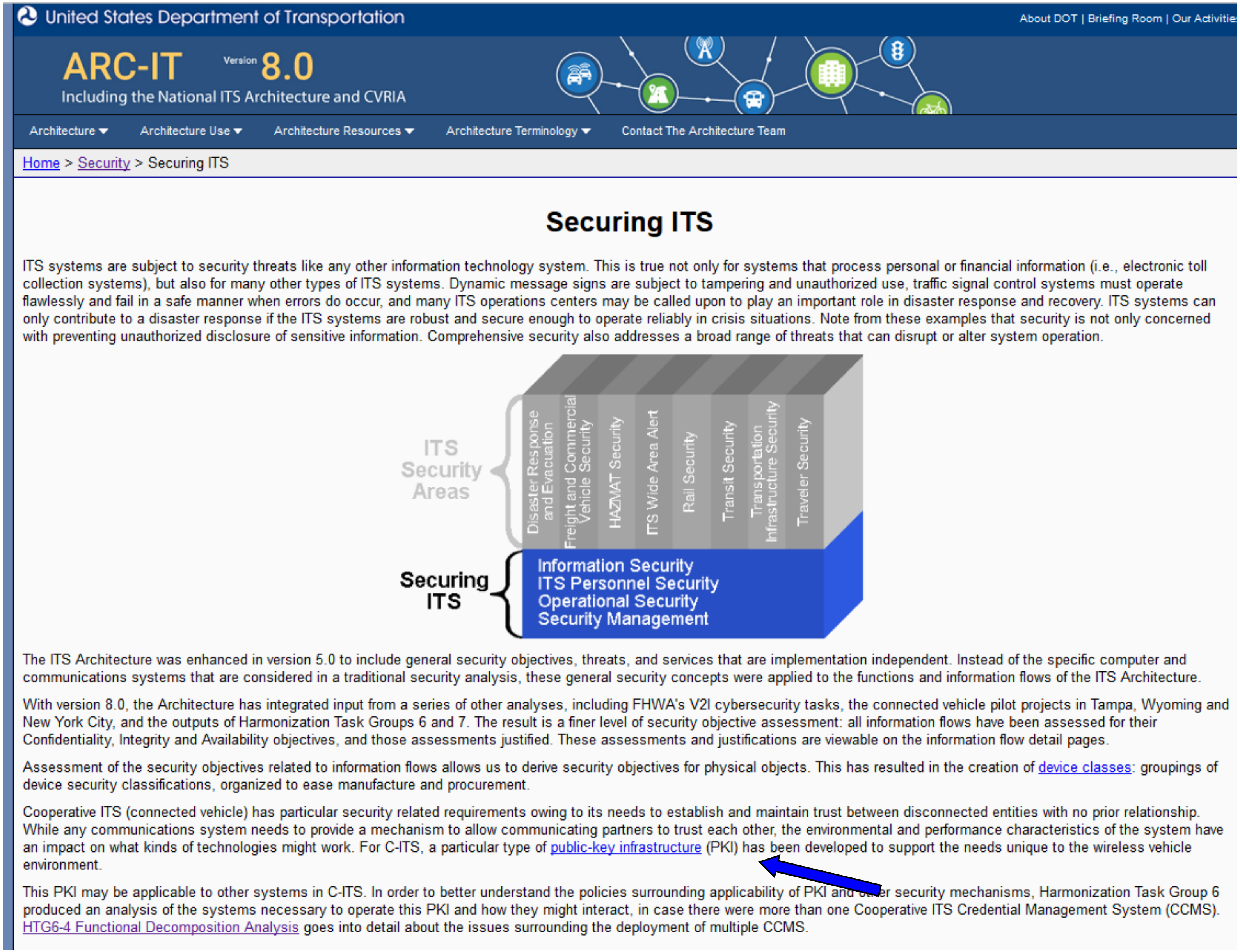
Key material
Stores root certificates along with single service certificate and associated private key.



Classes of certificates identified by the *'subject_type'*

Introduction – USDOT ITS National Architecture (Securing ITS)

http://local.iteris.com/arc-it/html/security/securingits.html


United States Department of Transportation
About DOT | Briefing Room | Our Activitie
ARC-IT Version 8.0
Including the National ITS Architecture and CVRIA
Architecture ▾
Architecture Use ▾
Architecture Resources ▾
Architecture Terminology ▾
Contact The Architecture Team
Home > Security > Securing ITS

Securing ITS

ITS systems are subject to security threats like any other information technology system. This is true not only for systems that process personal or financial information (i.e., electronic toll collection systems), but also for many other types of ITS systems. Dynamic message signs are subject to tampering and unauthorized use, traffic signal control systems must operate flawlessly and fail in a safe manner when errors do occur, and many ITS operations centers may be called upon to play an important role in disaster response and recovery. ITS systems can only contribute to a disaster response if the ITS systems are robust and secure enough to operate reliably in crisis situations. Note from these examples that security is not only concerned with preventing unauthorized disclosure of sensitive information. Comprehensive security also addresses a broad range of threats that can disrupt or alter system operation.

The ITS Architecture was enhanced in version 5.0 to include general security objectives, threats, and services that are implementation independent. Instead of the specific computer and communications systems that are considered in a traditional security analysis, these general security concepts were applied to the functions and information flows of the ITS Architecture.

With version 8.0, the Architecture has integrated input from a series of other analyses, including FHWA's V2I cybersecurity tasks, the connected vehicle pilot projects in Tampa, Wyoming and New York City, and the outputs of Harmonization Task Groups 6 and 7. The result is a finer level of security objective assessment: all information flows have been assessed for their Confidentiality, Integrity and Availability objectives, and those assessments justified. These assessments and justifications are viewable on the information flow detail pages.

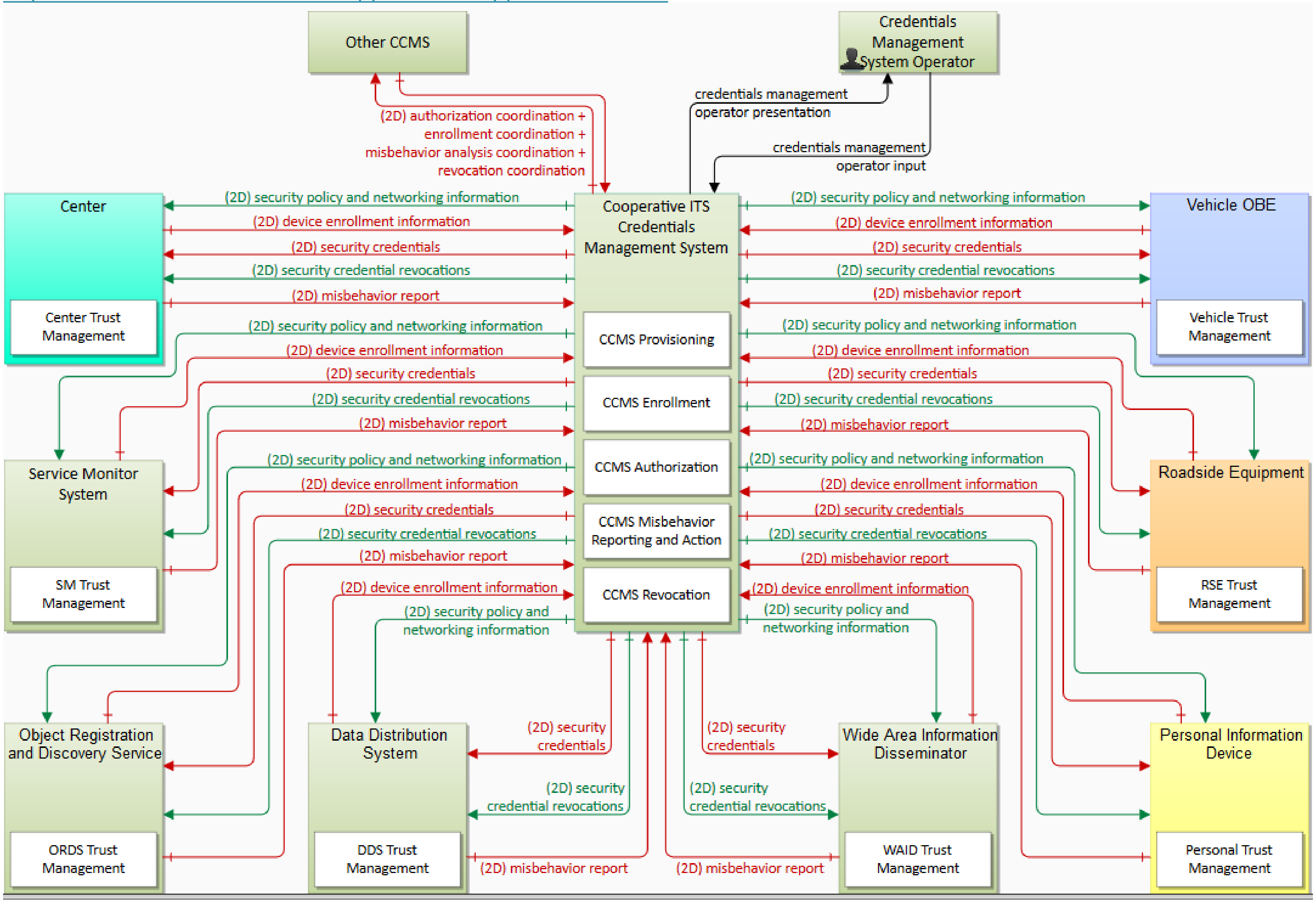
Assessment of the security objectives related to information flows allows us to derive security objectives for physical objects. This has resulted in the creation of device classes: groupings of device security classifications, organized to ease manufacture and procurement.

Cooperative ITS (connected vehicle) has particular security related requirements owing to its needs to establish and maintain trust between disconnected entities with no prior relationship. While any communications system needs to provide a mechanism to allow communicating partners to trust each other, the environmental and performance characteristics of the system have an impact on what kinds of technologies might work. For C-ITS, a particular type of public-key infrastructure (PKI) has been developed to support the needs unique to the wireless vehicle environment.

This PKI may be applicable to other systems in C-ITS. In order to better understand the policies surrounding applicability of PKI and other security mechanisms, Harmonization Task Group 6 produced an analysis of the systems necessary to operate this PKI and how they might interact, in case there were more than one Cooperative ITS Credential Management System (CCMS). HTG6-4 Functional Decomposition Analysis goes into detail about the issues surrounding the deployment of multiple CCMS.

Security and Credentials Management

http://local.iteris.com/cvria/html/applications/app63.html#tab-3



Other CCMS

Credentials Management System Operator

(2D) authorization coordination + enrollment coordination + misbehavior analysis coordination + revocation coordination

credentials management operator presentation

credentials management operator input

Cooperative ITS Credentials Management System

CCMS Provisioning

CCMS Enrollment

CCMS Authorization

CCMS Misbehavior Reporting and Action

CCMS Revocation

Center

Center Trust Management

Service Monitor System

SM Trust Management

Object Registration and Discovery Service

ORDS Trust Management

Data Distribution System

DDS Trust Management

Wide Area Information Disseminator

WAID Trust Management

Vehicle OBE

Vehicle Trust Management

Roadside Equipment

RSE Trust Management

Personal Information Device

Personal Trust Management

(2D) security policy and networking information

(2D) device enrollment information

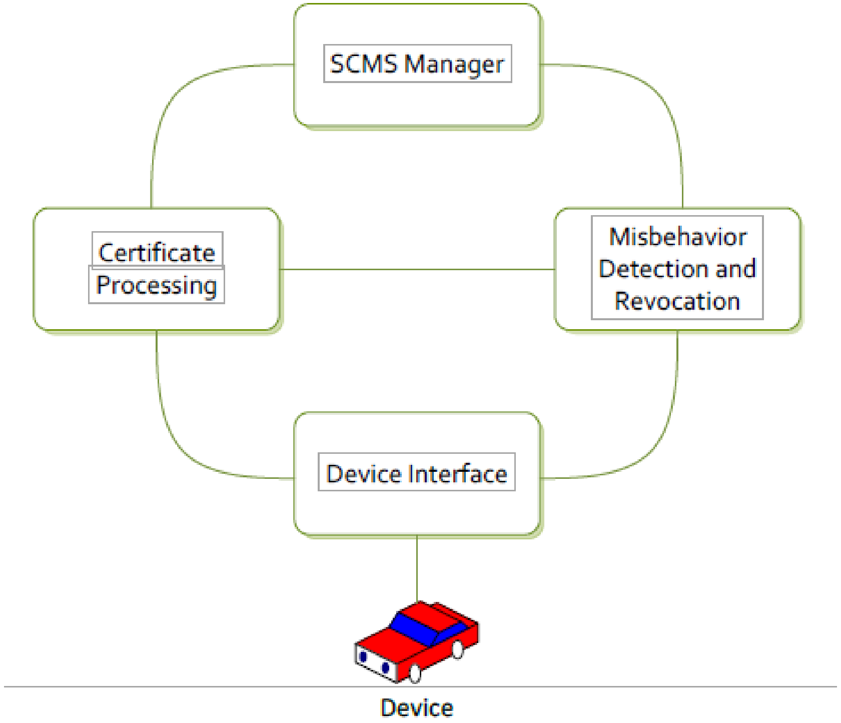
(2D) security credentials

(2D) security credential revocations

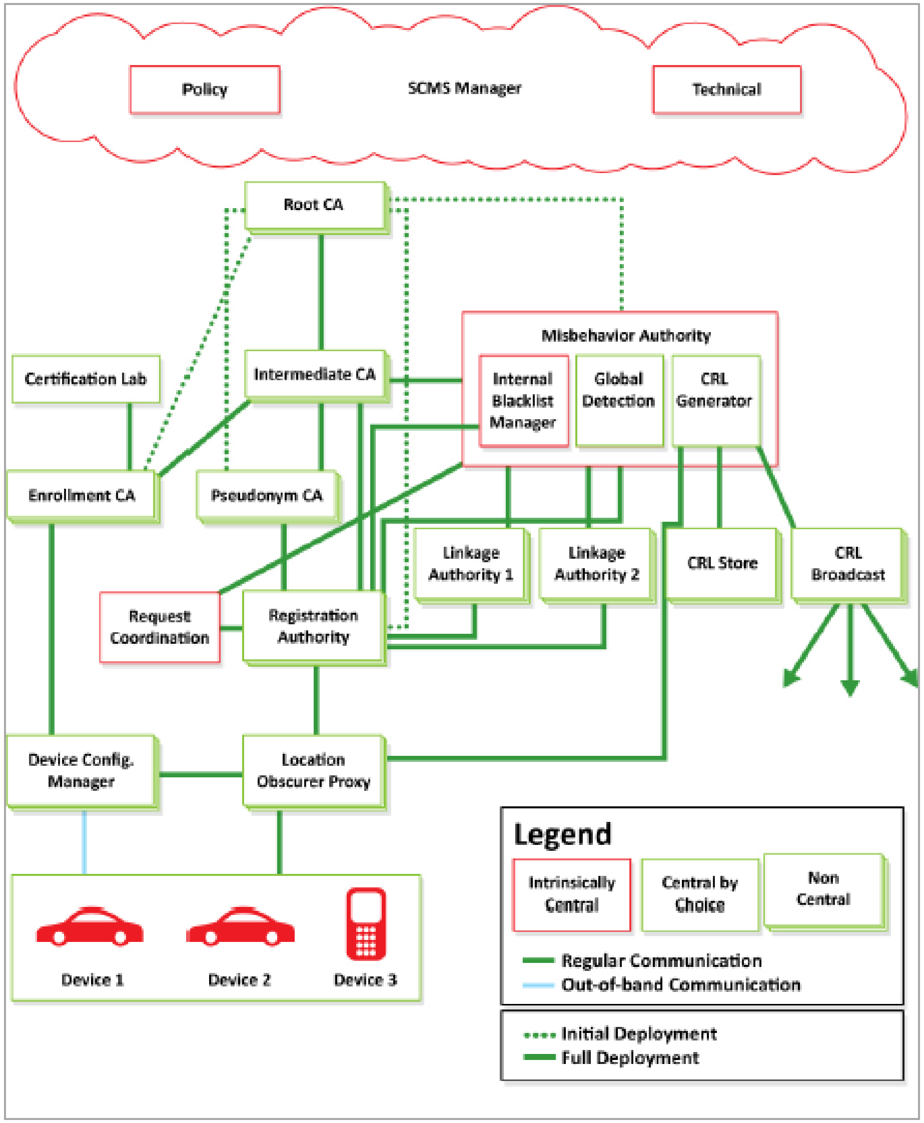
(2D) misbehavior report

Security Credential Management Systems (VPKI)

Simplified V2V Security System



Current V2V Security System Design for Deployment and Operations



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)

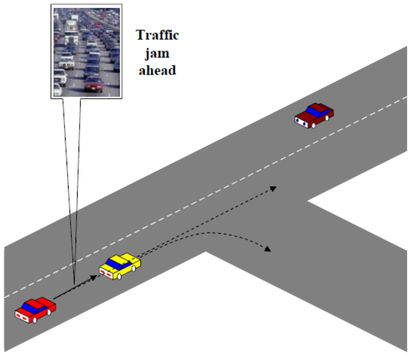
Concepts	Purpose
Pseudonym Functions / Certificate	A short-term digital certificates used by a vehicle's on-board equipment to authenticate and validate sent and received basic safety messages that form the foundation for V2V safety technologies. These short-term certificates contain no information about 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

Table of Contents

- Testbed and Pilot Programs (2004-2017)
- Evolving the Security and Privacy Model for Connected Car
- Wireless Access for Vehicular Environments (WAVE) Standard
- Secure Credential Management System (SCMS Implementation Details)
- Securing the Basic Safety Message (BSM)

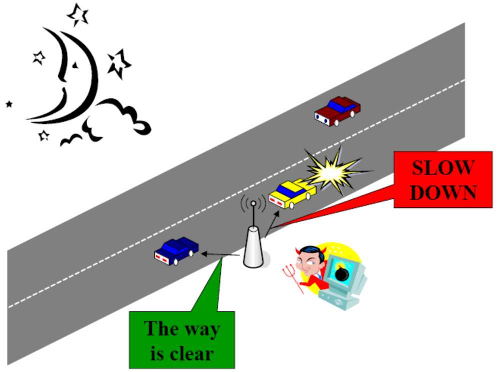
Security Architecture for VANETS (EPFL V-PKI – J.Hubaux et. al.) - 2004

Attack 1 : Bogus traffic information



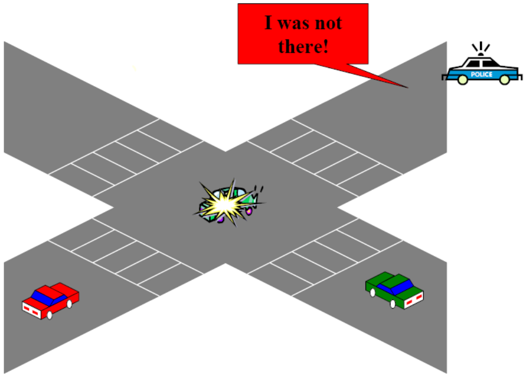
- Attacker: insider, rational, active

Attack 2 : Disruption of network operation



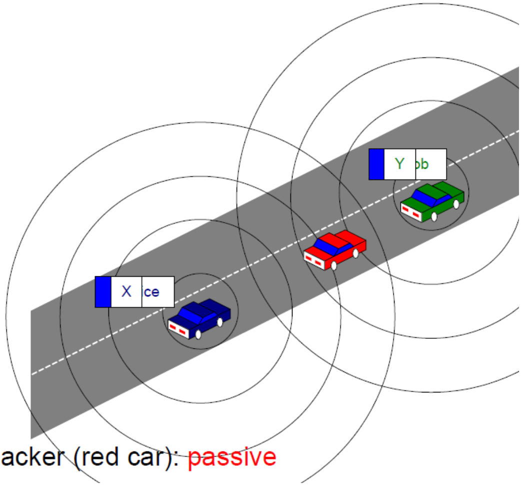
- Attacker: malicious, active

Attack 3: Cheating with identity, position or speed



- Attacker: insider, rational, active

Attack 4 : Uncovering the identities of other vehicles

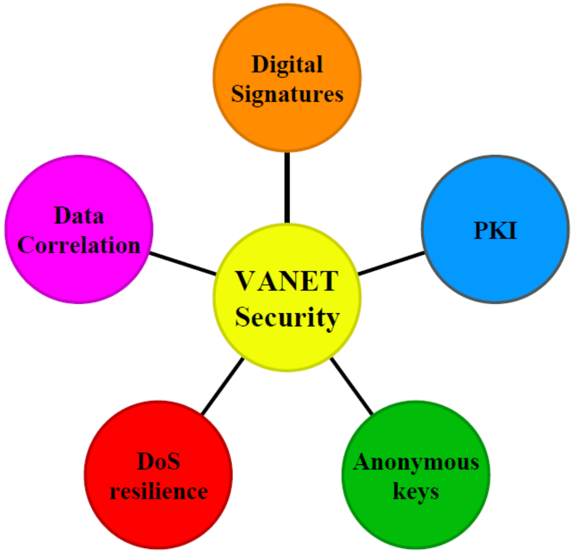


- Attacker (red car): passive

Attacker's model in Vehicular Communications

- An attacker can be an outsider or an insider and malicious or rational
- An attack can be active or passive
- Attacks against anonymous messages:
  - Bogus information
- Attacks against liability-related messages:
  - Cheating with own identity
  - Cheating with position or speed
- Attacks against both kinds of messages:
  - Uncovering identities of other vehicles
  - Disruption of network operation (Denial of Service attacks)

How to secure VANETs



Digital Signatures

Data Correlation

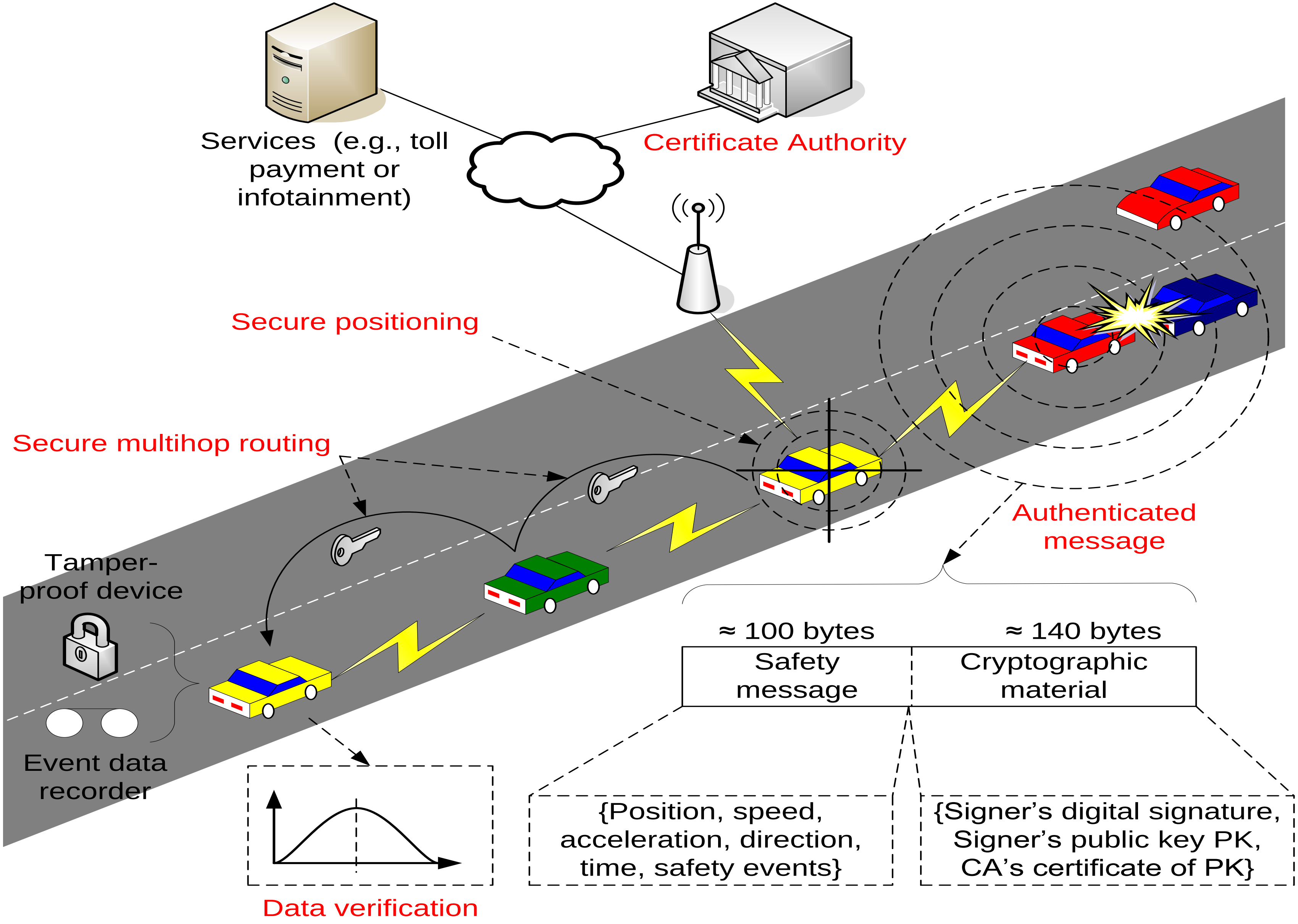
PKI

VANET Security

DoS resilience

Anonymous keys

Security Architecture (EPFL V-PKI – J.Hubaux et. al.)



