IEEE Communications Society – Denver Section Dine and Learn

VPKI Hits the Highway – Secure Communication for the US DOT Connected Vehicle Pilot Program

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

Denver, CO
9 May 2017

Objectives of this Presentation

ITS Security for Vehicular Networks

-- A Writer's Life

-- ITS Models (US DOT Connected Car, Use Cases, IEEE WAVE)

-- Connected Car Pilot (NYC, THEA, WYO)

-- 10 year evolution of the SCMS Approach – Connected Car Program

Show real-world examples

-- A Closer Look at the SCMS Approach – Connected Car Program

-- SCMS Standards –VPKI Architecture and Security (1609.2) / SAE 2757 DSRC Messaging

-- Vehicle Public Key Infrastructure (V-PKI)

Organizing Framework for Security Architecture

-- How to reduce Complexity for ITS Service Management Design

-- 'What if' scenarios - Issues regarding large scale deployments

Table of Contents

A Writer's Life –

Timothy Weil
Editor - IEEE IT Professional magazine
Cloud Security, RBAC, Identity Management, Vehicular Networks
Verified email at securityfeeds.com - Homepage

Citation indices	All	Since 2012
Citations	1148	1086
h-index	7	6
i10-index	7	4

Co-authors View all...
Georgios Karagiannis, D. Richard (Rick) Kuhn

Title 1–20	Cited by	Year
Vehicular networking: A survey and tutorial on requirements, architectures, challenges, standards and solutions G Karagiannis, O Altintas, E Ekici, G Heijenk, B Jarupan, K Lin, T Weil IEEE communications surveys & tutorials 13 (4), 584-616	705	2011
Adding attributes to role-based access control DR Kuhn, EJ Coyne, TR Weil Computer 43 (6), 79-81	306	2010
ABAC and RBAC: scalable, flexible, and auditable access management E Coyne, TR Weil IT Professional 15 (3), 0014-16	53	2013
Final report: Vehicle infrastructure integration (VII) proof of concept (POC) test–Executive summary R Kandarpa, M Chenzaie, M Dorfman, J Anderson, J Marousek, ... US Department of Transportation, IntelliDrive (SM), Tech. Rep	25	2009
Service management for ITS using WAVE (1609.3) networking T Weil GLOBECOM Workshops, 2009 IEEE, 1-6	14	2009
Final Report: Vehicle Infrastructure Integration Proof-of-Concept Results and Findings-Infrastructure R Kandarpa, M Chenzaie, J Anderson, J Marousek, T Weil, F Perry, ... US Department of Transportation, Washington, DC, USA	11	2009

IEEE National Capital Area **scanner**

IEEE SCANNER - Above the Fold (Mostly)

Stories in Engineering and Science (2005-2009)

In my tenure as Washington DC Editor of the IEEE SCANNER(2005-2007) and AdCom officer (2007-2009) I had the wonderful chance to tour the science, engineering and technology world of IEEE as a roving reporter and editor of this newspaper. My travels took me to Deep Space (NASA), Satellite Communication(Intelsat), the flagship conference of the Telecom industry (GLOBECOM) and beyond. As the son of an AP journalist and itinerant newspaper reporter the SCANNER gave me a front row seat to the journeys of science and engineering.

The stories and photographs below are the journalistic opportunities presented to me by the SCANNER newsletter.

- Nov-Dec 2009 - Celebrating the 125th IEEE Anniversary Year (UDC)
- Sept-Oct 2009 - Preserving History at the History of Technical Societies Conference
- July-Aug 2009 - Washington Section Participates in Congressional Visit Day
- May-June 2009 - Passing The Gavel
- Nov-Dec 2008 - A Tour of NASA Goddard Test and Integration Facility (pg. 6)
- Sept-Oct 2008 - Globecom Committee Closes the Books at ICC 2008 in Beijing
- Sept-Oct 2007 - Globecom Volunteers Prepare for the November Conference
- July-Aug 2007 - DC COMSOC Hosts WiMax Lecture at JDSU
- Jan-Feb 2007 - Globecom Volunteers Visit the San Francisco Conference
- Nov-Dec 2006 - Sensors Conference Panel Reviews DoD Technologies
- July-Aug 2006 - Globecom 2007 Committee Builds a Program
- Sept-Oct 2005 - COMSOC Members Tour the IntelSat Satellite Center
- May-June 2005 - DCCEAS Recognizes Jerry Gibbon as Engineer of the Year