Services (e.g., toll payment or infotainment)

Certificate Authority

Secure positioning

Secure multihop routing

Authenticated message

Tamper-proof device

Event data recorder

≈ 100 bytes	≈ 140 bytes
Safety message	Cryptographic material

{Position, speed, acceleration, direction, time, safety events}

{Signer's digital signature, Signer's public key PK, CA's certificate of PK}

Data verification

Secure vehicular communication systems: Design and architecture **

Security Vehicular Communications	Purpose
Adversary Model	VC system entities can be correct or benign; that is, they may comply with the implemented protocols or deviate from the protocol definition (i.e., be faulty or adversarial). Adversarial behavior can vary according to the implemented protocols and the capabilities of the adversary.
Message authentication and integrity	To protect against any alteration and allow the receiver of a message to corroborate the sender of the message
Message non-repudiation	The sender of a message cannot deny having sent a message
Entity Authentication	a receiver is ensured that the sender generated a message and has evidence of the liveness of the sender. In other words, ascertain that a received unmodified message was generated within an interval
Access Control	Determine via specific system-wide policies the assignment of distinct roles to different types of nodes and their allowed actions within the system. As part of access control, authorization establishes what each node is allowed to do in the network,
Message confidentiality	Keep the content of a message secret from those nodes not authorized to access it
Accountability	Map security related events to system entities.
Privacy Protection	Safeguard private information of VC system users. This is a general requirement that relates to the protection of private information stored offline. In the context of communication, which is the object of SeVeCom, we are interested in anonymity for the actions (messages and transactions) of the vehicles.
Authorities (CA)	a large number of certification authorities (CAs) will be instantiated. Each CA is responsible for a region (national territory, district, county, etc.), and manages identities and credentials of all nodes registered with it. To enable interactions between nodes from different regions, CAs provide certificates for other CAs (cross-certification) or provide foreigner certificates to vehicles that are registered with another CA when they cross thegeographical boundaries of their region
Node Identification	Each node is registered with only one CA, and has a unique long-term identity and a pair of private and public cryptographic keys, and it is equipped with a long-term certificate. A list of node attributes and a lifetime are included. The CA is also responsible for the eviction of nodes or the withdrawal of compromised cryptographic keys via the revocation

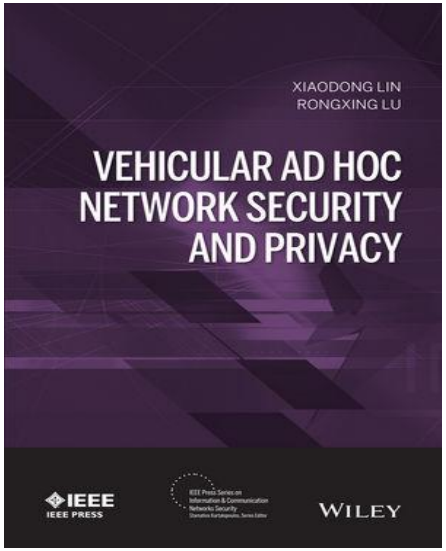
1) P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, “Secure vehicular communication systems: Design and architecture,” *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

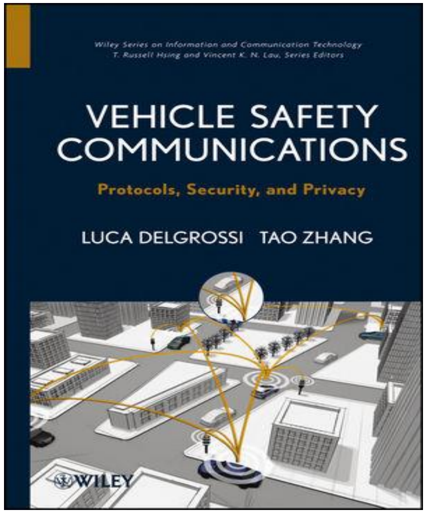
Secure vehicular communication systems: Design and architecture **

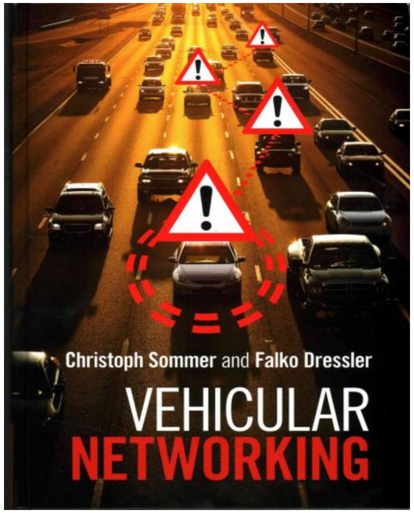
Security Vehicular Communications	Purpose
Digital Signatures	Digital signatures are used for all messages.To satisfy both the security and anonymity requirements, a pseudonymous authentication approach is used . Rather than utilizing the sa me long-term public and private key for securing communications, each vehicle utilizes multiple short-term private-public key pairs and certificates.
Identiy and Credential Management	**Long-Term Identification** — Each node has a unique long-term identity which will be the outcome of an agreement between car manufacturers and authorities, similar to the use of vehicle identification numbers (VINs). **Short-Term Identification** - Pseudonyms are stored and managed in the onboard pseudonym pool, with their corresponding secret keys kept in the HSM. This ensures that each vehicle has exactly one key pair (its own pseudonym and private key) that is active during each time period
Hardware Security Module (HSM)	Stores the private cryptographic key material and provides cryptographic functions to be used by other modules. The HSM is physically separated from the OBU, and it has some tamper-resistant properties in order to protect the private key materialagainst physical attacks. The HSM consists ofa CPU, some non-volatile memory, a built-inclock, and some I/O interface.
Certificate Revocation	The certificates of faulty nodes have to be revoked to prevent them from causing damage to the VC system. Revocation can be decided by the CA for administrative or technical reasons. The basic mechanism to achieve this is certificate revocation lists (CRLs) the CA creates and authenticates..
Secure Communication	**Secure Beaconing** - Beaconing denotes periodic single-hop broadcasts typically used for so-called cooperative awareness applications. In order to create awareness of other vehicles in the vicinity, every beacon contains information on the sender's status such as vehicle position, speed, and heading **Secure Neighbor Discovery** - Cooperative awareness or safety messaging allow vehicles to discover a frequently updated view of other vehicles in proximity, called physical neighbors. **Secure Geocast** - 1) Addressing of a geographically defined destination region 2) Forwarding toward this region 3) Distribution of the packet within the destination region **Pseudonym Handling** - An adversary analyzing which certificates areattached to signed messages can track the location of vehicles over time. If pseudonyms are changed at appropriate times and locations, messages signed under different pseudonyms are hard to link by an adversary.

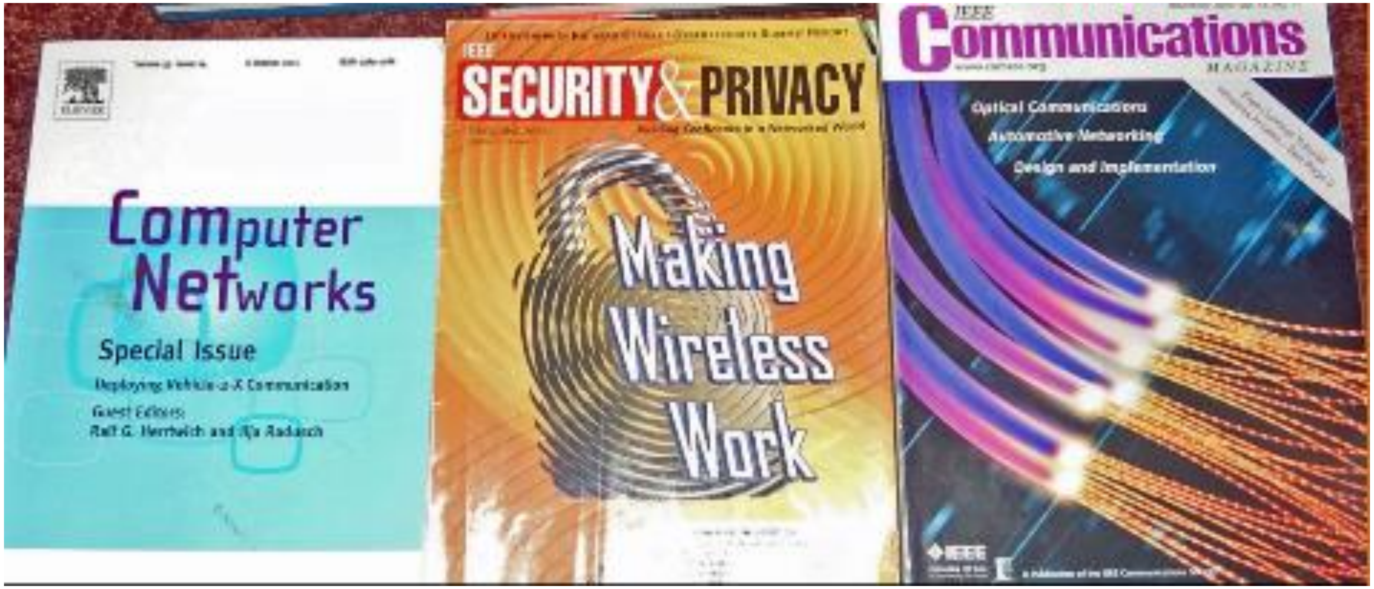
1) P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: Design and architecture," *IEEE Commun. Mag.*, vol. 46, no. 11, pp. 100–109, Nov. 2008.

Privacy-Preserving Vehicular PKI (a very broad subject)




Wiley Series on Information and Communication Technology
T. Russell Hsing and Vincent K. N. Lau, Series Editors
VEHICLE SAFETY COMMUNICATIONS
Protocols, Security, and Privacy
LUCA DELGROSSI TAO ZHANG
WILEY



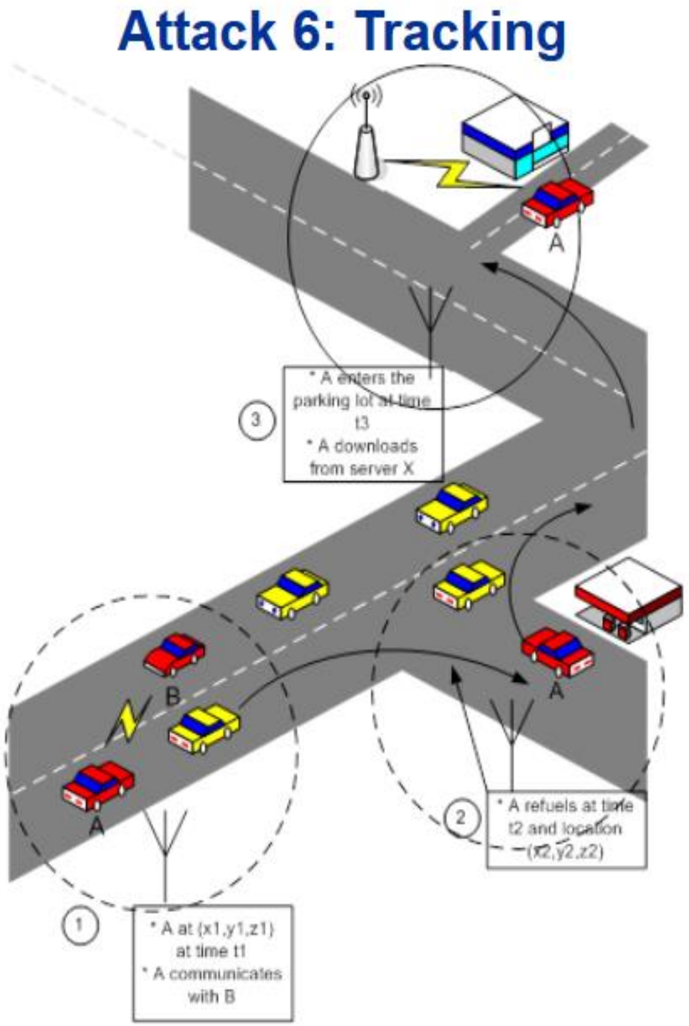


Privacy

- Need to protect against
  - Identification of vehicle
  - Re-identification of vehicle

- Identifying properties
  - Characteristic properties of application, system, radio
    - Timing, packet size, RF-fingerprint, ...
  - Plain identifiers
    - MAC address, IP address, Login, ...
    - Certificate (necessary for participation!)

- Absolute Anonymity?
  - Made impossible by most protocols and/or use cases



1) A. Pfitzmann, and M. Hansen, Anonymity, Unobservability, and Pseudonymity: A Proposal for Terminology, H. Federrath (Ed.), Designing Privacy Enhancing Technologies, LNCS 2009, pp. 1-9, 2000,
2) J Hubaux (et al) – Securng Vehicle Communications - http://lcawww.epfl.ch/hubaux/Talks/Securing%20Vehicular%20Communications.pdf

Pseudonymity

- Communication using pseudonyms
  - Sign messages using pseudonymous certificates
  - Receiver can check if signed by trusted CA
  - Base identity never revealed to other vehicles
- Revocation of Pseudonyms
  - Dissemination of Certificate Revocation List (CRL) via Internet, RSUs, or Car-to-Car
  - Open questions: availability, scalability (speed, size of CRL)
  - CA knows mapping from base identity ⇨ pseudonym;
    can revoke all related pseudonyms

Anonymity

Anonymity is…

“*the state of being not identifiable within a set of subjects, the anonymity set*”

(Pfitzmann/Hansen)

[1] A. Pfitzmann, and M. Hansen, Anonymity, Unobservability, and Pseudonymity: A Proposal for Terminology, H. Federrath (Ed.), Designing Privacy Enhancing

Anonymity and Privacy Issues

- The term “anonymity” describes the design goal that, as far as possible, broadcast transmissions from a vehicle operated by a private citizen should not leak information that can be used to identify that vehicle to unauthorized recipients. (Public safety vehicles, which are representing some state authority, do not generally have this requirement for anonymity).

- With the use of 1609.2 certificates, the OBE anonymity architecture will allow for broadcast transmissions from a vehicle operated by a private citizen to not leak information that can be used to identify that vehicle to unauthorized recipients. This will allow OBEs to maintain anonymous profiles while using the VII System’s public safety capabilities.

- For transactional applications, 1609.2 provides several mechanisms for anonymity

  A sender can ensure that long-lived identifying data such as application-specific certificates is always encrypted.

  A vehicle’s MAC address changes as it moves from one RSE zone of communications to the next, otherwise an attacker could track it by the static MAC address.

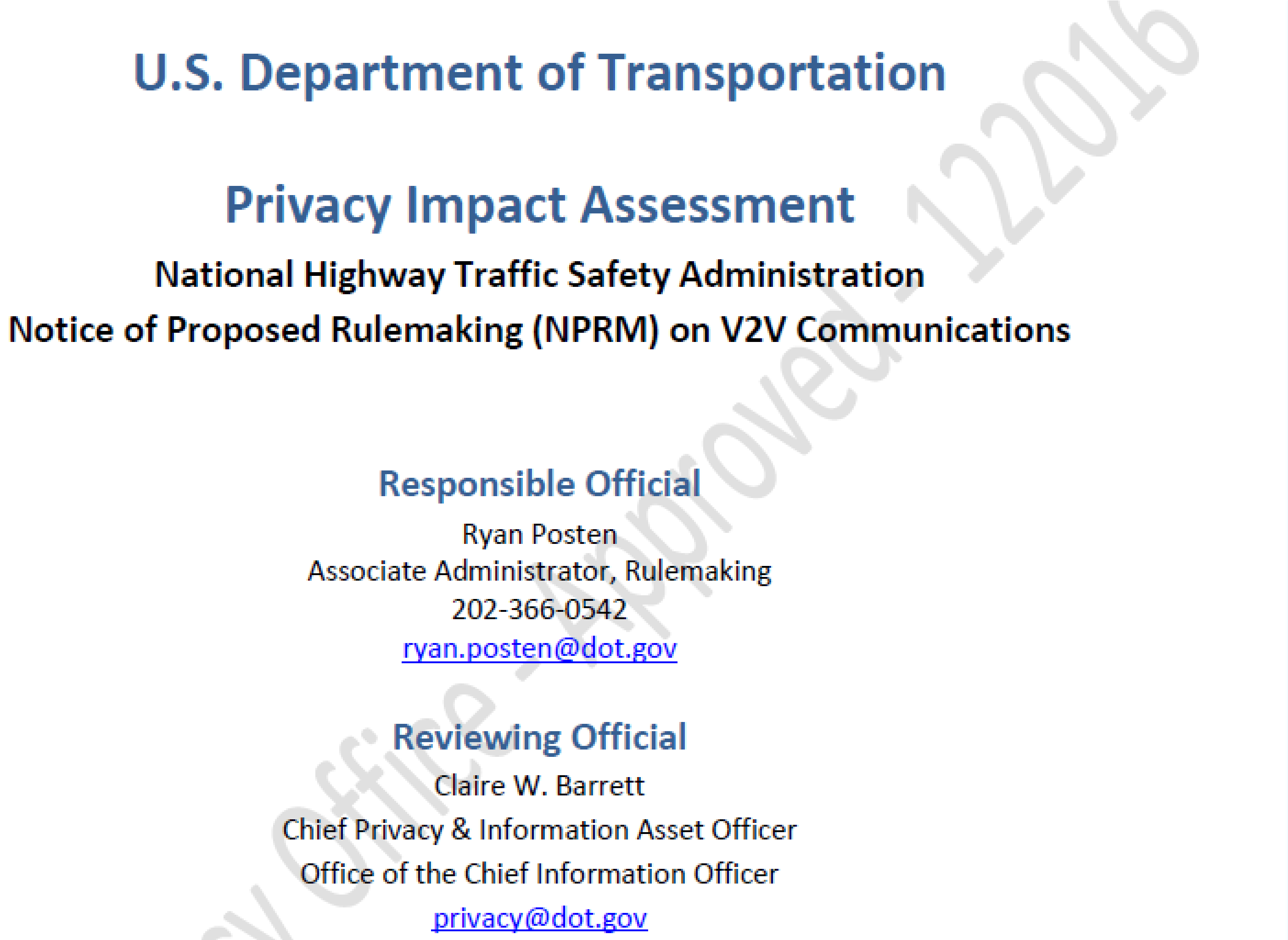
  The IP address of an application on a vehicle could be used to track it. However, currently DSRC/WAVE provides no mechanism to allow an IP connection to persist across a changing MAC address

Privacy Protections and Efficiency in the SCMS Design

- There is an efficient way of revoking all the certificates within a device
- There is an efficient way of revoking all the certificates within a group of devices
- Certificates are not linkable by an eavesdropper unless the owner has been revoked
- Membership to a group is not be disclosed unless that group has been revoked
- A vehicle is trackable after its credentials are revoked but not before it was revoked. Similarly, if a group of vehicles' security credentials are revoked, a device belonging to that group is identifiable as a member. However, it is not possible to determine the membership to a group before the group revocation took place.
- No single entity within the system is able to determine that two certificates belong to the same device or to the same group. An exception to this rule is the Misbehavior Authority (MA).
- No single entity within the SCMS is able to track a vehicle. Once a single LA is introduced, this requirement is not fulfilled any longer. For that reason, two LAs are used and the information which allows for tracking is split between them.

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

Privacy Impact Assessment (NHTSA NPRM on V2V Communications)



U.S. Department of Transportation

Privacy Impact Assessment

National Highway Traffic Safety Administration
Notice of Proposed Rulemaking (NPRM) on V2V Communications

Responsible Official

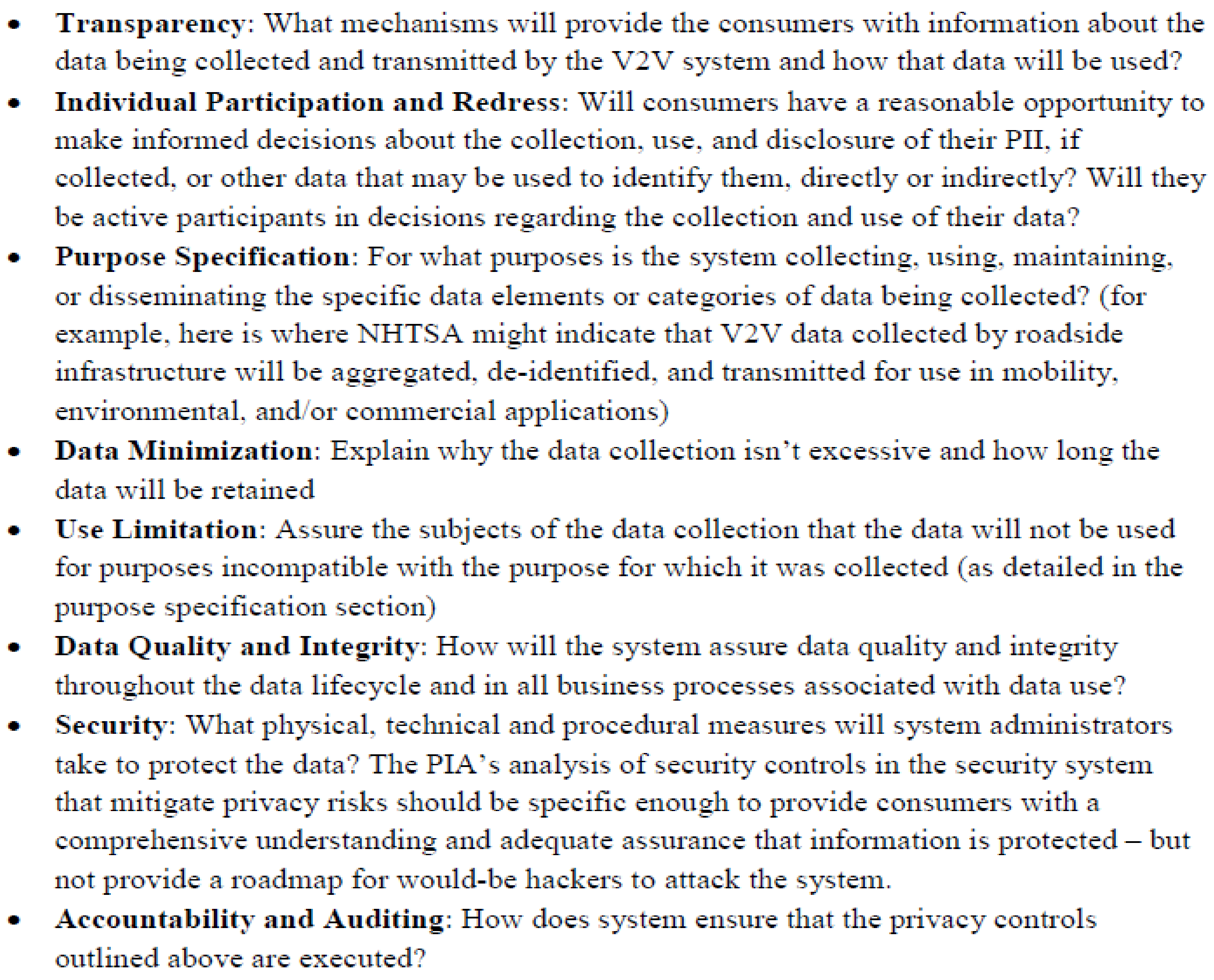
Ryan Posten
Associate Administrator, Rulemaking
202-366-0542
ryan.posten@dot.gov

Reviewing Official

Claire W. Barrett
Chief Privacy & Information Asset Officer
Office of the Chief Information Officer
privacy@dot.gov

https://cms.dot.gov/sites/dot.gov/files/docs/Privacy%20-%20NHTSA%20-%20V2V%20NPRM%20-%20PIA%20-%20Approved%20-%20122016.pdf

Privacy Assessment Fair Information Practice Principles (FIPPs) Control Families

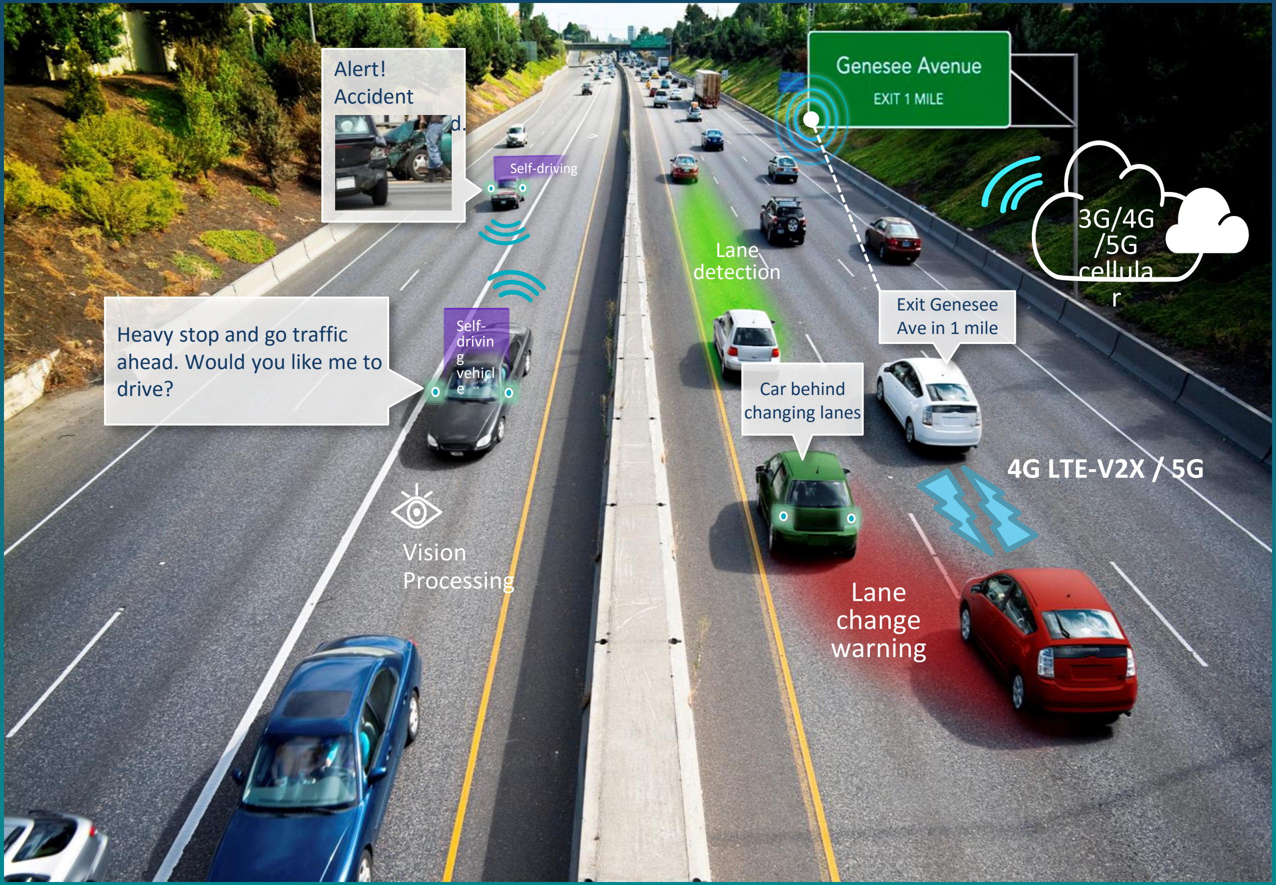


- **Transparency**: What mechanisms will provide the consumers with information about the data being collected and transmitted by the V2V system and how that data will be used?
- **Individual Participation and Redress**: Will consumers have a reasonable opportunity to make informed decisions about the collection, use, and disclosure of their PII, if collected, or other data that may be used to identify them, directly or indirectly? Will they be active participants in decisions regarding the collection and use of their data?
- **Purpose Specification**: For what purposes is the system collecting, using, maintaining, or disseminating the specific data elements or categories of data being collected? (for example, here is where NHTSA might indicate that V2V data collected by roadside infrastructure will be aggregated, de-identified, and transmitted for use in mobility, environmental, and/or commercial applications)
- **Data Minimization**: Explain why the data collection isn't excessive and how long the data will be retained
- **Use Limitation**: Assure the subjects of the data collection that the data will not be used for purposes incompatible with the purpose for which it was collected (as detailed in the purpose specification section)
- **Data Quality and Integrity**: How will the system assure data quality and integrity throughout the data lifecycle and in all business processes associated with data use?
- **Security**: What physical, technical and procedural measures will system administrators take to protect the data? The PIA's analysis of security controls in the security system that mitigate privacy risks should be specific enough to provide consumers with a comprehensive understanding and adequate assurance that information is protected – but not provide a roadmap for would-be hackers to attack the system.
- **Accountability and Auditing**: How does system ensure that the privacy controls outlined above are executed?

Table of Contents

- Testbed and Pilot Programs (2004-2017)
- Evolving the Security and Privacy Model for Connected Car
- Wireless Access for Vehicular Environments (WAVE) Standard
- Secure Credential Management System (SCMS Implementation Details)
- Securing the Basic Safety Message (BSM)
- What If Questions for SCMS

A New Era of Connected Car Capabilities

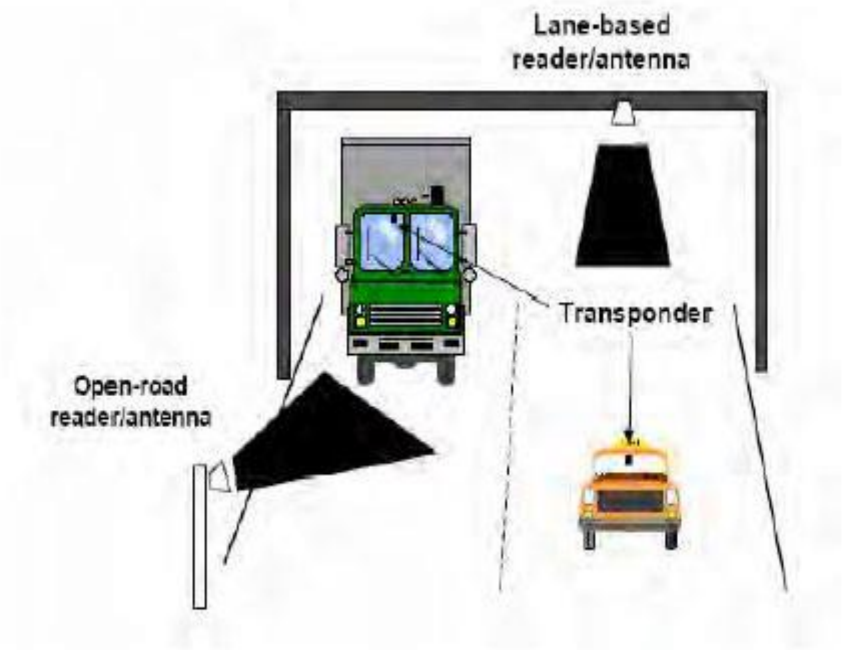


The variety of connected vehicle applications can be handled by a variety of over the air technologies, depending on application requirements

DSRC Operations Model

- Dedicated Short Range Communications (DSRC) technology has been chosen to support both Public Safety and Private operations
- DSRC fact sheet:
  - Based on IEEE 802.11p
  - Range up to 1000m
  - Data rates from 6-27 Mbps
  - 7 licensed channels in 5.9GHz
  - Low latency ~50ms
  - Security using public key infrastructure (PKI)
  - Long term stability (technology evolution is controlled by FCC and standards)
  - Postured for IPv6 at roll-out

DSRC Components



IEEE Standards Association Publications (WAVE) – https://standards.ieee.org/develop/wg/1609_WG.html

- **IEEE P802.11p**, Amendment to STANDARD FOR Information technology—Telecommunications and information exchange between systems—LAN/MAN Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Wireless Access in Vehicular Environments (WAVE).

- IEEE Std 1609.0-2013 – IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE) - Architecture

- **IEEE Std 1609.2-2016™**, IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Security Services for Applications and Management Messages.

- **IEEE Std 1609.3-2010™**, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services.

- **IEEE Std 1609.4-2011™**,, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)—Multi-Channel Operation.

- **IEEE Std 1609.11-2011™**, IEEE Draft Standard for Wireless Access in Vehicular Environments (WAVE)—Over-the-Air Data Exchange Protocol for Intelligent Transportation Systems (ITS) - Electronic Payment Service

- **IEEE Std 1609.12-2016™**, IEEE Draft Standard for Wireless Access in Vehicular Environments (WAVE)—Identifier Allocation

Overview of WAVE Services

WAVE system is a radio communications system intended to provide seamless, interoperable services to transportation. These services include those recognized by the U.S. National Intelligent Transportation Systems (ITS) Architecture a and many others contemplated by the automotive and transportation infrastructure industries. These services include vehicle-to-roadside communication, vehicle-to-vehicle communications, and potentially communication among other devices. Networking Services provides services to WAVE devices and systems. Layers 3 and 4 of the open system interconnect (OSI) model and the Internet Protocol (IP), User Datagram Protocol (UDP), and Transmission Control Protocol (TCP)elements of the Internet model are represented. Management and data services within WAVE devices are provided.

The term dedicated short range communications (DSRC) is sometimes used in the U. S. to refer to radio spectrum or technologies associated with WAVE. For example, U. S. Federal Communications Commission (FCC) documents allocate spectrum to “mobile service for use by DSRC systems operating in the Intelligent Transportation System (ITS) radio service,” and the Society of Automotive Engineers (SAE) has specified messages in SAE J2735 “for use by applications intended to utilize the 5.9 GHz dedicated short range communications for wireless access in vehicular environments.”

IEEE WAVE Standards Supporting Connected Car Pilot Program (DSRC) **

1609.0—Guide for Wireless Access in Vehicular Environments (WAVE) Architecture—This section of the standard describes the full set of 1609 standards and their relationships to each other and other relevant standards such as 802.11.

1609.2—Security Services for Application and Management Messages—Describes the secure message formats and processing for use by WAVE devices, including methods to secure WAVE management messages and methods to secure application messages. It also describes administrative functions necessary to support the core security functions. The V2V security design is based on this standard and incorporates an expanded application of Public-Key infrastructure to secure V2V communications and appropriately protect privacy. This standard is associated with Layer 5, session layer, and Layer 6, presentation layer.

1609.3—Networking Services—In relation to Layers 3 and 4, network and transport, this standard describes the Internet Protocol (IP), User Datagram Protocol (UDP), and the Transmission Protocol (TCP) elements of the internet model and management and data services for WAVE devices.

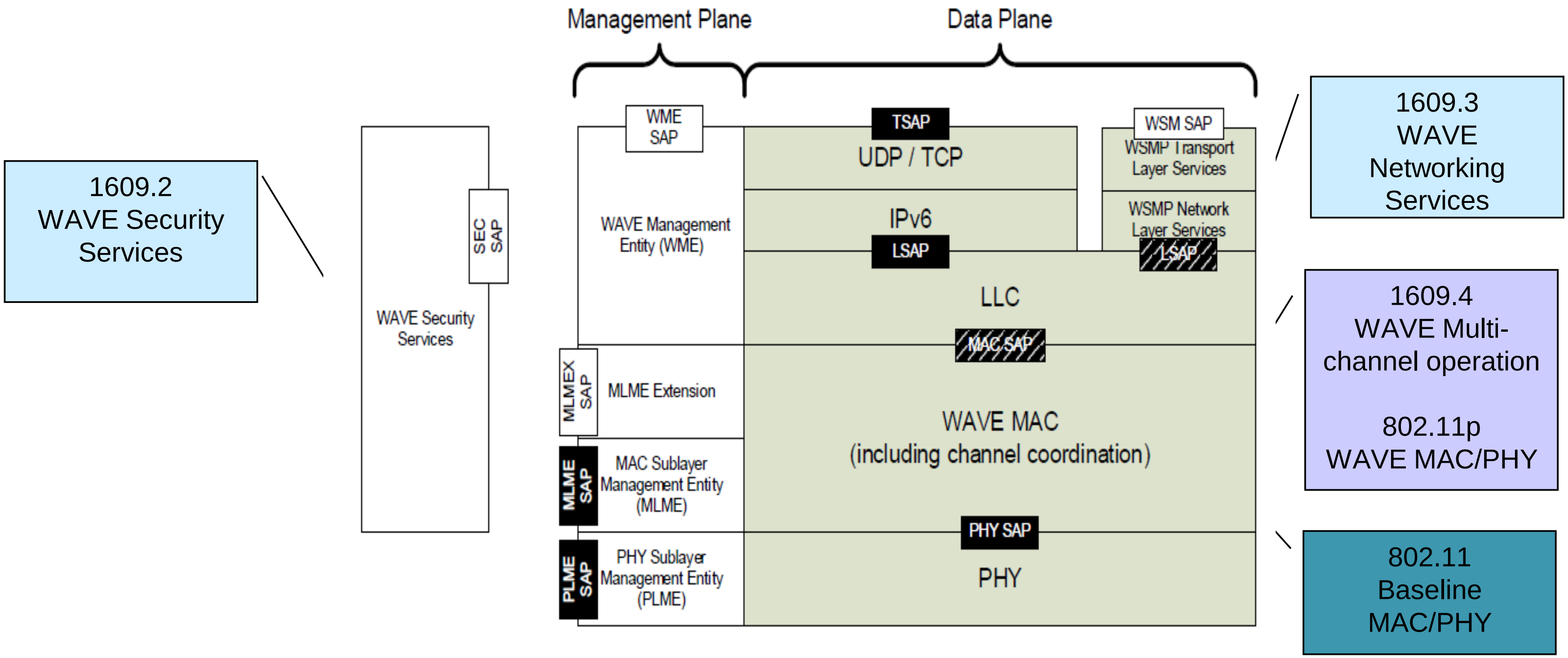
1609.4—Multi-Channel Operations—This standard crosses layers 2 through 5 to support multi-channel operations of the DSRC radio. Wireless radio operations that include the use of other channels need to provide instructions concerning the operation of the control channel (CCH), the service channel (SCH), interval times, priority access, channel switching, and routing. The current design for a V2V DSRC device uses two radios. One radio is tuned to channel 172 for transmission and reception of the safety-critical communication of the BSM. The second radio uses multi-channel operations to set the CCH and SCH, and use the other channels to support other messages transmission such as the messages associated with security materials.

1609.12—Identifier Allocations— For the WAVE system this standard describes the use of identifiers and the values that have been associated with the identifiers (PSID) for use by the WAVE 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,**

1609.0 Protocol Model, Updated, with Standards and Access Points

The air interface allows WAVE devices to communicate with each other over the wireless medium. Interfaces between protocol components are accomplished via services access points (SAPs). SAPs are specified in the appropriate standard and are illustrated below. SAPs describe information exchanged, but do not specify the interface implementation. SAPs are comprised of “primitives,” each of which is a logical message structure, generally containing a set of data elements for accomplishing a particular function.



[1] IEEE Vehicular Technology Society, "**IEEE1609.0 (WAVE Architecture)**," IEEE Std

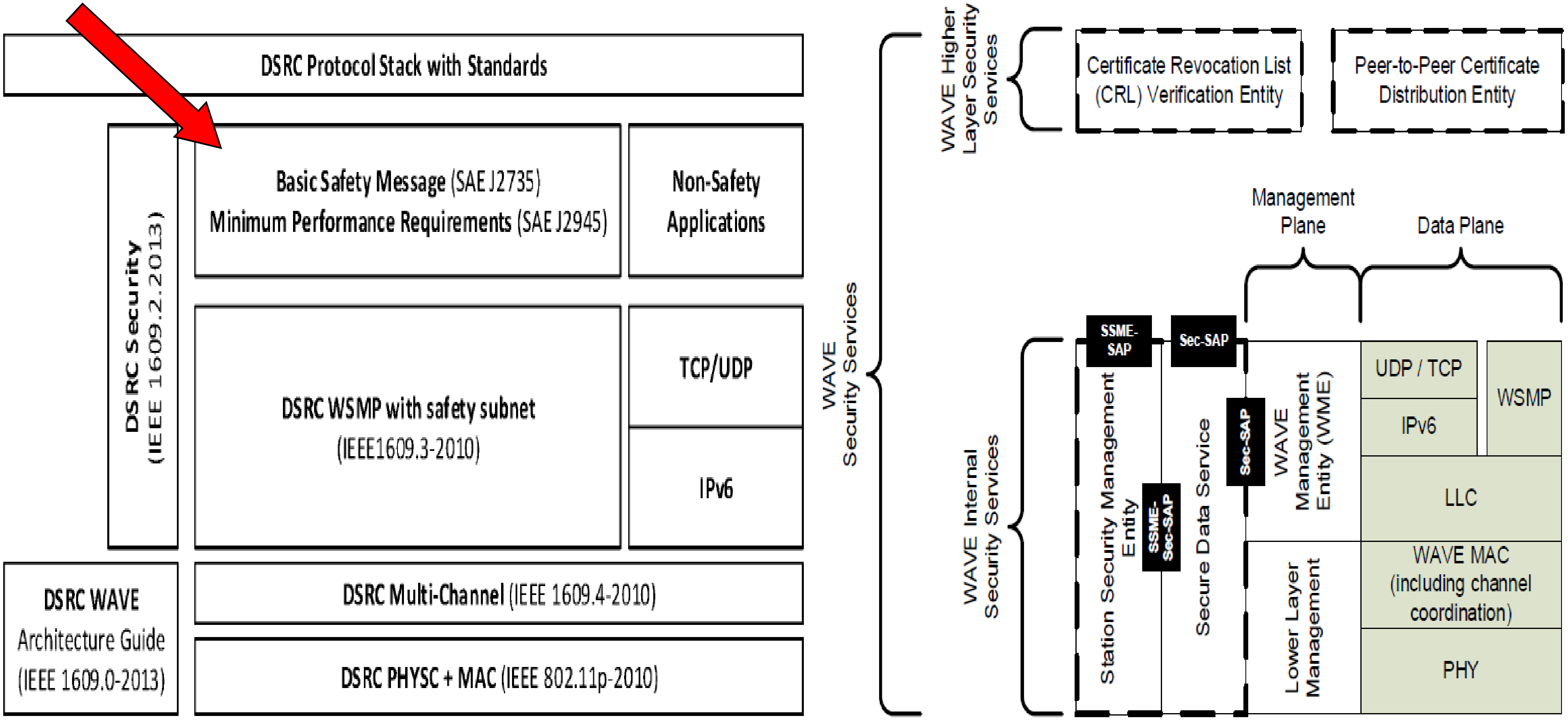
Networking and Service Managements Features addressed in the IEEE Standards (1609.0/.3)

Features of 1609.0 and 1609.3	Purpose
WAVE Services (1609.0)	An abstract entity, involving an exchange of data, generally provided by a higher layer entity on one WAVE device to a similar entity on another WAVE device, using WAVE communications. (IEEE Std 1609.3). May also be referred to as a WAVE service in certain contexts.
WAVE Management Entity (WME)	A set of management functions required to provide WAVE Networking Services.
WAVE Service Advertisement (WSA)	A data structure containing information that announces the availability of a service.
WAVE Short Message Protocl (WSMP)	The protocol specified in this standard that minimizes communications overhead
Provider Service Table (PST)	A collection of data describing the applications that are registered with and available though a WAVE device, with supporting channel information.
Provider Service ID (PSID)	A number that identifies a service provided by an application (see IEEE Std 1609.12)
Provider Service Context (PSC)	A field associated with a PSID containing supplementary information related to the service. The format of the PSC is PSID dependent.
Control Channel/Service Channel (CCH/SCH)	CCH – Control Channel. A radio channel used for exchange of management frames and WAVE Short Messages. . SCH – Service Channel. Any channel that is not the control channel

[1] IEEE Vehicular Technology Society, "**IEEE1609.0 (WAVE Architecture)**," IEEE Std

[2] IEEE Vehicular Technology Society, "**IEEE1609.3 (Networking Services)**," IEEE Std

WAVE Protocol stack showing DSRC layers and details of WAVE Security Services


DSRC Protocol Stack with Standards
DSRC Security (IEEE 1609.2.2013)
Basic Safety Message (SAE J2735)
Minimum Performance Requirements (SAE J2945)
Non-Safety Applications
DSRC WSMP with safety subnet (IEEE1609.3-2010)
TCP/UDP
IPv6
DSRC WAVE Architecture Guide (IEEE 1609.0-2013)
DSRC Multi-Channel (IEEE 1609.4-2010)
DSRC PHYSC + MAC (IEEE 802.11p-2010)
WAVE Security Services
WAVE Higher Layer Security Services
Certificate Revocation List (CRL) Verification Entity
Peer-to-Peer Certificate Distribution Entity
Management Plane
Data Plane
WAVE Internal Security Services
SSME-SAP
Sec-SAP
Station Security Management Entity
SSME-Sec-SAP
Secure Data Service
Sec-SAP
WAVE Management Entity (WME)
Lower Layer Management
UDP / TCP
IPv6
WSMP
LLC
WAVE MAC (including channel coordination)
PHY

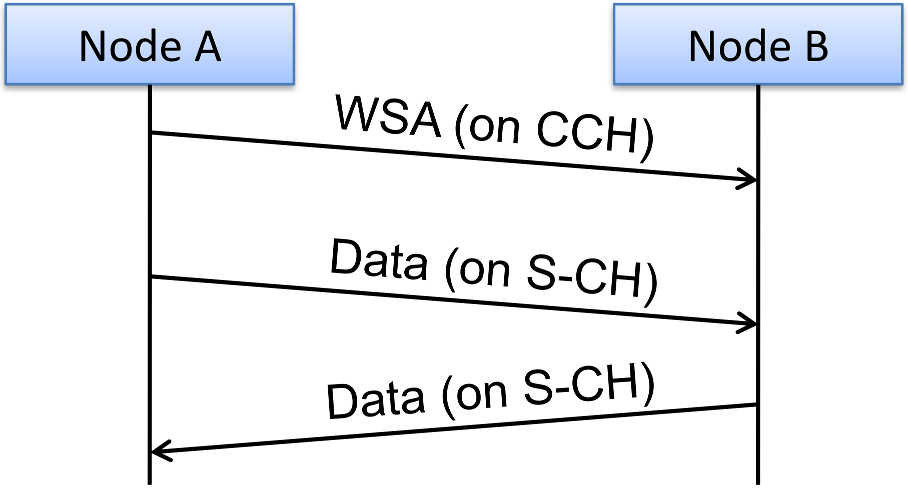
[1] IEEE Vehicular Technology Society, "IEEE1 609.3 (Networking Services)," IEEE Std