SECURING IT

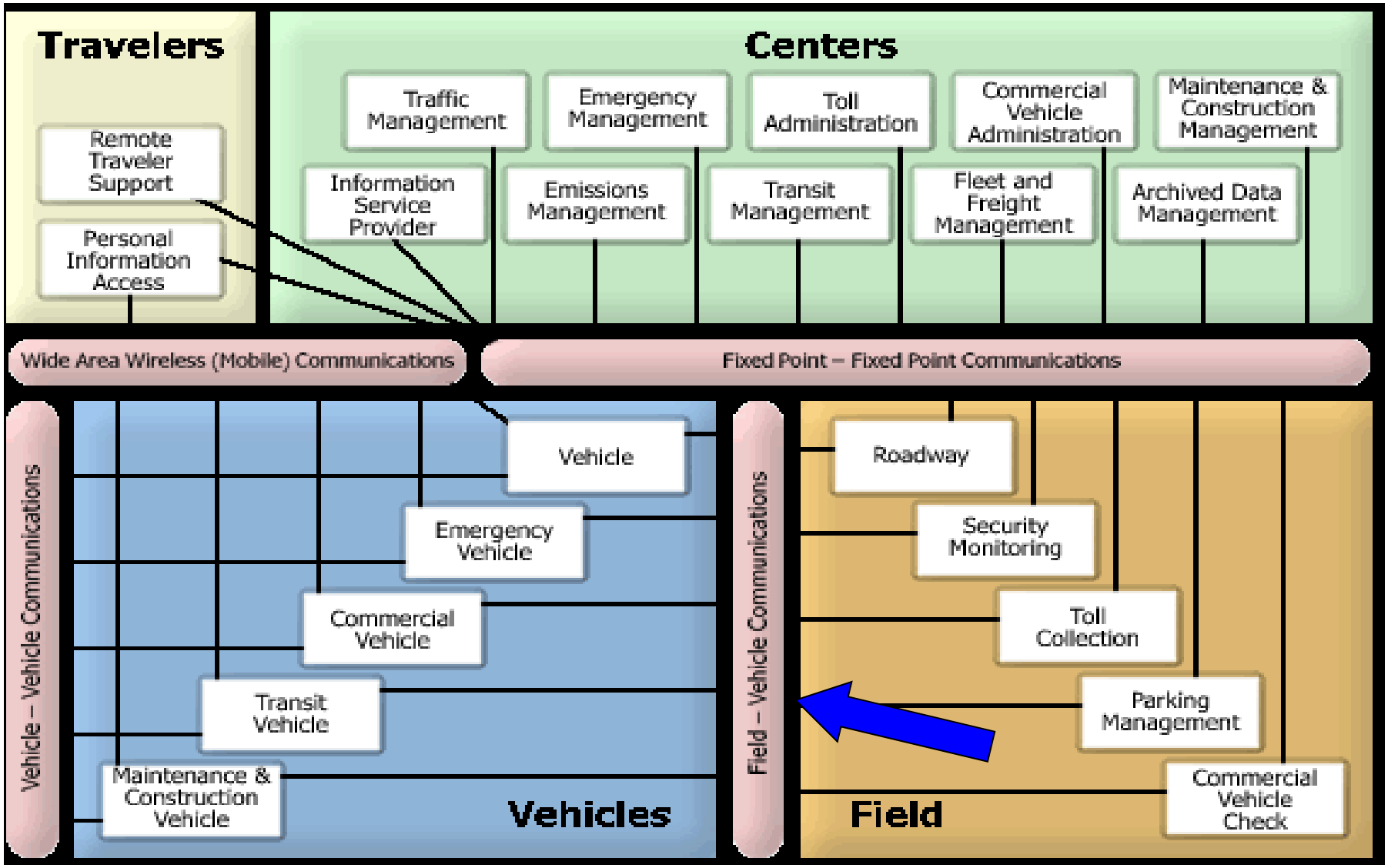
VPKI Hits the Highway

Secure Communication for the Connected Vehicle Program

Tim Weil, SCRAM Systems

Introduction – USDOT ITS National Architecture

http://www.iteris.com/itsarch/html/entity/paents.htm



Introduction − ITS Use Cases Services and Applications

CONNECTED VEHICLE APPLICATIONS

V2I Safety

- Red Light Violation Warning
- Curve Speed Warning
- Stop Sign Gap Assist
- Spot Weather Impact Warning
- Reduced Speed/Work Zone Warning
- Pedestrian in Signalized Crosswalk Warning (Transit)

V2V Safety

- Emergency Electronic Brake Lights (EEBL)
- Forward Collision Warning (FCW)
- Intersection Movement Assist (IMA)
- Left Turn Assist (LTA)
- Blind Spot/Lane Change Warning (BSW/LCW)
- Do Not Pass Warning (DNPW)
- Vehicle Turning Right in Front of Bus Warning (Transit)

Agency Data

- Probe-based Pavement Maintenance
- Probe-enabled Traffic Monitoring
- Vehicle Classification-based Traffic Studies
- CV-enabled Turning Movement & Intersection Analysis
- CV-enabled Origin-Destination Studies
- Work Zone Traveler Information

Environment

- Eco-Approach and Departure at Signalized Intersections
- Eco-Traffic Signal Timing
- Eco-Traffic Signal Priority
- Connected Eco-Driving
- Wireless Inductive/Resonance Charging
- Eco-Lanes Management
- Eco-Speed Harmonization
- Eco-Cooperative Adaptive Cruise Control
- Eco-Traveler Information
- Eco-Ramp Metering
- Low Emissions Zone Management
- AFV Charging / Fueling Information
- Eco-Smart Parking
- Dynamic Eco-Routing (light vehicle, transit, freight)
- Eco-ICM Decision Support System