WAVE Security Services for Applications and Management Messages (1609.0/1609.2)

Features of 1609.2 and 1609.0	Purpose
Classes of Digital Certificates	**Implicit certificate**: A digital certificate that allows the associated public key to be reconstructed from a reconstruction value and the certificate authority's public key rather than directly providing the associated public key. **Explicit certificate**: A certificate that contains a public key and the certificate authority's signature.
Secure Data Service (SDS)	A subset of 1609.2 services that allow secure data service entities to request communications security services to be applied to secured protocol data units (SPDUs).
Types of Certificates	Enrolment certificate, authorization certificate, certificate authority certificate, end-entity certificate, root certificate, pseudonym certificate, encryption certificate
Bootstrapping Trust	All WAVE equipment are provisioned with a public key that can be used to validate root certificate updates. At the start of bootstrapping, OBE has no SCMS certificates and no knowledge of how to contact the SCMS. At the end of bootstrapping OBE has the following: Certificates and information that allows an OBE to trust the SCMS Credentials and information allowing an OBE to communicate with the SCMS
WAVE Service Advertisement (WSA)	A WAVE system may advertise available services by sending periodic messages known as WAVE Service Advertisements (WSA). Each WSA may include a list of PSIDs for services that are accessible locally via the WAVE protocol stack, as well
End Entity	An entity that is not acting as a Certificate Authority, i.e., an entity that is requesting certificates or signing Protocol Data Units.
Provider Service ID (PSID)	An identifier of an application area. A signed number that identifies a service provided by an application and announced in the WAVE Service Announcement (WSA) PSID
Certificate Signing Requests	A protocol data unit (PDU) sent from an entity to a certificate authority (CA), requesting that the CA issues a certificate on behalf of the entity.
Certificate Revocation Lists	A list identifying certificates that have been revoked. **Revocation**: The publication by a relevant authority of the information that a particular certificate is no onger to be trusted.
Pseudonymity	A property wherein an entity's permanent or long-lived identities, and its long-term patterns of behavior, cannot be deduced from its network traffic and are only observable by appropriately authorized parties.
Cryptographic Mechanisms	Elliptic Curve Digital Signature Algorithm (ECDSA) for signing and the Elliptic Curve Integrated Encryption Scheme (ECIES) for encryption

IEEE 1609

- WAVE service advertisement (WSA)
  - Broadcast on Control Channel (CCH)
  - Identifies WAVE BSSs on Service Channels (SCHs)
  - Can be sent at arbitrary times, by arbitrary nodes
  - Only possibility to make others aware of data being sent on SCHs, as well as the required channel parameters to decode them



1). F. Dressler, C. Sommer, Vehicular Networking

IEEE 1609

- WAVE service advertisement (WSA)
  - WAVE Version (= 0)
  - Provider Service Table (PST)
    - n × Provider Service Info
      - Provider Service Identifier (PSID, max. 0x7FFF FFFF)
      - Provider Service Context (PSC, max. 31 chars)
      - Application priority (max priority: 63)
      - (opt.: IPv6 address and port, if IP service)
      - (opt.: Source MAC address, if sender ≠ data source)
      - Channel number (max. 200)
    - 1..n × Channel Info (for each channel used in PST table)
      - Data rate (fixed or minimum value)
      - Transmission power (fixed or maximum value)
  - (opt.: WAVE Routing Announcement)

[1] IEEE Vehicular Technology Society, "**IEEE 1609.3 (Networking Services)**," IEEE Std

WAVE Service Announcement (WSA) 1 of 2

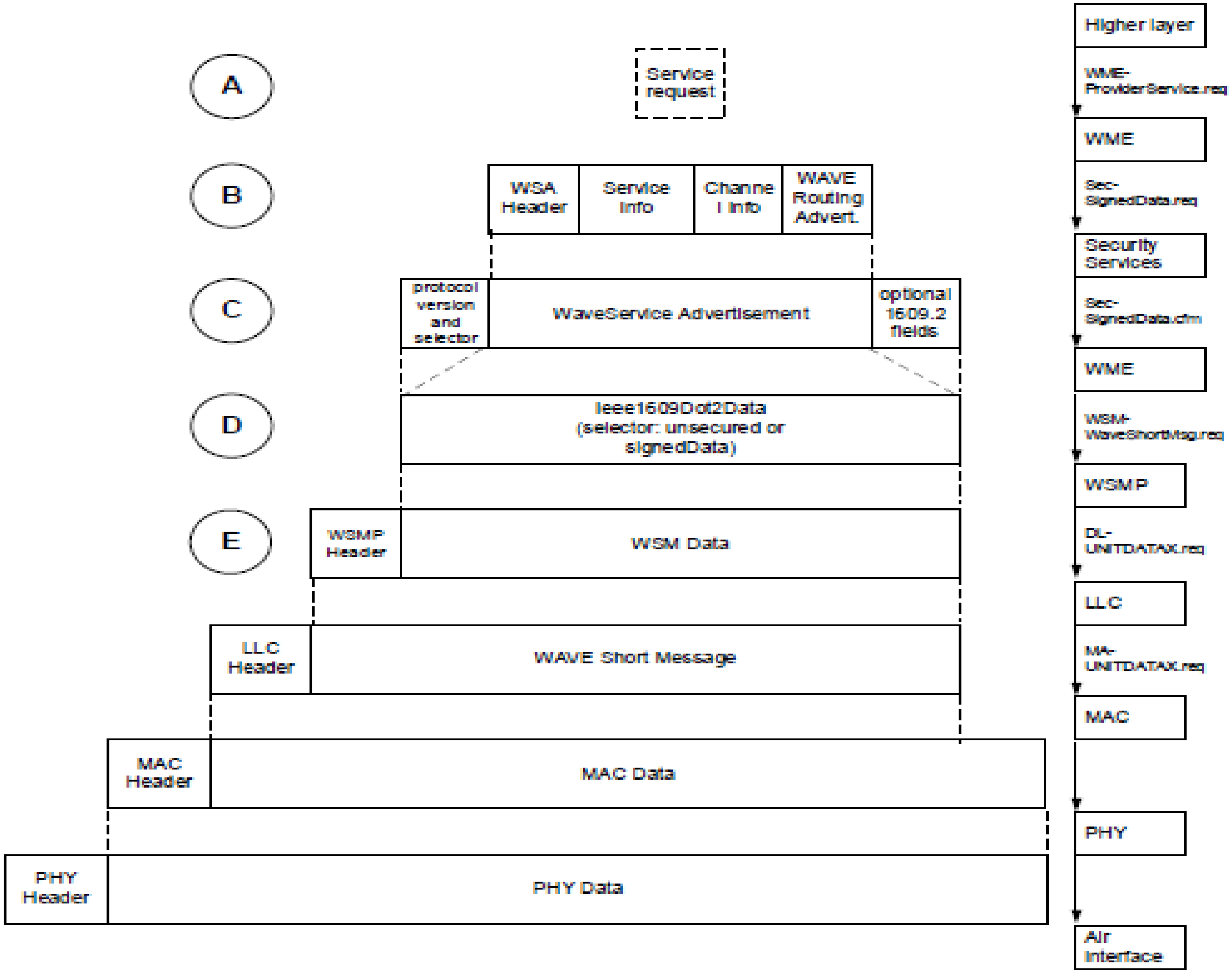
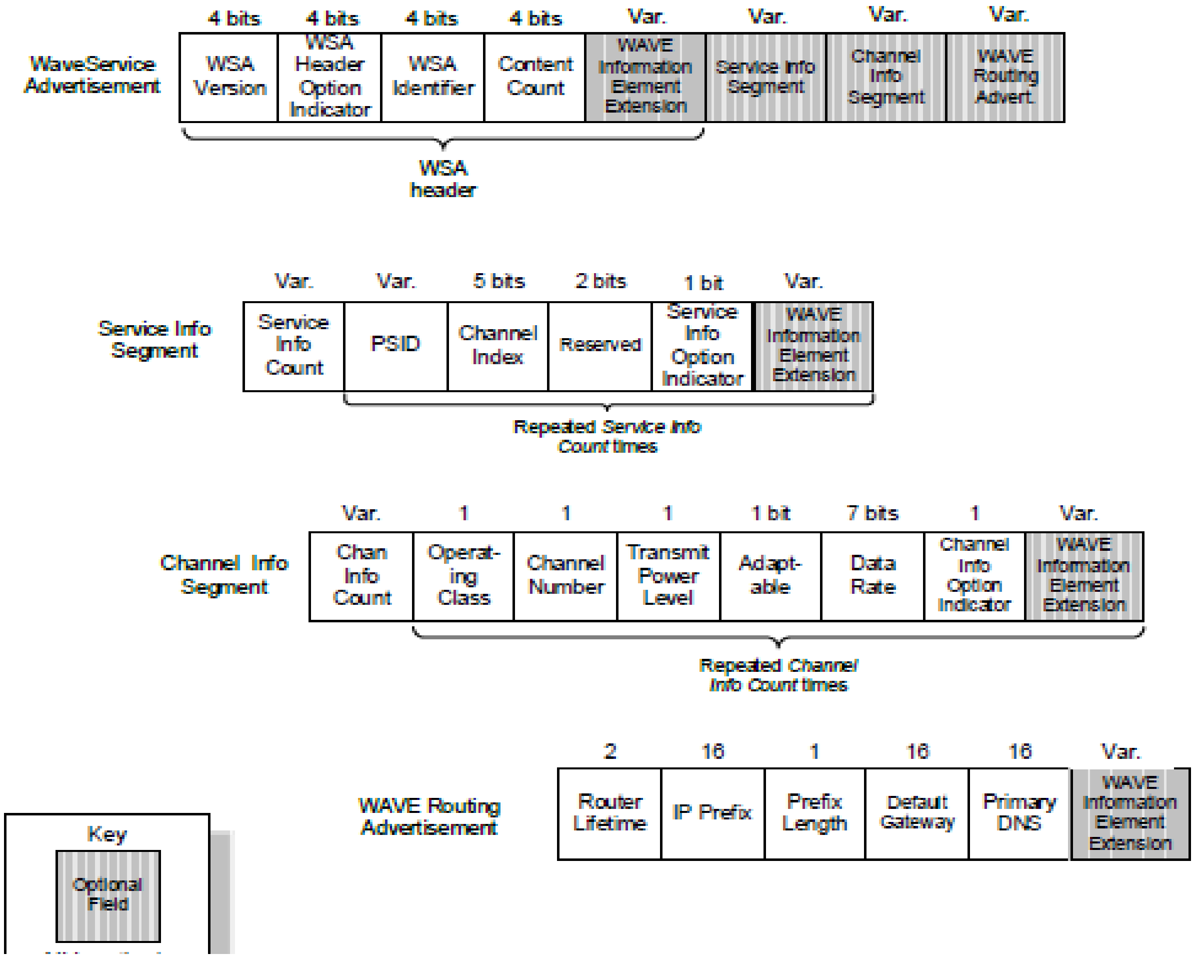


Figure 13— Building the WSA

[1] IEEE Vehicular Technology Society, "IEEE1609.3 (Networking Services)," IEEE Std

WAVE Service Announcement (WSA) 2 of 2



	4 bits	4 bits	4 bits	4 bits	Var.	Var.	Var.	Var.
WaveService Advertisement	WSA Version	WSA Header Option Indicator	WSA Identifier	Content Count	WAVE Information Element Extension	Service Info Segment	Channel Info Segment	WAVE Routing Advert.

WSA header

	Var.	Var.	5 bits	2 bits	1 bit	Var.
Service Info Segment	Service Info Count	PSID	Channel Index	Reserved	Service Info Option Indicator	WAVE Information Element Extension

Repeated *Service Info Count* times

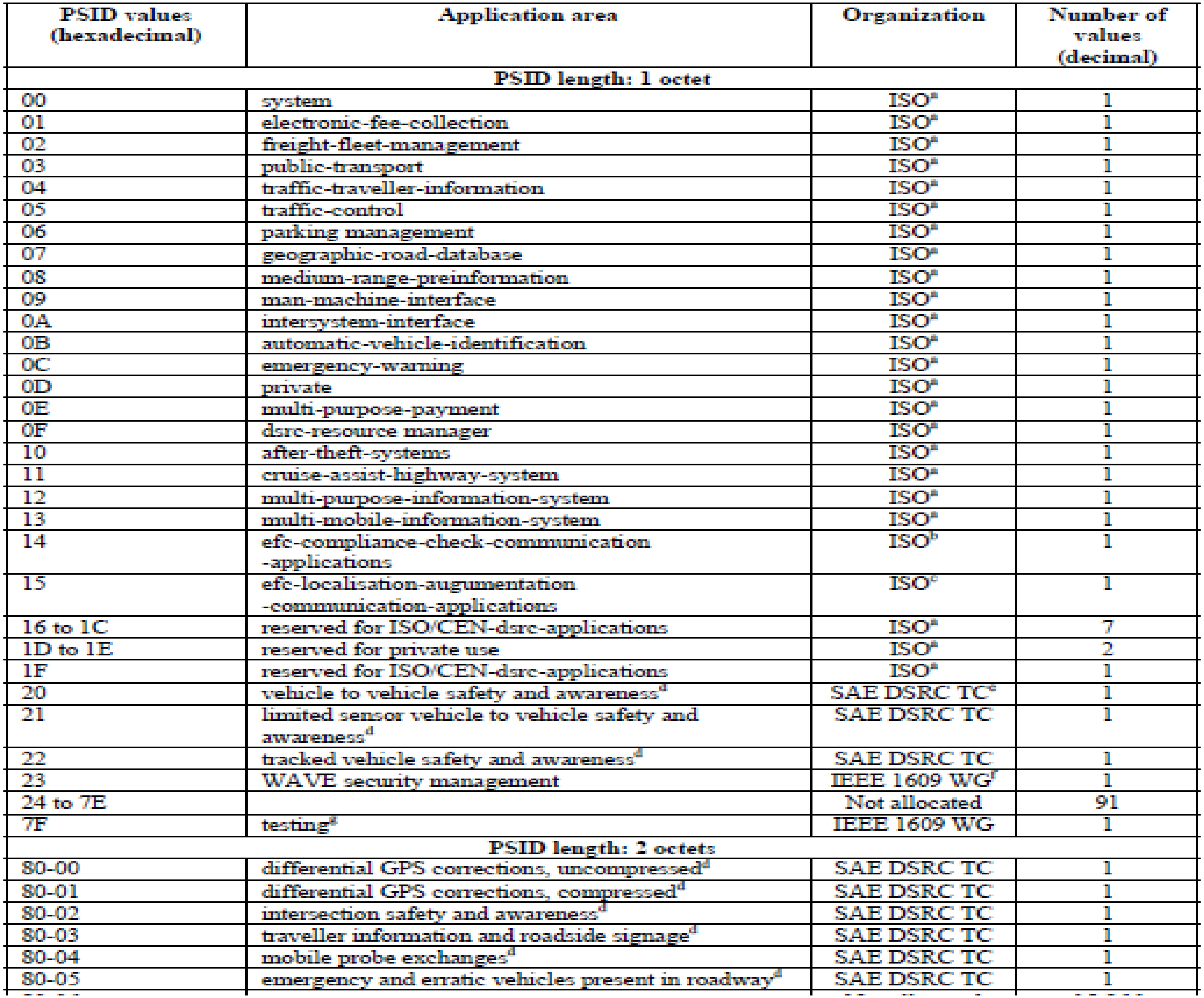
	Var.	1	1	1	1 bit	7 bits	1	Var.
Channel Info Segment	Chan Info Count	Operat-ing Class	Channel Number	Transmit Power Level	Adapt-able	Data Rate	Channel Info Option Indicator	WAVE Information Element Extension

Repeated *Channel Info Count* times

	2	16	1	16	16	Var.
WAVE Routing Advertisement	Router Lifetime	IP Prefix	Prefix Length	Default Gateway	Primary DNS	WAVE Information Element Extension

[1] IEEE Vehicular Technology Society, "IEEE1609.0 (WAVE Architecture)," IEEE Std

Provider Service Identifiers (PSID) Allocations – IEEE 1609.12



PSID values (hexadecimal)	Application area	Organization	Number of values (decimal)
	PSID length: 1 octet		
00	system	ISO[a]	1
01	electronic-fee-collection	ISO[a]	1
02	freight-fleet-management	ISO[a]	1
03	public-transport	ISO[a]	1
04	traffic-traveller-information	ISO[a]	1
05	traffic-control	ISO[a]	1
06	parking management	ISO[a]	1
07	geographic-road-database	ISO[a]	1
08	medium-range-preinformation	ISO[a]	1
09	man-machine-interface	ISO[a]	1
0A	intersystem-interface	ISO[a]	1
0B	automatic-vehicle-identification	ISO[a]	1
0C	emergency-warning	ISO[a]	1
0D	private	ISO[a]	1
0E	multi-purpose-payment	ISO[a]	1
0F	dsrc-resource manager	ISO[a]	1
10	after-theft-systems	ISO[a]	1
11	cruise-assist-highway-system	ISO[a]	1
12	multi-purpose-information-system	ISO[a]	1
13	multi-mobile-information-system	ISO[a]	1
14	efc-compliance-check-communication -applications	ISO[b]	1
15	efc-localisation-augumentation -communication-applications	ISO[c]	1
16 to 1C	reserved for ISO/CEN-dsrc-applications	ISO[a]	7
1D to 1E	reserved for private use	ISO[a]	2
1F	reserved for ISO/CEN-dsrc-applications	ISO[a]	1
20	vehicle to vehicle safety and awareness[d]	SAE DSRC TC[e]	1
21	limited sensor vehicle to vehicle safety and awareness[d]	SAE DSRC TC	1
22	tracked vehicle safety and awareness[d]	SAE DSRC TC	1
23	WAVE security management	IEEE 1609 WG[f]	1
24 to 7E		Not allocated	91
7F	testing[g]	IEEE 1609 WG	1
	PSID length: 2 octets		
80-00	differential GPS corrections, uncompressed[d]	SAE DSRC TC	1
80-01	differential GPS corrections, compressed[d]	SAE DSRC TC	1
80-02	intersection safety and awareness[d]	SAE DSRC TC	1
80-03	traveller information and roadside signage[d]	SAE DSRC TC	1
80-04	mobile probe exchanges[d]	SAE DSRC TC	1
80-05	emergency and erratic vehicles present in roadway[d]	SAE DSRC TC	1

[1] IEEE Vehicular Technology Society, "**IEEE1609.12 (Identifier Allocations)**," IEEE Std

SAE Standards Supporting Connected Car Pilot Program (DSRC) **

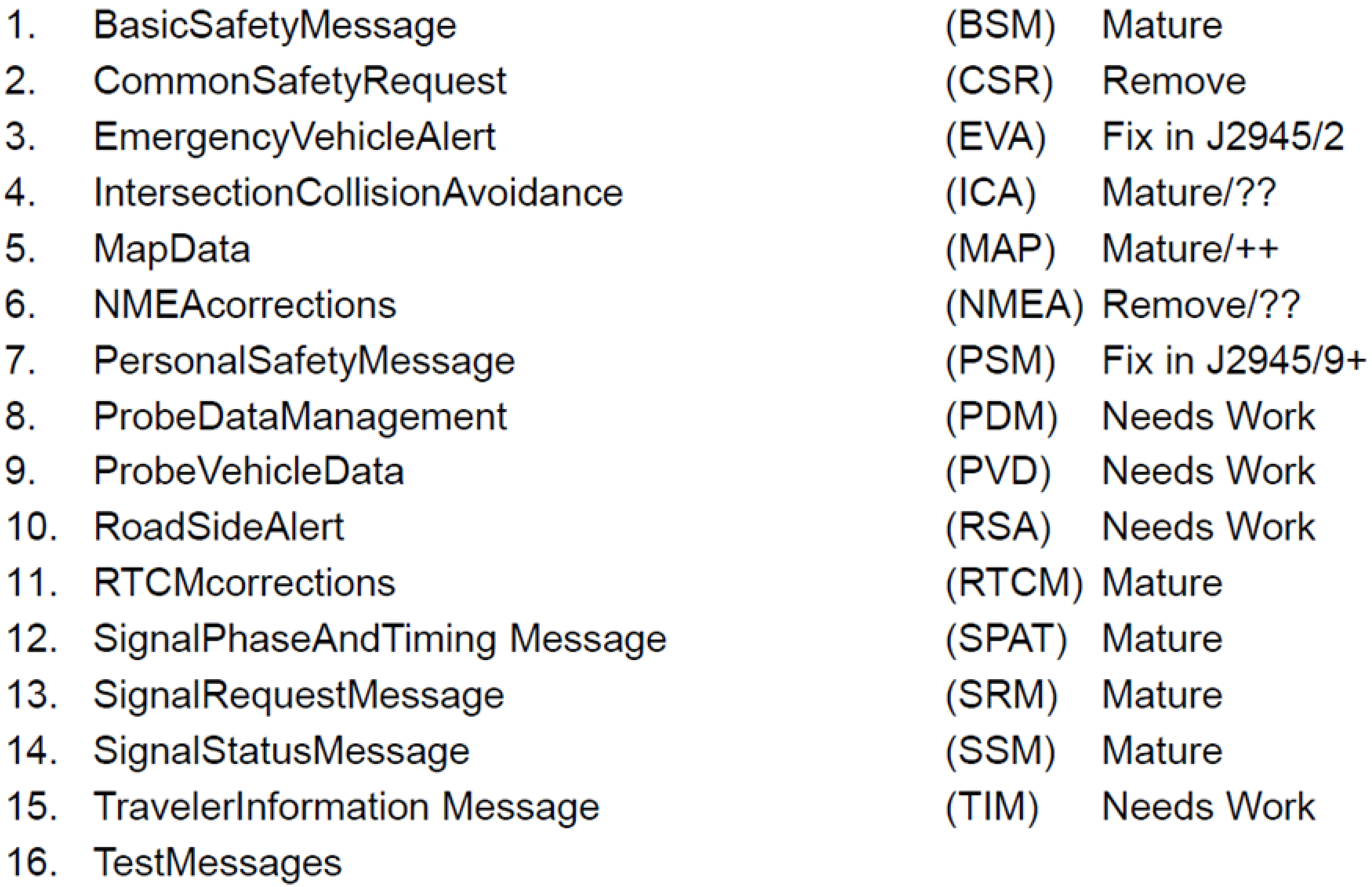
Layers 6, Presentation, and Layers 7, Application, are supported by the two SAE standards that define the elements and the minimum performance requirements for the BSM data elements.

SAE J2735—DSRC Message Set Dictionary specifies a message set, and its data frames and data elements specifically for use by application intended to utilize the 5.9 GHz frequency. For crash avoidance safety, the standard identifies the Basic Safety Message (BSM). The standard includes an extensive list of BSM data elements divided into two parts. Part one includes elements that are transmitted with every message. Part two includes elements that are included in the transmission when there is a change of status. The BSM is exclusive to the support of crash avoidance safety applications. Section III.E identifies the BSM elements that are identified as minimum performance requirements for V2V devices.

SAE J2945—DSRC Minimum Performance Requirements—This standard resulted from research indicating a need for a separate standard that would describe the specific requirements for the data elements that would be used in the BSM. The standard will also cover other DSRC messages; however, the first part of the standard will specify the performance requirements for the BSM data elements. The draft of the first part of the standard is being developed using results of V2V research. The standard for BSM performance requirements is scheduled to be completed and balloted late 2015. The standards explained above represent voluntary consensus standards that have been developed by standards development organization. These standards are not regulatory. These standards, however, do provide a basis of investigation as to what is needed in relation to identifying the minimum performance requirements that if met ensure the proper and safe functionality of V2V DSRC device that will result in the avoidance of crashes.

** 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,

J2735 Messages



1.	BasicSafetyMessage	(BSM)	Mature
2.	CommonSafetyRequest	(CSR)	Remove
3.	EmergencyVehicleAlert	(EVA)	Fix in J2945/2
4.	IntersectionCollisionAvoidance	(ICA)	Mature/??
5.	MapData	(MAP)	Mature/++
6.	NMEAcorrections	(NMEA)	Remove/??
7.	PersonalSafetyMessage	(PSM)	Fix in J2945/9+
8.	ProbeDataManagement	(PDM)	Needs Work
9.	ProbeVehicleData	(PVD)	Needs Work
10.	RoadSideAlert	(RSA)	Needs Work
11.	RTCMcorrections	(RTCM)	Mature
12.	SignalPhaseAndTiming Message	(SPAT)	Mature
13.	SignalRequestMessage	(SRM)	Mature
14.	SignalStatusMessage	(SSM)	Mature
15.	TravelerInformation Message	(TIM)	Needs Work
16.	TestMessages		

[1] J. Misener, SAE Connected Vehicle Standards, CES 2016, Jan 2016

Field trials and deployments running v2 versions of the WAVE standards (2010-2013) IEEE 1609.0 (Appendix F)

Scalability tests run by the Vehicle Safety Communications 3 (VSC3) consortium, which have involved up to 200 vehicles in 2011–2013.

New York State Affiliated Test Bed fielded a demo system for the 2008 WorldCongress Technology Showcase with 22 RSUs on I-495 corridor and in Manhattan..

Michigan Affiliated Test Bed, on the same site as the VII POC.

Anthem, Arizona, with six pole mounted RSUs integrated with signal controllers, and OBUs deployed in emergency response vehicles.

Palo Alto, California, with RSUs mounted along El Camino Real and OBUs in personal vehicles, transit buses and commercial trucks. Applications include traveler information, electronic payment, ramp metering and curve over-speed warning.

Orlando, Florida, demo system at the 18th World Congress Technology Showcase, with 24 RSUs.

Minnesota deployments including 500 volunteer vehicles and 80 snow plows.

Two testbeds in Virgina support a mix of vehicular types and dozens of RSUs.

[1] IEEE Vehicular Technology Society, "IEEE1609.0 (WAVE Architecture)," IEEE Std

Ongoing field trials and deployments running v3 versions of the WAVE) IEEE 1609.0 (Appendix F)

A follow-on project to the Safety Pilot Model Deployment began in 2015. This project is the Connected Vehicle Pilot Deployment Program. At the time of writing, up-to-date information about the project is available from http://www.its.dot.gov/pilots/index.htm.

There are three ongoing Connected Vehicle Pilot Deployments planned in New York City, Tampa,and Wyoming. The largest of these, in New York City, is anticipated to grow to 10,000 vehicles and 250 instrumented intersections.

University of Michigan Technology Research Institute (UMTRI), is in the process of upgrading the existing CV implementation located at Ann Arbor, MI. The upgrade will use the latest technology based on v3 (2016) of IEEE Std 1609 and IEEE Std 802.11-2016.

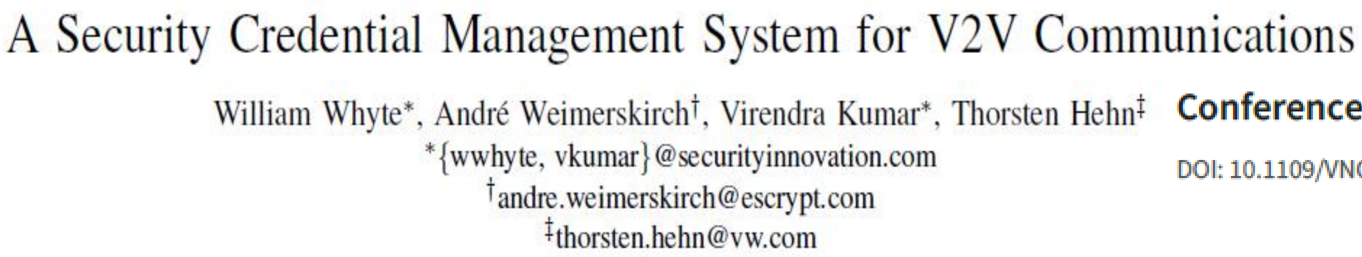
In June 2016, the city of Columbus, Ohio, won the Smart City Challenge sponsored by the USDOT. It is expected that V2V and V2I will be used based on v3 (2016) of IEEE Std 1609 and IEEE Std 802.11-2016. At the time of writing, up-to-date information about the project is available from http://www.transportation.gov/smartcity

[1] IEEE Vehicular Technology Society, "**IEEE1609.0 (WAVE Architecture)**," IEEE Std

Table of Contents

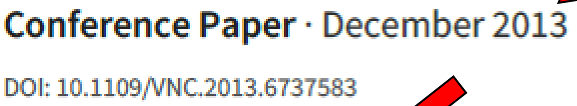
- Testbed and Pilot Programs (2004-2017)
- Evolving the Security and Privacy Model for Connected Car
- Wireless Access for Vehicular Environments (WAVE) Standard
- Secure Credential Management System (SCMS Implementation Details)
- Securing the Basic Safety Message (BSM)

Adoption of V-PKI Models



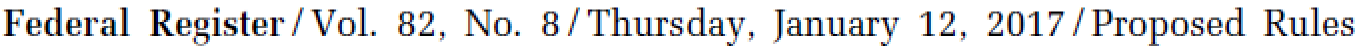
A Security Credential Management System for V2V Communications

William Whyte*, André Weimerskirch†, Virendra Kumar*, Thorsten Hehn‡
*{wwhyte, vkumar}@securityinnovation.com
†andre.weimerskirch@escrypt.com
‡thorsten.hehn@vw.com

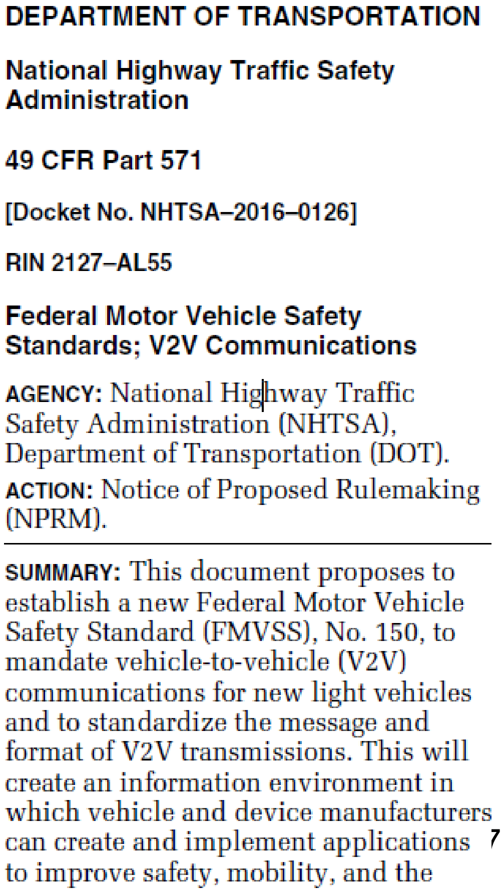


Conference Paper · December 2013

DOI: 10.1109/VNC.2013.6737583



Federal Register / Vol. 82, No. 8 / Thursday, January 12, 2017 / Proposed Rules



DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

49 CFR Part 571

[Docket No. NHTSA–2016–0126]

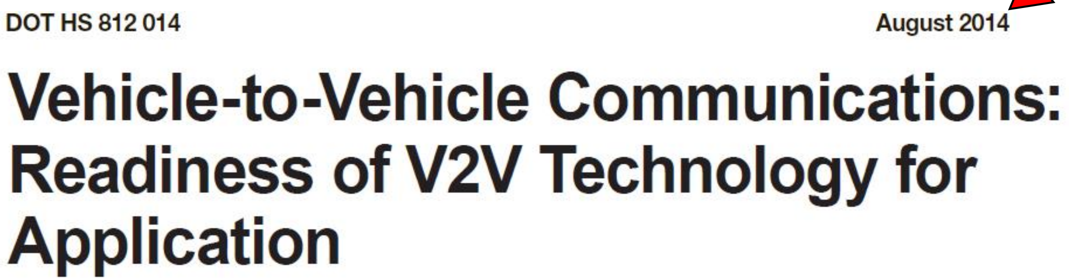
RIN 2127–AL55

Federal Motor Vehicle Safety Standards; V2V Communications

AGENCY: National Highway Traffic Safety Administration (NHTSA), Department of Transportation (DOT).

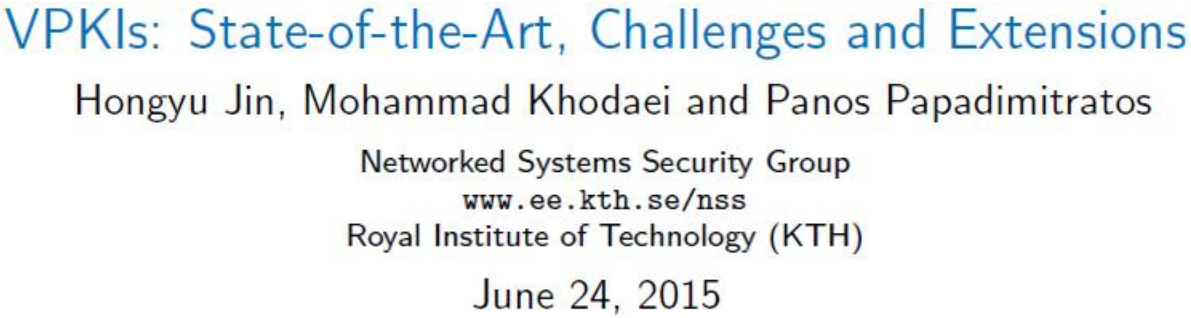
ACTION: Notice of Proposed Rulemaking (NPRM).

SUMMARY: This document proposes to establish a new 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. This will create an information environment in which vehicle and device manufacturers can create and implement applications to improve safety, mobility, and the



DOT HS 812 014 August 2014

Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application



VPKIs: State-of-the-Art, Challenges and Extensions

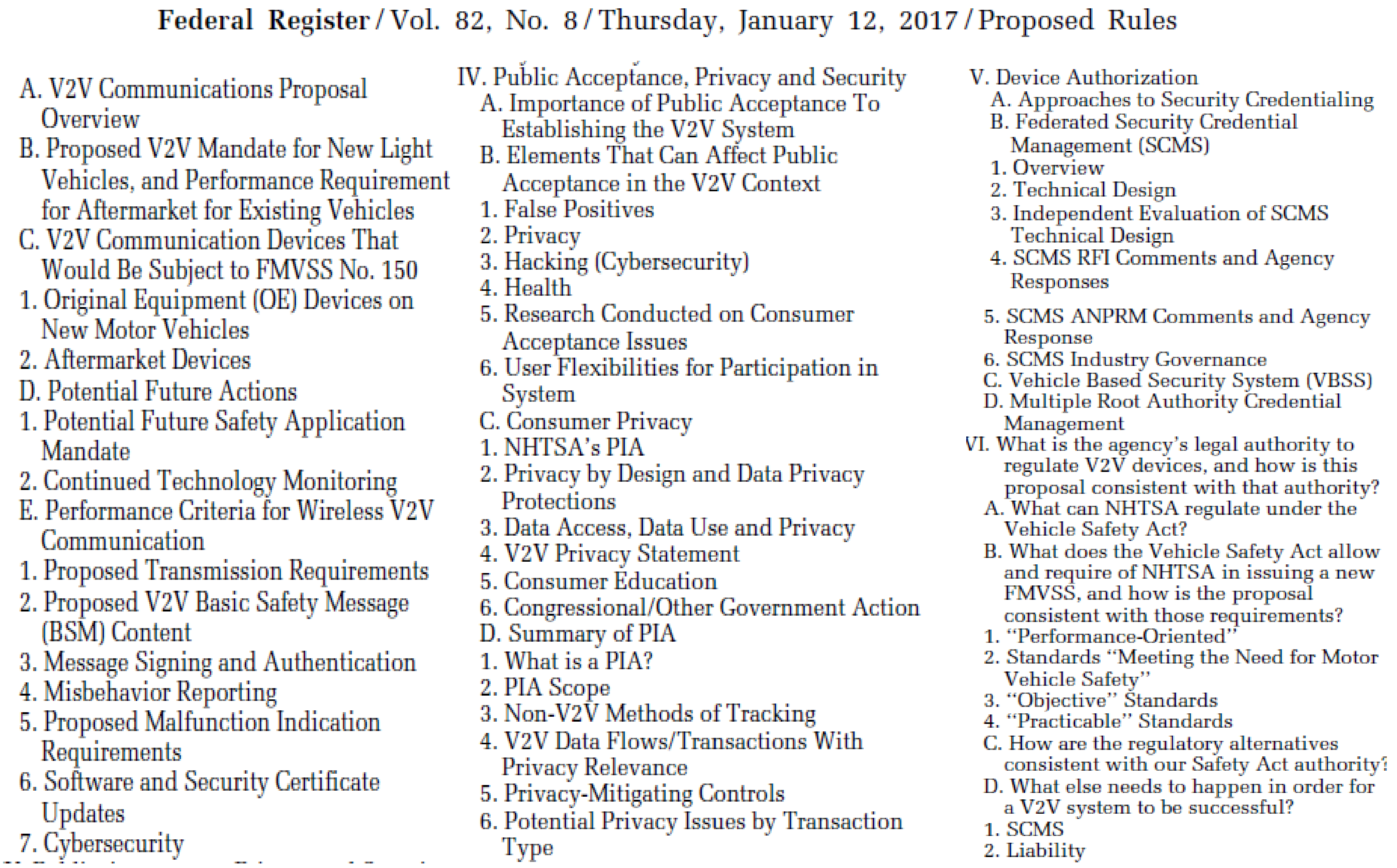
Hongyu Jin, Mohammad Khodaei and Panos Papadimitratos

Networked Systems Security Group
www.ee.kth.se/nss
Royal Institute of Technology (KTH)

June 24, 2015

V2V Requirements from the NHTSA Notice of Proposed Rule Making

https://www.federalregister.gov/documents/2017/01/12/2016-31059/federal-motor-vehicle-safety-standards-v2v-communications



Federal Register / Vol. 82, No. 8 / Thursday, January 12, 2017 / Proposed Rules

A. V2V Communications Proposal Overview
B. Proposed V2V Mandate for New Light Vehicles, and Performance Requirement for Aftermarket for Existing Vehicles
C. V2V Communication Devices That Would Be Subject to FMVSS No. 150
1. Original Equipment (OE) Devices on New Motor Vehicles
2. Aftermarket Devices
D. Potential Future Actions
1. Potential Future Safety Application Mandate
2. Continued Technology Monitoring
E. Performance Criteria for Wireless V2V Communication
1. Proposed Transmission Requirements
2. Proposed V2V Basic Safety Message (BSM) Content
3. Message Signing and Authentication
4. Misbehavior Reporting
5. Proposed Malfunction Indication Requirements
6. Software and Security Certificate Updates
7. Cybersecurity

IV. Public Acceptance, Privacy and Security
A. Importance of Public Acceptance To Establishing the V2V System
B. Elements That Can Affect Public Acceptance in the V2V Context
1. False Positives
2. Privacy
3. Hacking (Cybersecurity)
4. Health
5. Research Conducted on Consumer Acceptance Issues
6. User Flexibilities for Participation in System
C. Consumer Privacy
1. NHTSA's PIA
2. Privacy by Design and Data Privacy Protections
3. Data Access, Data Use and Privacy
4. V2V Privacy Statement
5. Consumer Education
6. Congressional/Other Government Action
D. Summary of PIA
1. What is a PIA?
2. PIA Scope
3. Non-V2V Methods of Tracking
4. V2V Data Flows/Transactions With Privacy Relevance
5. Privacy-Mitigating Controls
6. Potential Privacy Issues by Transaction Type

V. Device Authorization
A. Approaches to Security Credentialing
B. Federated Security Credential Management (SCMS)
1. Overview
2. Technical Design
3. Independent Evaluation of SCMS Technical Design
4. SCMS RFI Comments and Agency Responses
5. SCMS ANPRM Comments and Agency Response
6. SCMS Industry Governance
C. Vehicle Based Security System (VBSS)
D. Multiple Root Authority Credential Management
VI. What is the agency's legal authority to regulate V2V devices, and how is this proposal consistent with that authority?
A. What can NHTSA regulate under the Vehicle Safety Act?
B. What does the Vehicle Safety Act allow and require of NHTSA in issuing a new FMVSS, and how is the proposal consistent with those requirements?
1. "Performance-Oriented"
2. Standards "Meeting the Need for Motor Vehicle Safety"
3. "Objective" Standards
4. "Practicable" Standards
C. How are the regulatory alternatives consistent with our Safety Act authority?
D. What else needs to happen in order for a V2V system to be successful?
1. SCMS
2. Liability

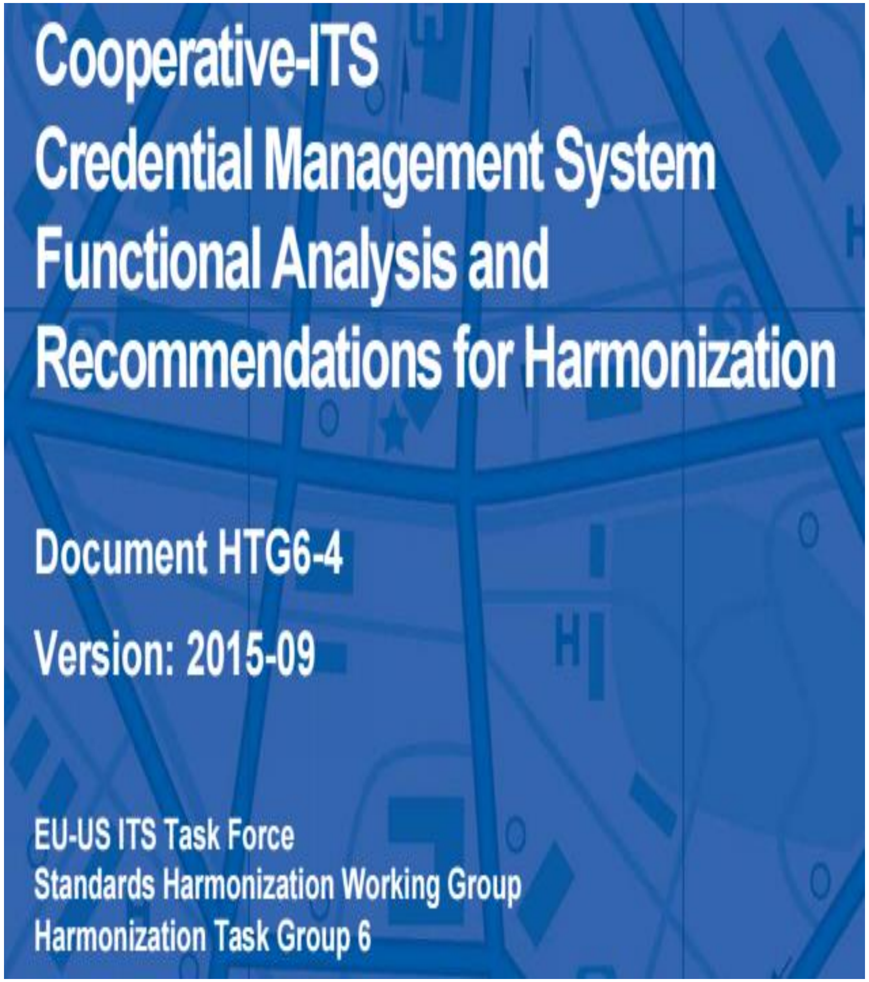
Highlights from the NHTSA Notice of Proposed Rule Making

- SCMS Harmonization with EU CCMS Standards activities
- Privacy Protection (NHTSA PIA) – Inventory of Privacy Controls, Privacy Risk Assessment
- Independent Assessment of CAMP/US DOT Security Design
- Cryptographic Algorithms (and resiliency)
- Misbehavior Authority
- False Positive Detection and Mitigations (US DOT Volpe Center)
- Test Metrics Validation (US DOT Volpe Center)

**** 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,**

SCMS Harmonization with EU CCMS Standards

http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=11398

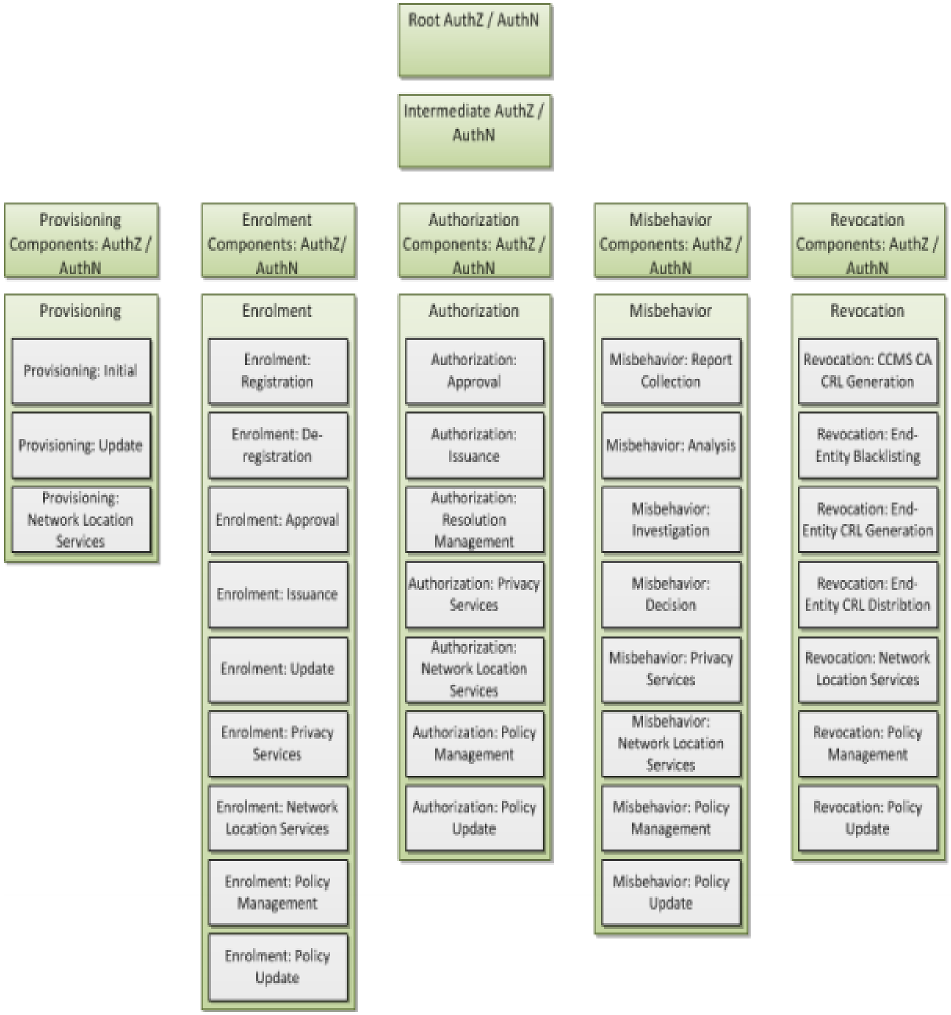


Cooperative-ITS
Credential Management System
Functional Analysis and
Recommendations for Harmonization

Document HTG6-4

Version: 2015-09

EU-US ITS Task Force
Standards Harmonization Working Group
Harmonization Task Group 6



Root AuthZ / AuthN

Intermediate AuthZ / AuthN

Provisioning Components: AuthZ / AuthN
- Provisioning
  - Provisioning: Initial
  - Provisioning: Update
  - Provisioning: Network Location Services

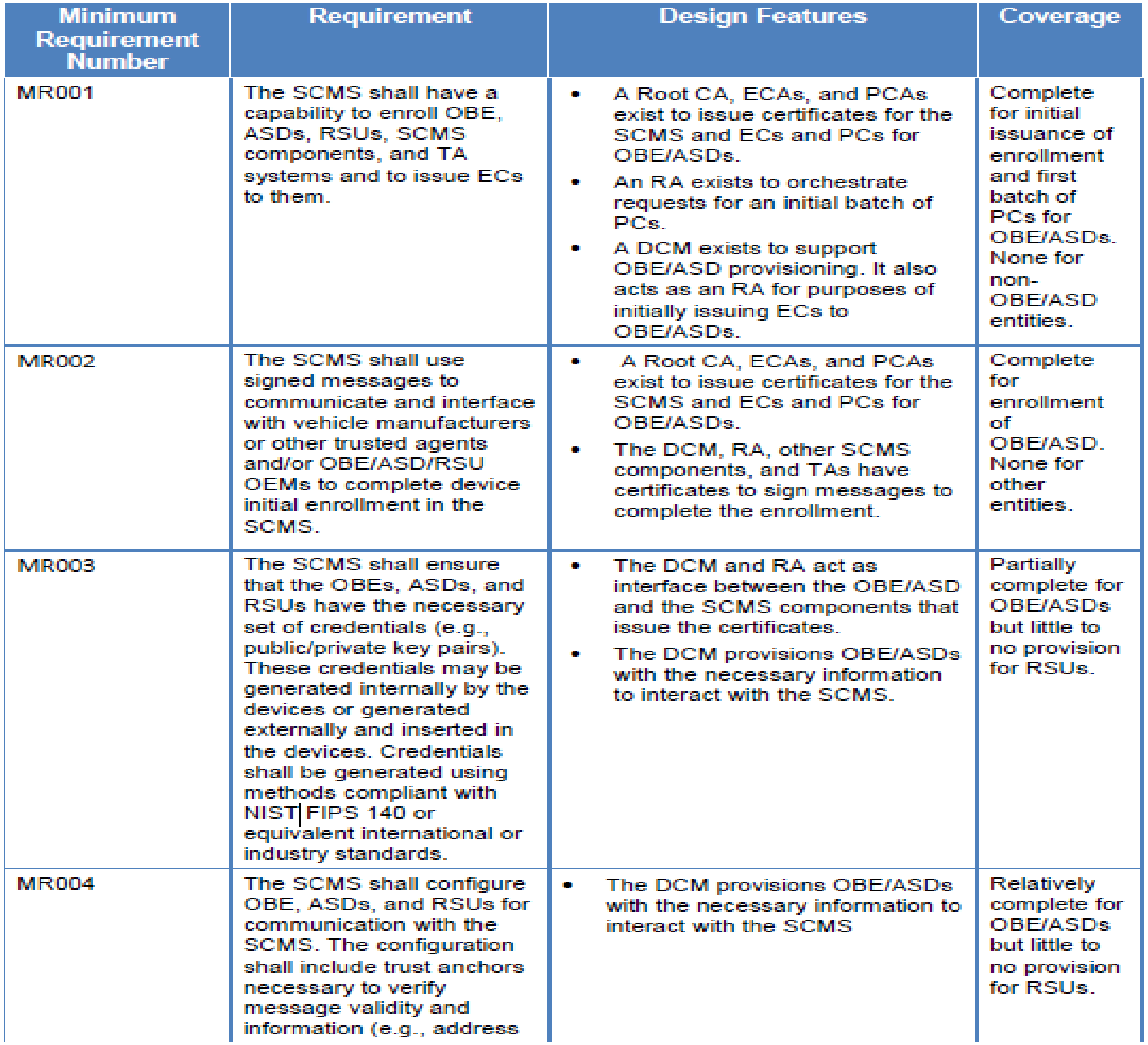
Enrolment Components: AuthZ/ AuthN
- Enrolment
  - Enrolment: Registration
  - Enrolment: De-registration
  - Enrolment: Approval
  - Enrolment: Issuance
  - Enrolment: Update
  - Enrolment: Privacy Services
  - Enrolment: Network Location Services
  - Enrolment: Policy Management
  - Enrolment: Policy Update

Authorization Components: AuthZ / AuthN
- Authorization
  - Authorization: Approval
  - Authorization: Issuance
  - Authorization: Resolution Management
  - Authorization: Privacy Services
  - Authorization: Network Location Services
  - Authorization: Policy Management
  - Authorization: Policy Update

Misbehavior Components: AuthZ / AuthN
- Misbehavior
  - Misbehavior: Report Collection
  - Misbehavior: Analysis
  - Misbehavior: Investigation
  - Misbehavior: Decision
  - Misbehavior: Privacy Services
  - Misbehavior: Network Location Services
  - Misbehavior: Policy Management
  - Misbehavior: Policy Update

Revocation Components: AuthZ / AuthN
- Revocation
  - Revocation: CCMS CA CRL Generation
  - Revocation: End-Entity Blacklisting
  - Revocation: End-Entity CRL Generation
  - Revocation: End-Entity CRL Distribtion
  - Revocation: Network Location Services
  - Revocation: Policy Management
  - Revocation: Policy Update

Assessment of US DOT/CAMP Security Design (MITRE)

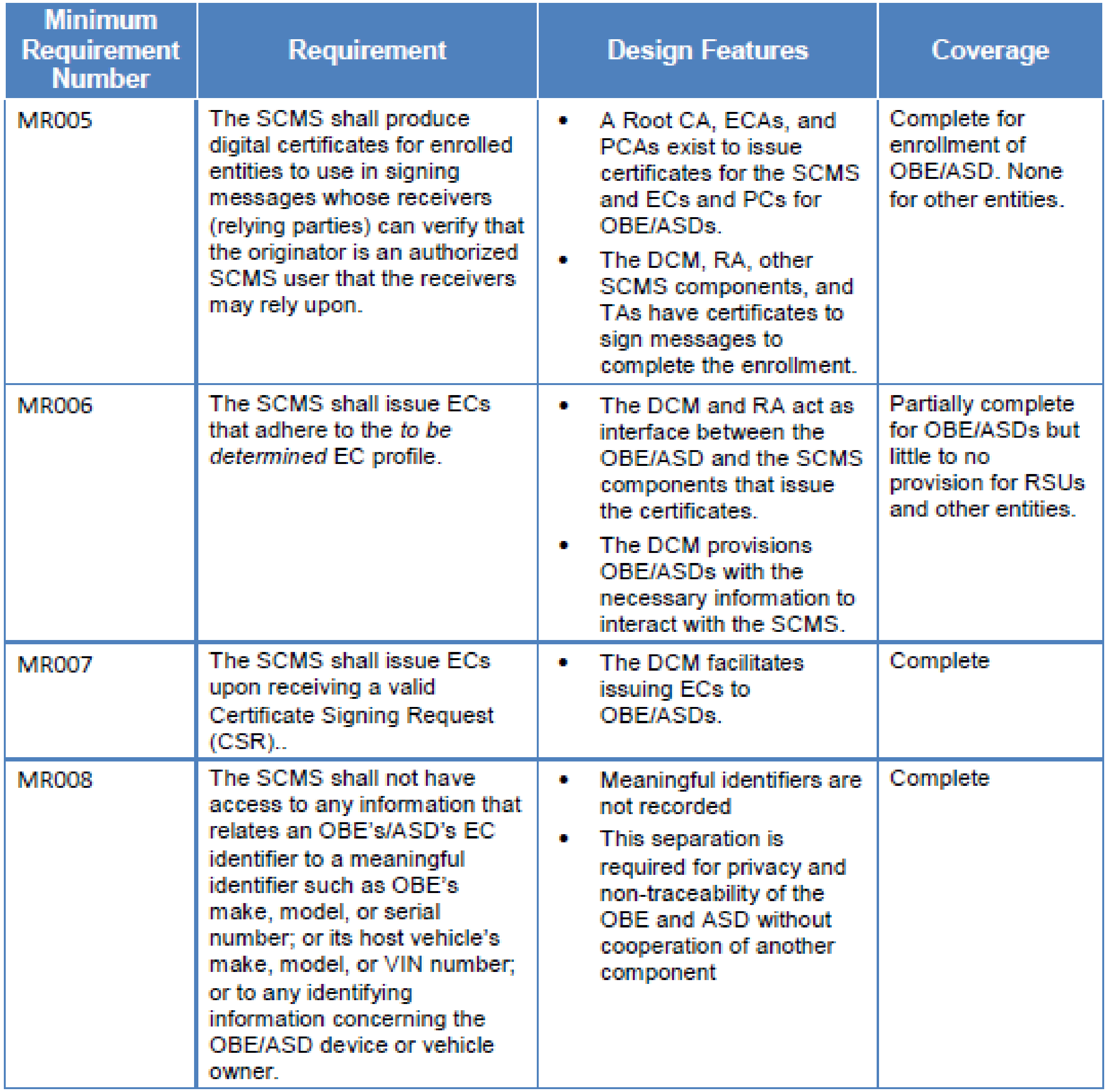


Minimum Requirement Number	Requirement	Design Features	Coverage
MR001	The SCMS shall have a capability to enroll OBE, ASDs, RSUs, SCMS components, and TA systems and to issue ECs to them.	• A Root CA, ECAs, and PCAs exist to issue certificates for the SCMS and ECs and PCs for OBE/ASDs. • An RA exists to orchestrate requests for an initial batch of PCs. • A DCM exists to support OBE/ASD provisioning. It also acts as an RA for purposes of initially issuing ECs to OBE/ASDs.	Complete for initial issuance of enrollment and first batch of PCs for OBE/ASDs. None for non-OBE/ASD entities.
MR002	The SCMS shall use signed messages to communicate and interface with vehicle manufacturers or other trusted agents and/or OBE/ASD/RSU OEMs to complete device initial enrollment in the SCMS.	• A Root CA, ECAs, and PCAs exist to issue certificates for the SCMS and ECs and PCs for OBE/ASDs. • The DCM, RA, other SCMS components, and TAs have certificates to sign messages to complete the enrollment.	Complete for enrollment of OBE/ASD. None for other entities.
MR003	The SCMS shall ensure that the OBEs, ASDs, and RSUs have the necessary set of credentials (e.g., public/private key pairs). These credentials may be generated internally by the devices or generated externally and inserted in the devices. Credentials shall be generated using methods compliant with NIST FIPS 140 or equivalent international or industry standards.	• The DCM and RA act as interface between the OBE/ASD and the SCMS components that issue the certificates. • The DCM provisions OBE/ASDs with the necessary information to interact with the SCMS.	Partially complete for OBE/ASDs but little to no provision for RSUs.
MR004	The SCMS shall configure OBE, ASDs, and RSUs for communication with the SCMS. The configuration shall include trust anchors necessary to verify message validity and information (e.g., address	• The DCM provisions OBE/ASDs with the necessary information to interact with the SCMS	Relatively complete for OBE/ASDs but little to no provision for RSUs.

Final Design Analysis Report ," FHWA-JPO-15-237 in Docket No. NHTSA–2016–0126-0004, Section 4.1.4 (Dec. 2016)
https://www.regulations.gov/document?D=NHTSA-2016-0126-0004

Assessment of US DOT/CAMP Security Design (MITRE) – Certificate Issuance

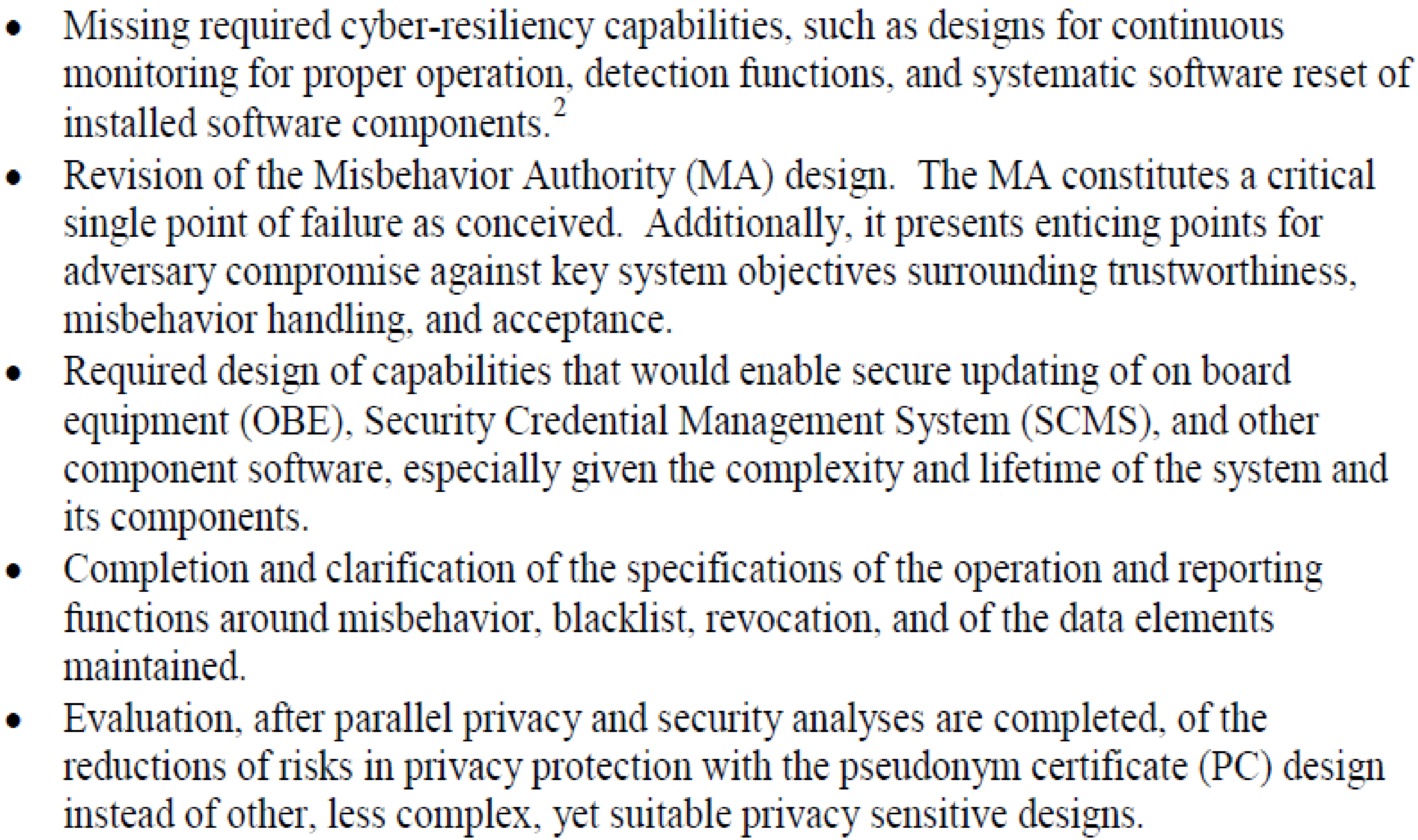
Table 2. Certificate Issuance Requirements and Design Analysis



Minimum Requirement Number	Requirement	Design Features	Coverage
MR005	The SCMS shall produce digital certificates for enrolled entities to use in signing messages whose receivers (relying parties) can verify that the originator is an authorized SCMS user that the receivers may rely upon.	• A Root CA, ECAs, and PCAs exist to issue certificates for the SCMS and ECs and PCs for OBE/ASDs. • The DCM, RA, other SCMS components, and TAs have certificates to sign messages to complete the enrollment.	Complete for enrollment of OBE/ASD. None for other entities.
MR006	The SCMS shall issue ECs that adhere to the *to be determined* EC profile.	• The DCM and RA act as interface between the OBE/ASD and the SCMS components that issue the certificates. • The DCM provisions OBE/ASDs with the necessary information to interact with the SCMS.	Partially complete for OBE/ASDs but little to no provision for RSUs and other entities.
MR007	The SCMS shall issue ECs upon receiving a valid Certificate Signing Request (CSR)..	• The DCM facilitates issuing ECs to OBE/ASDs.	Complete
MR008	The SCMS shall not have access to any information that relates an OBE's/ASD's EC identifier to a meaningful identifier such as OBE's make, model, or serial number; or its host vehicle's make, model, or VIN number; or to any identifying information concerning the OBE/ASD device or vehicle owner.	• Meaningful identifiers are not recorded • This separation is required for privacy and non-traceability of the OBE and ASD without cooperation of another component	Complete

Final Design Analysis Report ," FHWA-JPO-15-237 in Docket No. NHTSA–2016–0126-0004, Section 4.1.4 (Dec. 2016)

Assessment of US DOT/CAMP Security Design (MITRE)



- Missing required cyber-resiliency capabilities, such as designs for continuous monitoring for proper operation, detection functions, and systematic software reset of installed software components.[2]
- Revision of the Misbehavior Authority (MA) design. The MA constitutes a critical single point of failure as conceived. Additionally, it presents enticing points for adversary compromise against key system objectives surrounding trustworthiness, misbehavior handling, and acceptance.
- Required design of capabilities that would enable secure updating of on board equipment (OBE), Security Credential Management System (SCMS), and other component software, especially given the complexity and lifetime of the system and its components.
- Completion and clarification of the specifications of the operation and reporting functions around misbehavior, blacklist, revocation, and of the data elements maintained.
- Evaluation, after parallel privacy and security analyses are completed, of the reductions of risks in privacy protection with the pseudonym certificate (PC) design instead of other, less complex, yet suitable privacy sensitive designs.

Final Design Analysis Report ," FHWA-JPO-15-237 in Docket No. NHTSA–2016–0126-0004, Section 4.1.4 (Dec. 2016)
https://www.regulations.gov/document?D=NHTSA-2016-0126-0004

Privacy Protection

Public Key Infrastructure Proposal:

NHTSA proposes V2V devices sign and verify their basic safety messages using a Public Key Infrastructure (PKI) digital signature algorithm in accordance with performance requirements and test procedures for BSM transmission and the signing of BSMs. The agency believes this will establish a level of confidence in the messages exchanged between vehicles and ensure that basic safety message information is being received from devices that have been certified to operate properly, are enrolled in the security network, and are in good working condition. It is also important that safety applications be able to distinguish these from messages originated by ‘‘bad actors,’’ or defective devices, as well as from messages that have been modified or changed while in transit.

**** 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,**

Privacy Protection

The system will not collect or store any data directly identifying specific individuals or their vehicles, nor will it enable the government to do so. There is no information in the safety messages exchanged by vehicles or collected by the V2V system that directly identifies the driver of a speeding or erratic vehicle for law enforcement purposes, or to third parties. The system—expected to be operated by private entities—will make it difficult to track through space and time specific vehicles, owners or drivers on a persistent basis. Third parties attempting to use the system to track a vehicle would find that it requires significant resources and effort to do so, particularly in light of existing means available for that purpose.

The system will not collect financial information, personal communications, or other information directly linked to individuals. The system will enroll V2V enabled vehicles automatically, without collecting any information that identifies specific vehicles or owners. The system will not provide a ‘‘pipe’’ into the vehicle for extracting data. The system is designed to enable NHTSA and motor vehicle manufacturers to find lots or production runs of potentially defective V2V equipment without use of VIN numbers or other information that could identify specific drivers or vehicles.

**** 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,**

Linkability – Comments on the SCMS Design

NHTSA asks whether "any data element (or combination of data elements) currently in the Basic Safety Message (BSM) is reasonably linkable to an individual on a persistent basis?"[3] We argue that the answer is, unfortunately, "yes." BSMs from a single vehicle will be linkable to each other and to the individual who drives the vehicle via a variety of readily available, inexpensive means.

- Linking a vehicle to an individual: The NPRM proposes that vehicle location accurate to within 1.5 meters be included in every BSM. Such high accuracy is sufficient to identify a vehicle's specific parking spot. Assuming a suburban environment where the parking spot is a driveway, this information is enough to identify the owners or tenants of the unit through the use of a geographic information system and public address data, thus linking a vehicle to a person or a household

- Linking BSMs to construct a pattern of vehicle movement : Linking by Observing the Moment when IDs and Certificates Change The temporary ID and the security certificate, with their five-minute lifetimes, make it trivial to link BSMs until these values change. Moreover, linking BSMs observed shortly before and after the changeover of these values presents only a minor challenge. Speed, heading, acceleration, and yaw data provide enough information that two BSMs sent within a short time of each other can be linked together based on location (at 60 miles per hour, a vehicle travels only about 2.7m between two consecutive BSMs, which are sent at every 0.1 seconds

Comments on NHTSA Notice of Proposed Rule for FMVSS No. 150, V2V Communications (Docket No. NHTSA-2016-0126)
Submitted by Professors Leonid Reyzin, Anna Lysyanskaya, Vitaly Shmatikov, and Adam D. Smith and the Center for Democracy & Technology

Linkability - Comments on the SCMS Design

- Linking through security certificates - The proposed security certificates present an additional possibility for linking across days and hours, even when observation is sporadic and linking based on other attributes is unreliable. NHTSA proposes a system where each vehicle will have 20 valid security certificates each week to “strike a balance between privacy and efficiency.” All BSMs sent with these certificates are linkable regardless of whether the moment of certificate changeover is observed. Furthermore, assuming a vehicle is driven for about 1 hour per day, we expect about 84 certificate changeovers to happen during a week. It is enough to observe only a portion of those changeovers in order to link most of the 20 weekly certificates together

- Linking through other vehicles - In a high-density highway traffic scenario, BSMs from the same vehicle can also be linked with high confidence based on the vehicles immediately before and after it in its lane, because the order of vehicles in a lane often persists for a few minutes

Privacy Issues in the SCMS Design

- Much of the complexity of the SCMS design is driven by privacy concerns which dictate that individual persons or vehicles not be identifiable based on broadcast message contents, and tracking vehicles or their operators over extended periods of time. The design recognizes that the certificates used for establishing trust in BSMs can act as unique identifiers which would violate the privacy goals and therefore uses a method of frequently changing pseudonym certificates (PCs) in order to eliminate long-term certificates as persistent identifiers.

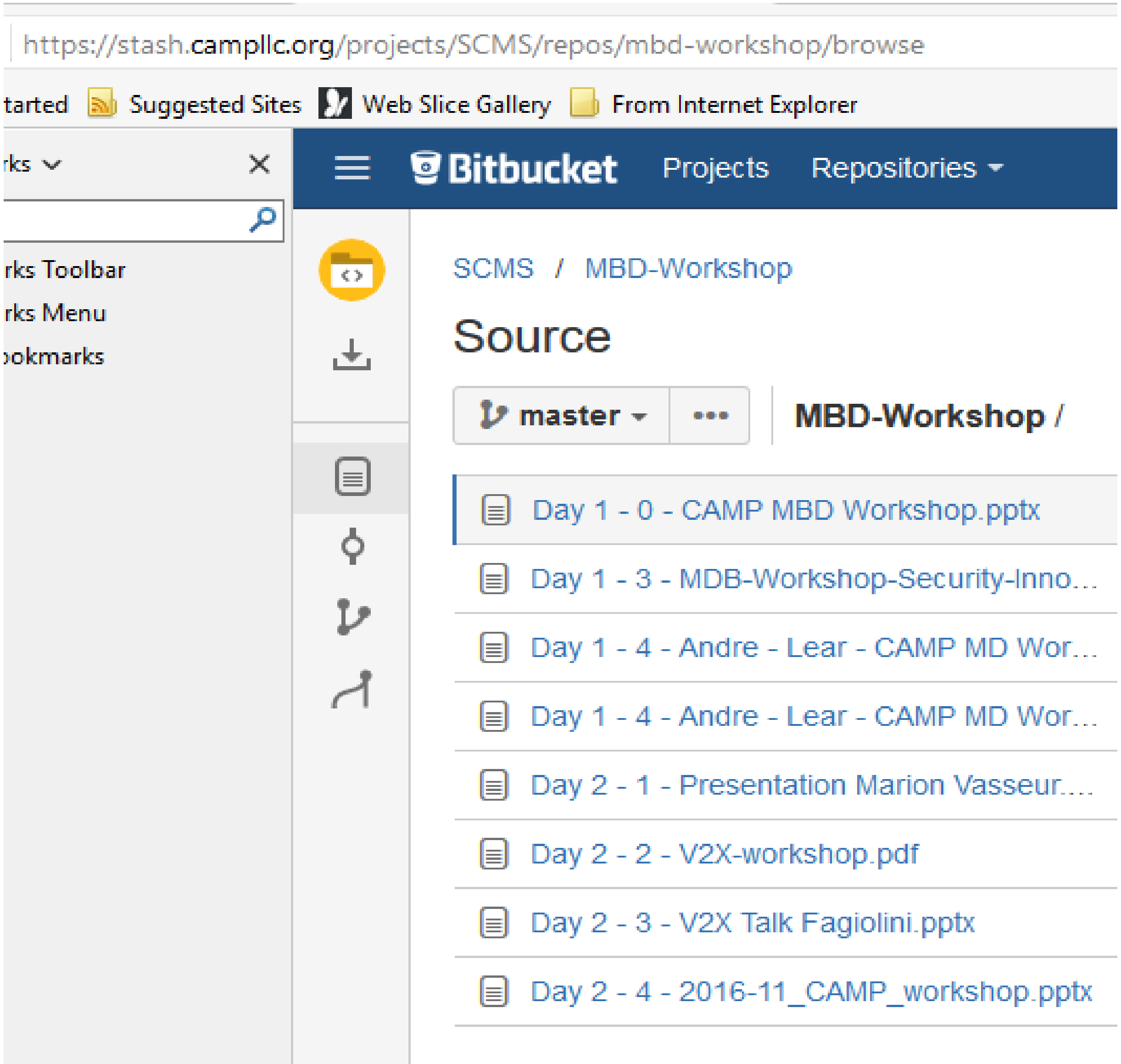
- However, privacy may also be impacted by factors other than long-term certificates, including exploitation of necessary data fields in the messages and transmission protocols (such as position coordinates and direction, or certificate expiration times) and it is difficult to know without further evaluation whether such factors offset the benefit provided by the frequently changing PC approach. Further analysis should be performed to investigate these risks and the degree of difficulty in exploitation to determine if these factors do, in fact, pose a long-term tracking threat despite frequent pseudonym certificate changes.

- Should such analysis conclude that the pseudonym certificate scheme does not significantly reduce the risk of tracking, then the SCMS design complexity, especially that of the pseudonym certificate design, should be reduced. Linking through other vehicles - In a high-density highway traffic scenario, BSMs from the same vehicle can also be linked with high confidence based on the vehicles immediately before and after it in its lane, because the order of vehicles in a lane often persists for a few minutes

Comments on NHTSA Notice of Proposed Rule for FMVSS No. 150, V2V Communications (Docket No. NHTSA-2016-0004) SCMS Design Analysis Report, FHWA-JPO-15-237

CAMP Misbehavior Detection Workshop Presentations

https://stash.campllc.org/projects/SCMS/repos/mbd-workshop/browse



https://stash.campllc.org/projects/SCMS/repos/mbd-workshop/browse

SCMS / MBD-Workshop

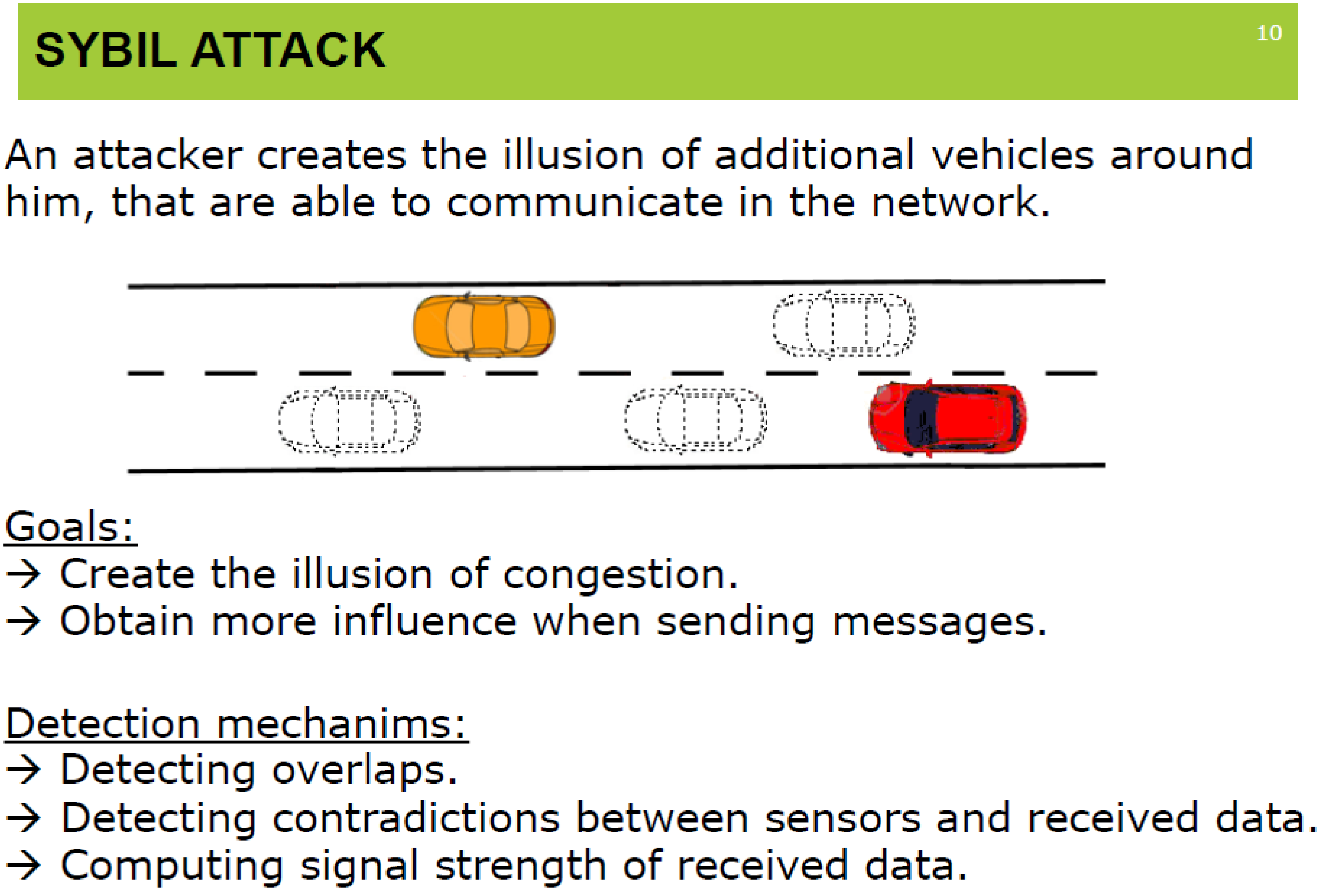
Source

MBD-Workshop /

- Day 1 - 0 - CAMP MBD Workshop.pptx
- Day 1 - 3 - MDB-Workshop-Security-Inno...
- Day 1 - 4 - Andre - Lear - CAMP MD Wor...
- Day 1 - 4 - Andre - Lear - CAMP MD Wor...
- Day 2 - 1 - Presentation Marion Vasseur....
- Day 2 - 2 - V2X-workshop.pdf
- Day 2 - 3 - V2X Talk Fagiolini.pptx
- Day 2 - 4 - 2016-11_CAMP_workshop.pptx

CAMP Misbehavior Detection Workshop Presentations

https://stash.campllc.org/projects/SCMS/repos/mbd-workshop/browse



SYBIL ATTACK

10

An attacker creates the illusion of additional vehicles around him, that are able to communicate in the network.

Goals:

→ Create the illusion of congestion.
→ Obtain more influence when sending messages.

Detection mechanims:

→ Detecting overlaps.
→ Detecting contradictions between sensors and received data.
→ Computing signal strength of received data.

** M. Vasseur, "Misbehavior Detection in C-ITS)", CAMP Workshop on Misbehavior Detection - https://stash.campllc.org/projects/SCMS/repos/mbd-workshop/browse/Day%202%20-%201%20-%20Presentation%20Marion%20Vasseur.pdf

Table of Contents

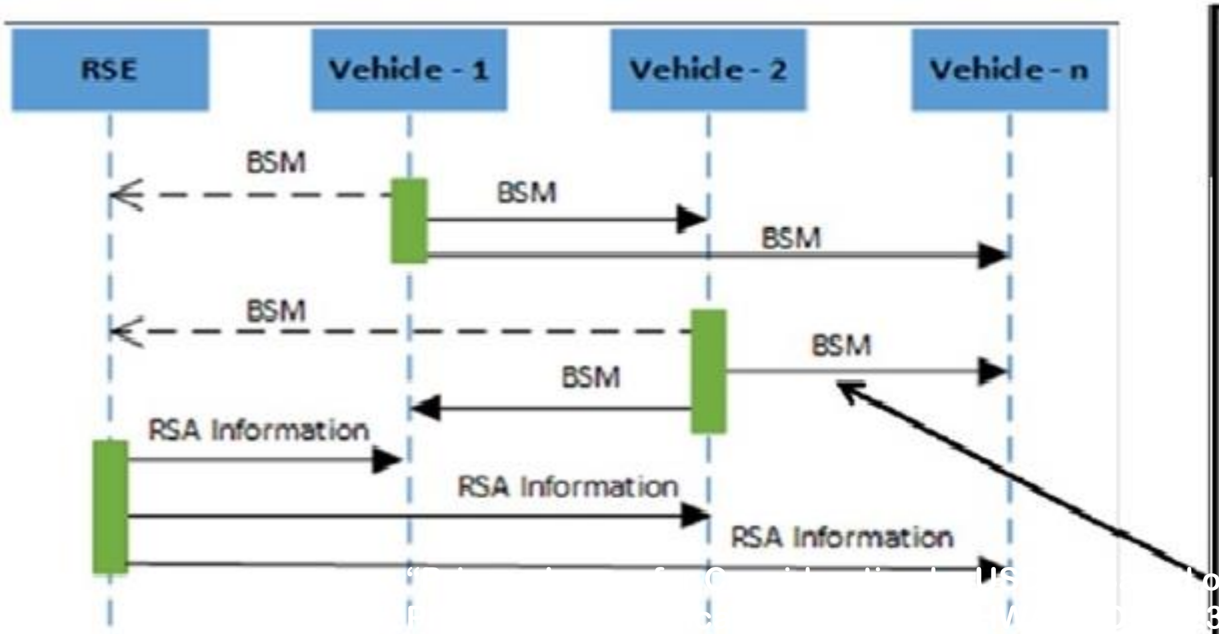
- Testbed and Pilot Programs (2004-2017)
- Evolving the Security and Privacy Model for Connected Car
- Wireless Access for Vehicular Environments (WAVE) Standard
- Secure Credential Management System (SCMS Implementation Details)
- Securing the Basic Safety Message (BSM)

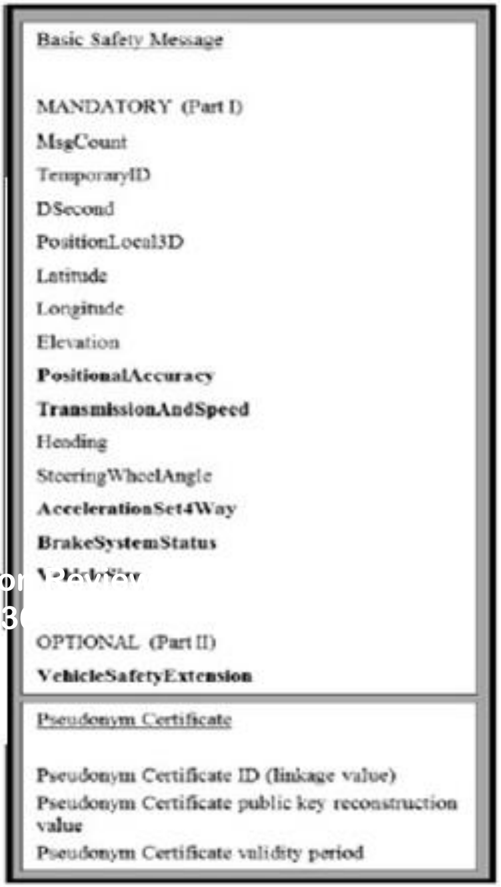
BSM Highlights from the NHTSA Notice of Proposed Rule Making

- Basic Safety Message Definition
- Privacy Protection (NHTSA PIA) – Inventory of Privacy Controls, Independent Assessment of CAMP/US DOT Privacy Design
- Location Tracking via BSM
- V2V Identification Capabilities
- Misbehavior Detection

** 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,

Vehicle Broadcast of a Basic Safety Message




Basic Safety Message

MANDATORY (Part I)
MsgCount
TemporaryID
DSecond
PositionLocal3D
Latitude
Longitude
Elevation
PositionalAccuracy
TransmissionAndSpeed
Heading
SteeringWheelAngle
AccelerationSet4Way
BrakeSystemStatus
VehicleSize

OPTIONAL (Part II)
VehicleSafetyExtension

Pseudonym Certificate

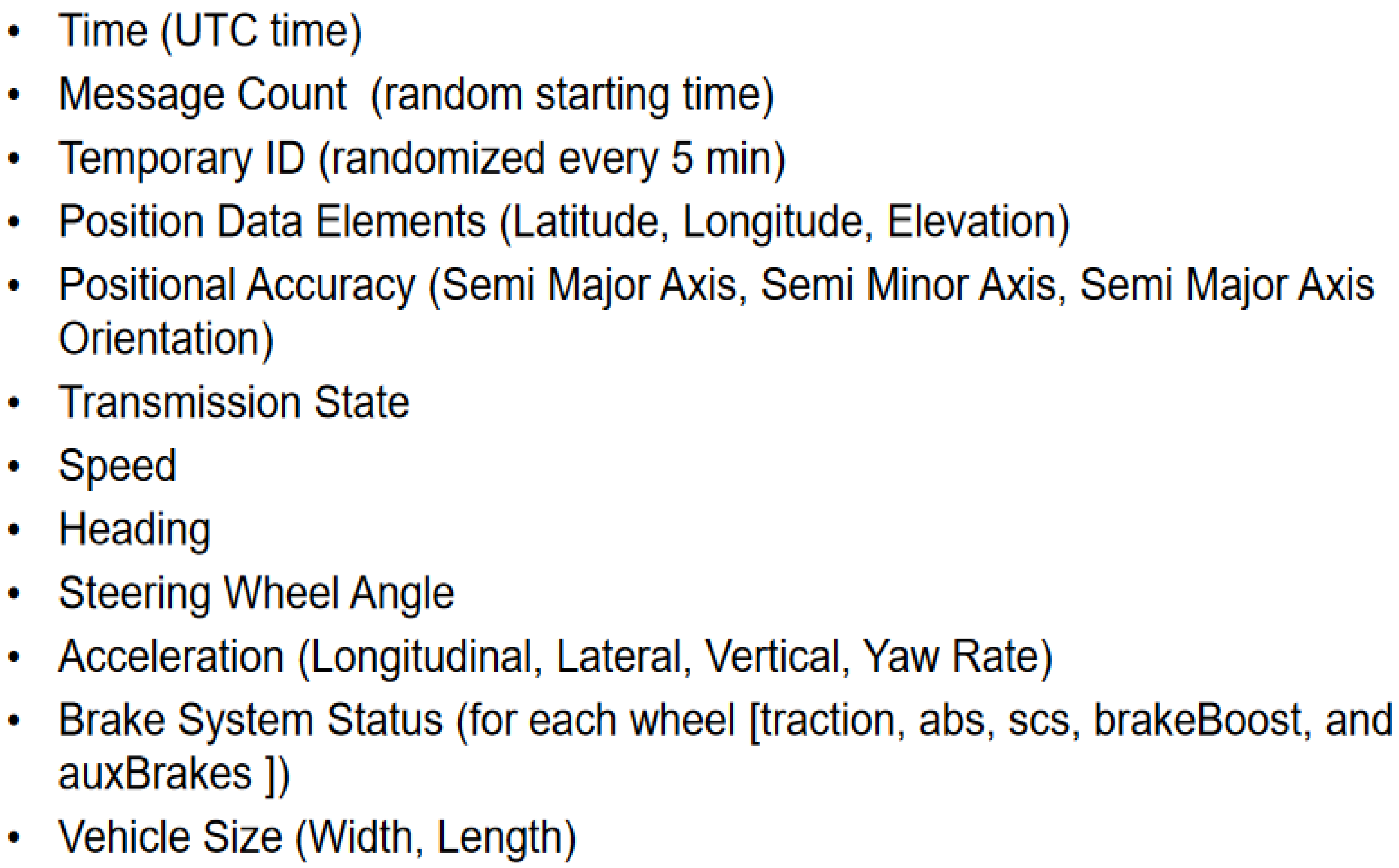
Pseudonym Certificate ID (linkage value)
Pseudonym Certificate public key reconstruction value
Pseudonym Certificate validity period

Basic connectivity options between vehicles and RSUs. BSMs are one of the primary building blocks for V2V communications. They provide situational awareness information to individual vehicles regarding traffic and safety items including imminent crash avoidance applications. These messages are broadcast to all OBE within range but may also be received by RSUs. BSMs originate only from vehicles. Messages that will be broadcast from an RSU to vehicle OBE in support of safety are not classified as BSM by SAE J2735 but include RSA, TIM, SPAT, MAP, EVA, or other message types; “RSA” is used on the figure to represent all safety messages originating from RSUs.

Using V2V communications for imminent crash avoidance applications requires frequent transmission of BSMs—nominally, 10 times per second. These messages contain unencrypted information regarding the device’s position, speed, and further values as defined in SAE J2735. These messages are broadcast and can be received by all OBE and RSUs within range. Although the body of the messages is unencrypted, the sender signs each message and the receiver verifies whether the signature is valid, In order to verify the authenticity and integrity of the message. This requires an SCMS, which, in this case, is realized by a public key infrastructure to provide necessary signing credentials.

“Privacy Issues for Consideration by USDOT Based on Review of Preliminary Technical Framework,” FHWA-JPO-15-236
https://www.regulations.gov/document?D=NHTSA-2016-0126-0003

SAE J2945/1 – On-board Minimum Performance Requirements for V2V Safety Systems - BSM Part 1 Data



- Time (UTC time)
- Message Count (random starting time)
- Temporary ID (randomized every 5 min)
- Position Data Elements (Latitude, Longitude, Elevation)
- Positional Accuracy (Semi Major Axis, Semi Minor Axis, Semi Major Axis Orientation)
- Transmission State
- Speed
- Heading
- Steering Wheel Angle
- Acceleration (Longitudinal, Lateral, Vertical, Yaw Rate)
- Brake System Status (for each wheel [traction, abs, scs, brakeBoost, and auxBrakes])
- Vehicle Size (Width, Length)

[1] J. Misener, SAE Connected Vehicle Standards, CES 2016, Jan 2016

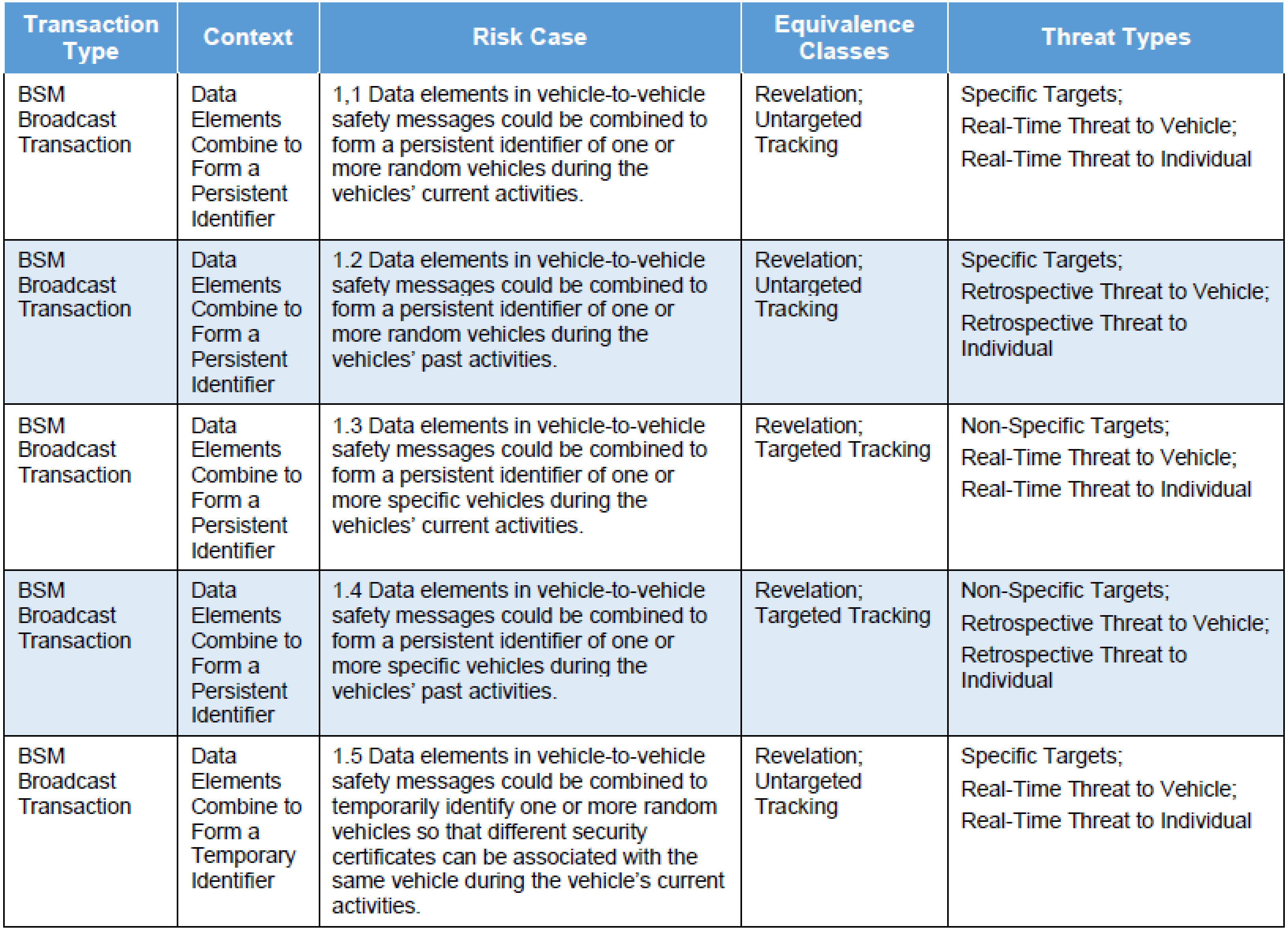
BSM Message Authentication Requirements

Public Key Infrastructure Proposal:

NHTSA proposes V2V devices sign and verify their basic safety messages using a Public Key Infrastructure (PKI) digital signature algorithm in accordance with performance requirements and test procedures for BSM transmission and the signing of BSMs. The agency believes this will establish a level of confidence in the messages exchanged between vehicles and ensure that basic safety message information is being received from devices that have been certified to operate properly, are enrolled in the security network, and are in good working condition. It is also important that safety applications be able to distinguish these from messages originated by ‘‘bad actors,’’ or defective devices, as well as from messages that have been modified or changed while in transit.

**** 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,**

Assessment of US DOT/CAMP Privacy Design (MITRE 1 of 4 – 166 pgs)



Transaction Type	Context	Risk Case	Equivalence Classes	Threat Types

BSM Broadcast Transaction	Data Elements Combine to Form a Persistent Identifier	1,1 Data elements in vehicle-to-vehicle safety messages could be combined to form a persistent identifier of one or more random vehicles during the vehicles' current activities.	Revelation; Untargeted Tracking	Specific Targets;
				Real-Time Threat to Vehicle;
				Real-Time Threat to Individual

BSM Broadcast Transaction	Data Elements Combine to Form a Persistent Identifier	1.2 Data elements in vehicle-to-vehicle safety messages could be combined to form a persistent identifier of one or more random vehicles during the vehicles' past activities.	Revelation; Untargeted Tracking	Specific Targets;
				Retrospective Threat to Vehicle;
				Retrospective Threat to Individual

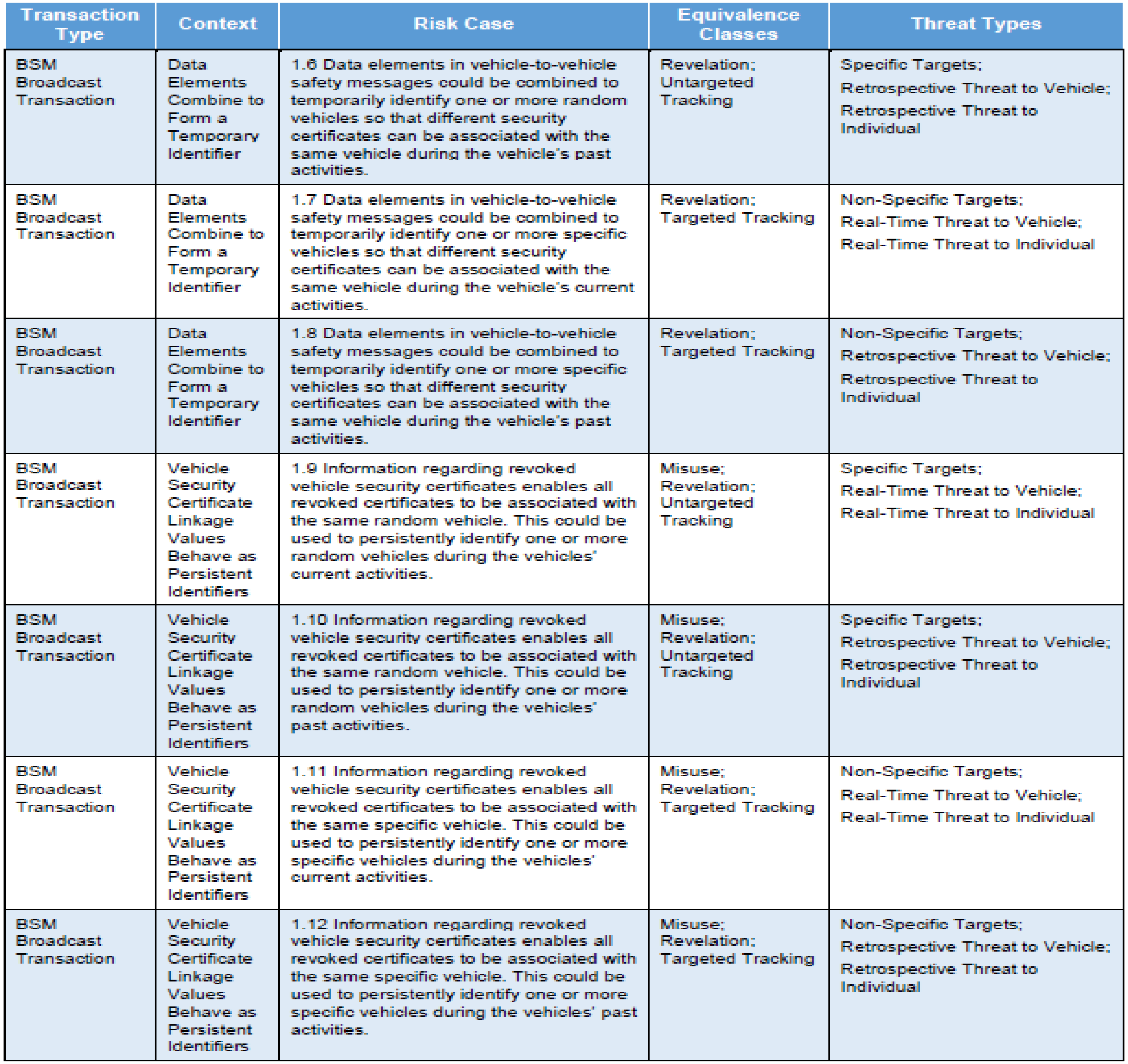
BSM Broadcast Transaction	Data Elements Combine to Form a Persistent Identifier	1.3 Data elements in vehicle-to-vehicle safety messages could be combined to form a persistent identifier of one or more specific vehicles during the vehicles' current activities.	Revelation; Targeted Tracking	Non-Specific Targets;
				Real-Time Threat to Vehicle;
				Real-Time Threat to Individual

BSM Broadcast Transaction	Data Elements Combine to Form a Persistent Identifier	1.4 Data elements in vehicle-to-vehicle safety messages could be combined to form a persistent identifier of one or more specific vehicles during the vehicles' past activities.	Revelation; Targeted Tracking	Non-Specific Targets;
				Retrospective Threat to Vehicle;
				Retrospective Threat to Individual

BSM Broadcast Transaction	Data Elements Combine to Form a Temporary Identifier	1.5 Data elements in vehicle-to-vehicle safety messages could be combined to temporarily identify one or more random vehicles so that different security certificates can be associated with the same vehicle during the vehicle's current activities.	Revelation; Untargeted Tracking	Specific Targets;
				Real-Time Threat to Vehicle;
				Real-Time Threat to Individual

Privacy Issues for Consideration by USDOT Based on Review of Preliminary Technical Framework," FHWA-JPO-15-235 in Docket No. NHTSA–2016–0126, Section 4.1.4 (Feb. 2016) 9 82 Fed. Reg. 3911

Assessment of US DOT/CAMP Privacy Design (MITRE 2 of 4 – 166 pgs)



Transaction Type	Context	Risk Case	Equivalence Classes	Threat Types

BSM Broadcast Transaction	Data Elements Combine to Form a Temporary Identifier	1.6 Data elements in vehicle-to-vehicle safety messages could be combined to temporarily identify one or more random vehicles so that different security certificates can be associated with the same vehicle during the vehicle's past activities.	Revelation; Untargeted Tracking	Specific Targets;
				Retrospective Threat to Vehicle;
				Retrospective Threat to Individual

BSM Broadcast Transaction	Data Elements Combine to Form a Temporary Identifier	1.7 Data elements in vehicle-to-vehicle safety messages could be combined to temporarily identify one or more specific vehicles so that different security certificates can be associated with the same vehicle during the vehicle's current activities.	Revelation; Targeted Tracking	Non-Specific Targets;
				Real-Time Threat to Vehicle;
				Real-Time Threat to Individual

BSM Broadcast Transaction	Data Elements Combine to Form a Temporary Identifier	1.8 Data elements in vehicle-to-vehicle safety messages could be combined to temporarily identify one or more specific vehicles so that different security certificates can be associated with the same vehicle during the vehicle's past activities.	Revelation; Targeted Tracking	Non-Specific Targets;
				Retrospective Threat to Vehicle;
				Retrospective Threat to Individual

BSM Broadcast Transaction	Vehicle Security Certificate Linkage Values Behave as Persistent Identifiers	1.9 Information regarding revoked vehicle security certificates enables all revoked certificates to be associated with the same random vehicle. This could be used to persistently identify one or more random vehicles during the vehicles' current activities.	Misuse; Revelation; Untargeted Tracking	Specific Targets;
				Real-Time Threat to Vehicle;
				Real-Time Threat to Individual

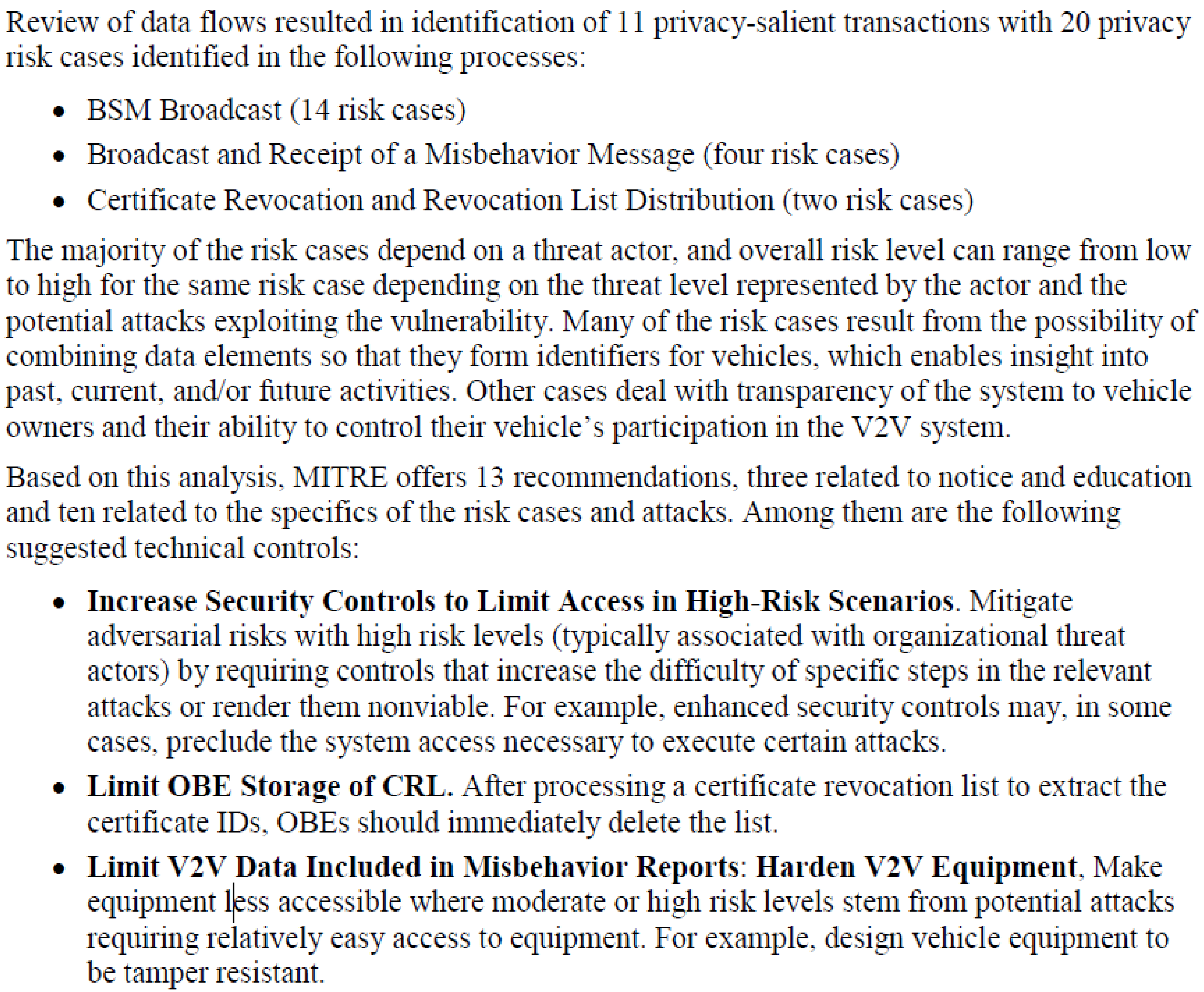
BSM Broadcast Transaction	Vehicle Security Certificate Linkage Values Behave as Persistent Identifiers	1.10 Information regarding revoked vehicle security certificates enables all revoked certificates to be associated with the same random vehicle. This could be used to persistently identify one or more random vehicles during the vehicles' past activities.	Misuse; Revelation; Untargeted Tracking	Specific Targets;
				Retrospective Threat to Vehicle;
				Retrospective Threat to Individual

BSM Broadcast Transaction	Vehicle Security Certificate Linkage Values Behave as Persistent Identifiers	1.11 Information regarding revoked vehicle security certificates enables all revoked certificates to be associated with the same specific vehicle. This could be used to persistently identify one or more specific vehicles during the vehicles' current activities.	Misuse; Revelation; Targeted Tracking	Non-Specific Targets;
				Real-Time Threat to Vehicle;
				Real-Time Threat to Individual

BSM Broadcast Transaction	Vehicle Security Certificate Linkage Values Behave as Persistent Identifiers	1.12 Information regarding revoked vehicle security certificates enables all revoked certificates to be associated with the same specific vehicle. This could be used to persistently identify one or more specific vehicles during the vehicles' past activities.	Misuse; Revelation; Targeted Tracking	Non-Specific Targets;
				Retrospective Threat to Vehicle;
				Retrospective Threat to Individual

Privacy Issues for Consideration by USDOT Based on Review of Preliminary Technical Framework," FHWA-JPO-15-235 in Docket No. NHTSA–2016–0126, Section 4.1.4 (Feb. 2016) 9 82 Fed. Reg. 3911

Assessment of US DOT/CAMP Privacy Design (MITRE 3 of 4)



Review of data flows resulted in identification of 11 privacy-salient transactions with 20 privacy risk cases identified in the following processes:

- BSM Broadcast (14 risk cases)
- Broadcast and Receipt of a Misbehavior Message (four risk cases)
- Certificate Revocation and Revocation List Distribution (two risk cases)

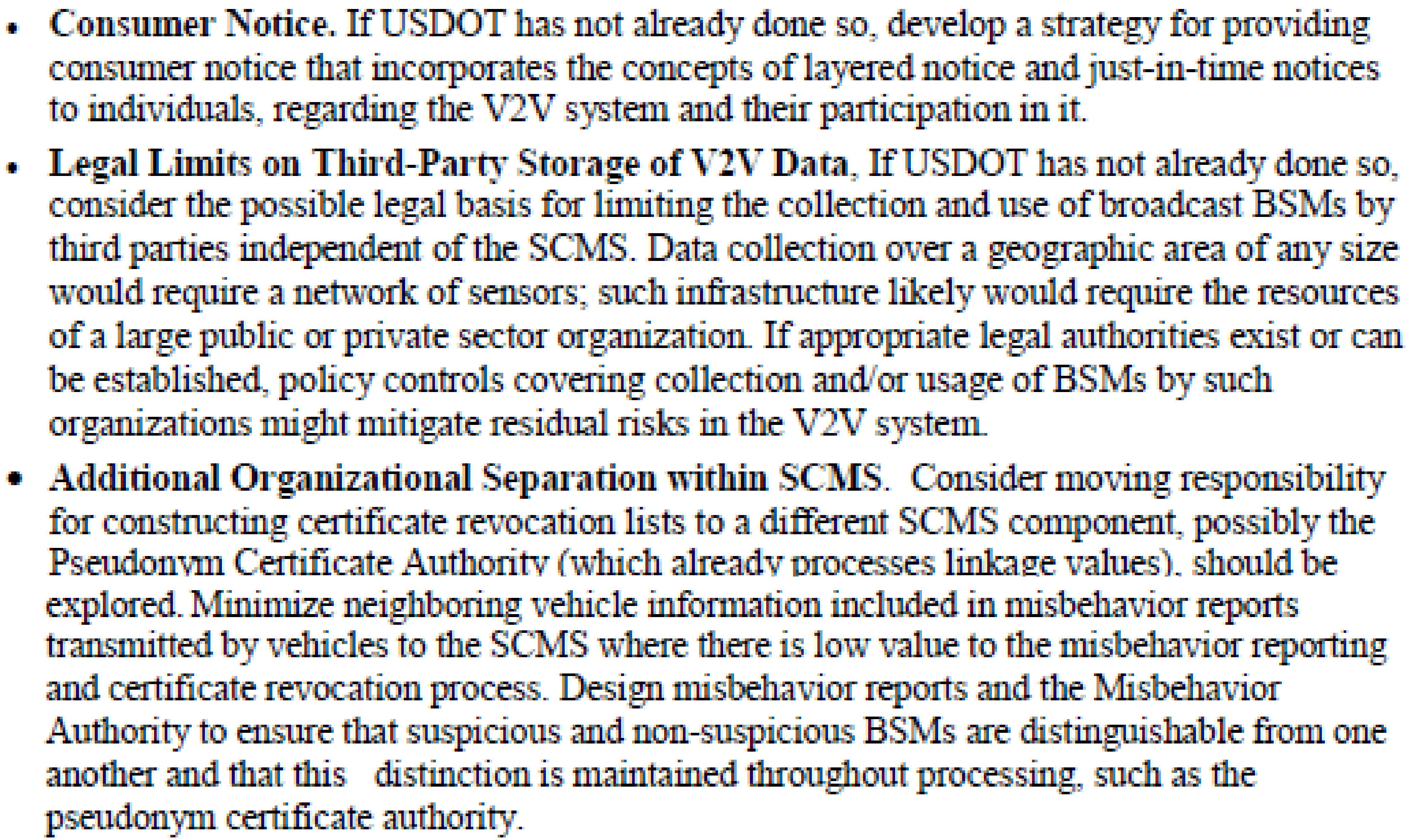
The majority of the risk cases depend on a threat actor, and overall risk level can range from low to high for the same risk case depending on the threat level represented by the actor and the potential attacks exploiting the vulnerability. Many of the risk cases result from the possibility of combining data elements so that they form identifiers for vehicles, which enables insight into past, current, and/or future activities. Other cases deal with transparency of the system to vehicle owners and their ability to control their vehicle's participation in the V2V system.

Based on this analysis, MITRE offers 13 recommendations, three related to notice and education and ten related to the specifics of the risk cases and attacks. Among them are the following suggested technical controls:

- **Increase Security Controls to Limit Access in High-Risk Scenarios**. Mitigate adversarial risks with high risk levels (typically associated with organizational threat actors) by requiring controls that increase the difficulty of specific steps in the relevant attacks or render them nonviable. For example, enhanced security controls may, in some cases, preclude the system access necessary to execute certain attacks.
- **Limit OBE Storage of CRL.** After processing a certificate revocation list to extract the certificate IDs, OBEs should immediately delete the list.
- **Limit V2V Data Included in Misbehavior Reports**: **Harden V2V Equipment**, Make equipment less accessible where moderate or high risk levels stem from potential attacks requiring relatively easy access to equipment. For example, design vehicle equipment to be tamper resistant.

Privacy Issues for Consideration by USDOT Based on Review of Preliminary Technical Framework," FHWA-JPO-15-235 in Docket No. NHTSA–2016–0126, Section 4.1.4 (Feb. 2016) 9 82 Fed. Reg. 3911

Assessment of US DOT/CAMP Privacy Design (MITRE 4 of 4) - Suggested Policy Controls



- **Consumer Notice.** If USDOT has not already done so, develop a strategy for providing consumer notice that incorporates the concepts of layered notice and just-in-time notices to individuals, regarding the V2V system and their participation in it.
- **Legal Limits on Third-Party Storage of V2V Data.** If USDOT has not already done so, consider the possible legal basis for limiting the collection and use of broadcast BSMs by third parties independent of the SCMS. Data collection over a geographic area of any size would require a network of sensors; such infrastructure likely would require the resources of a large public or private sector organization. If appropriate legal authorities exist or can be established, policy controls covering collection and/or usage of BSMs by such organizations might mitigate residual risks in the V2V system.
- **Additional Organizational Separation within SCMS.** Consider moving responsibility for constructing certificate revocation lists to a different SCMS component, possibly the Pseudonym Certificate Authority (which already processes linkage values), should be explored. Minimize neighboring vehicle information included in misbehavior reports transmitted by vehicles to the SCMS where there is low value to the misbehavior reporting and certificate revocation process. Design misbehavior reports and the Misbehavior Authority to ensure that suspicious and non-suspicious BSMs are distinguishable from one another and that this distinction is maintained throughout processing, such as the pseudonym certificate authority.

Privacy Issues for Consideration by USDOT Based on Review of Preliminary Technical Framework," FHWA-JPO-15-235 in Docket No. NHTSA–2016–0126, Section 4.1.4 (Feb. 2016) 9 82 Fed. Reg. 3911

The real challenges of VC data sharing are policy and cultural issues

STOP
PROCEED WITH CAUTION
NO PARKING
PARKING ONLY
NOTICE
MANAGEMENT NOT RESPONSIBLE FOR THEFT OR DAMAGE TO VEHICLES OR THEIR CONTENTS
EXIT
SLOW CHILDREN
SPEED LIMIT 10
NOTICE
ALCOHOLIC BEVERAGES & DRUGS ARE PROHIBITED ON THIS PROPERTY
STOP
ALL VISITORS MUST REPORT TO MAIN OFFICE
ENTRANCE
EXIT
NOTICE
NO TRESPASSING LOITERING SOLICITING ON THIS PROPERTY
PRIVATE ROAD
NO THRU TRAFFIC
EMPLOYEE ENTRANCE ONLY
CAUTION DRIVE SLOWLY
NO THRU TRAFFIC

References Used in This Presentation (1 of 2)

- IEEE 1609 Standards for Wireless Access in Vehicular Environments (WAVE), online available (fee based) - https://standards.ieee.org/develop/wg/1609_WG.html

- 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

- 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

- P. Papadimitratos, L. Buttyan, T. Holczer, E. Schoch, J. Freudiger, M. Raya, Z. Ma, F. Kargl, A. Kung, and J.-P. Hubaux, "Secure vehicular communication systems: Design and architecture," IEEE Commun. Mag., vol. 46, no. 11, pp. 100–109, Nov. 2008.

- A security credential management system for V2V communications, Authors - William Whyte, André Weimerskirch, Virendra Kumar, Thorsten Hehn, 2013, IEEE Vehicular Networking Conference (VNC), https://www.researchgate.net/publication/271554151_A_security_credential_management_system_for_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

- "SCMS Design Analysis Report," FHWA-JPO-15-235 in Docket No. NHTSA–2016–0126, Section 4.1.4 (Feb. 2016) 9 82 Fed. Reg. 3911 - https://www.regulations.gov/document?D=NHTSA-2016-0126-0004

References Used in This Presentation (2 of 2)

- “Privacy Issues for Consideration by USDOT Based on Review of Preliminary Technical Framework,” FHWA-JPO-15-235 in Docket No. NHTSA–2016–0126, Section 4.1.4 (Feb. 2016) 9 82 Fed. Reg. 3911 - https://www.regulations.gov/document?D=NHTSA-2016-0126-0003.

- Security architecture - Integrating security into the communicating vehicle, Norbert Bissmeyer, Fraunhofer SIT June 18th 2015 https://www.preserve-project.eu/sites/preserve-project.eu/files/preserve-ws-02-security-architecture.pdf

- 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

- F. Dressler, C. Sommer, Vehicular Networking, Cambridge University Press, Dec 2014 - http://book.car2x.org/Vehicular_Networking_Slides.pdf

- J. Misener, SAE Connected Vehicle Standards, CES 2016, Jan 2016, http://www.sae.org/events/ces/2016/attend/program/presentations/misener.pdf.

- P. Papadimitratos, A. de La Fortelle, K. Evenssen, R. Brignolo, S. Cosenze, “Vehicular communication systems: Enabling Technologies, Applications and Future Outlook on Intelligent Transportation,” IEEE Commun. Mag., vol. 47, no. 11, pp. 84-95, Nov. 2009.