Road Weather

- Motorist Advisories and Warnings (MAW)
- Enhanced MDSS
- Vehicle Data Translator (VDT)
- Weather Response Traffic Information (WxTINFO)

Mobility

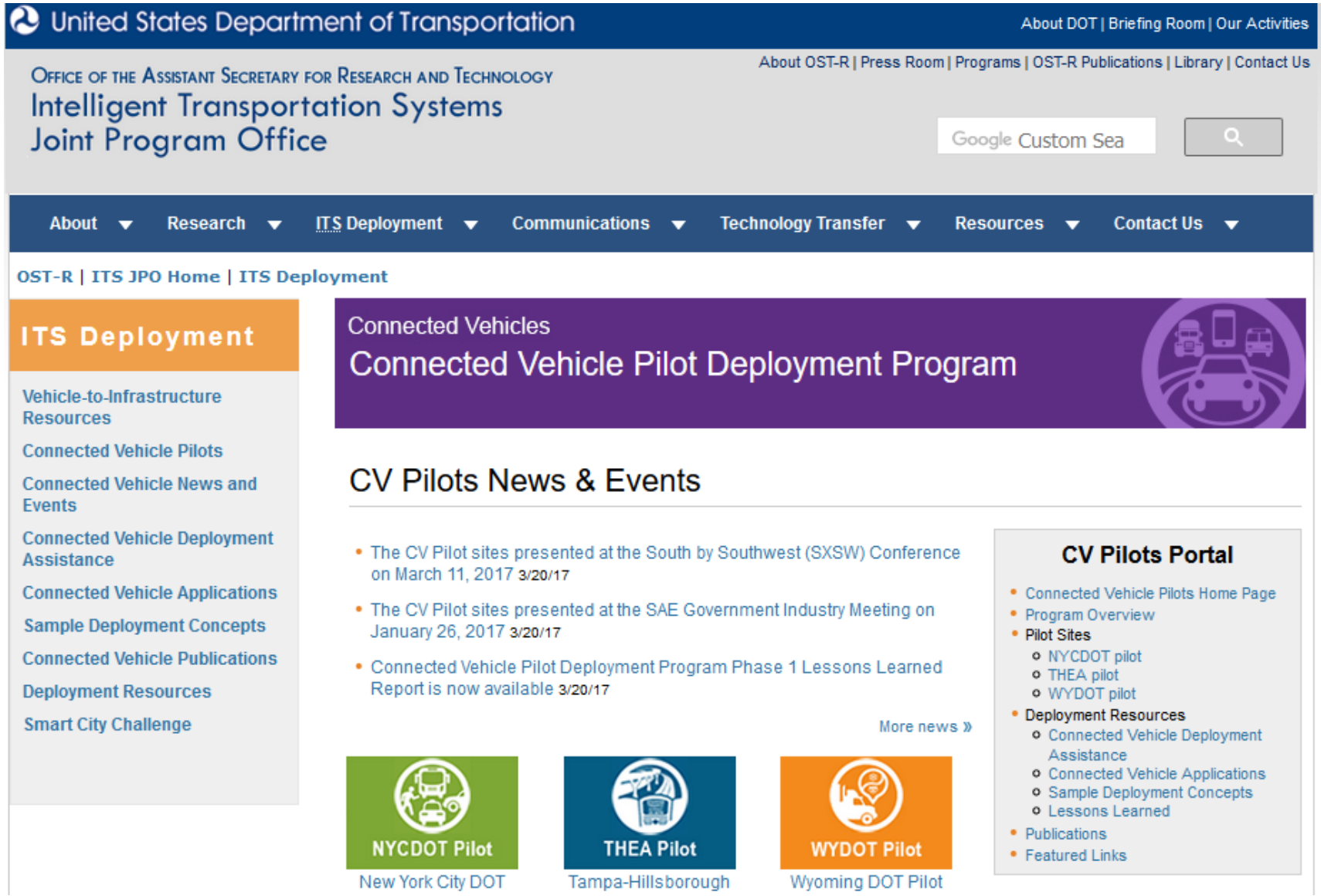
- Advanced Traveler Information System
- Intelligent Traffic Signal System (I-SIG)
- Signal Priority (transit, freight)
- Mobile Accessible Pedestrian Signal System (PED-SIG)
- Emergency Vehicle Preemption (PREEMPT)
- Dynamic Speed Harmonization (SPD-HARM)
- Queue Warning (Q-WARN)
- Cooperative Adaptive Cruise Control (CACC)
- Incident Scene Pre-Arrival Staging Guidance for Emergency Responders (RESP-STG)
- Incident Scene Work Zone Alerts for Drivers and Workers (INC-ZONE)
- Emergency Communications and Evacuation (EVAC)
- Connection Protection (T-CONNECT)
- Dynamic Transit Operations (T-DISP)
- Dynamic Ridesharing (D-RIDE)
- Freight-Specific Dynamic Travel Planning and Performance
- Drayage Optimization

Smart Roadside

- Wireless Inspection
- Smart Truck Parking

US DOT ITS JPO – Connected Vehicle Pilot Deployment Program

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



Tampa-Hillsborough Expressway Authority (THEA) Pilot

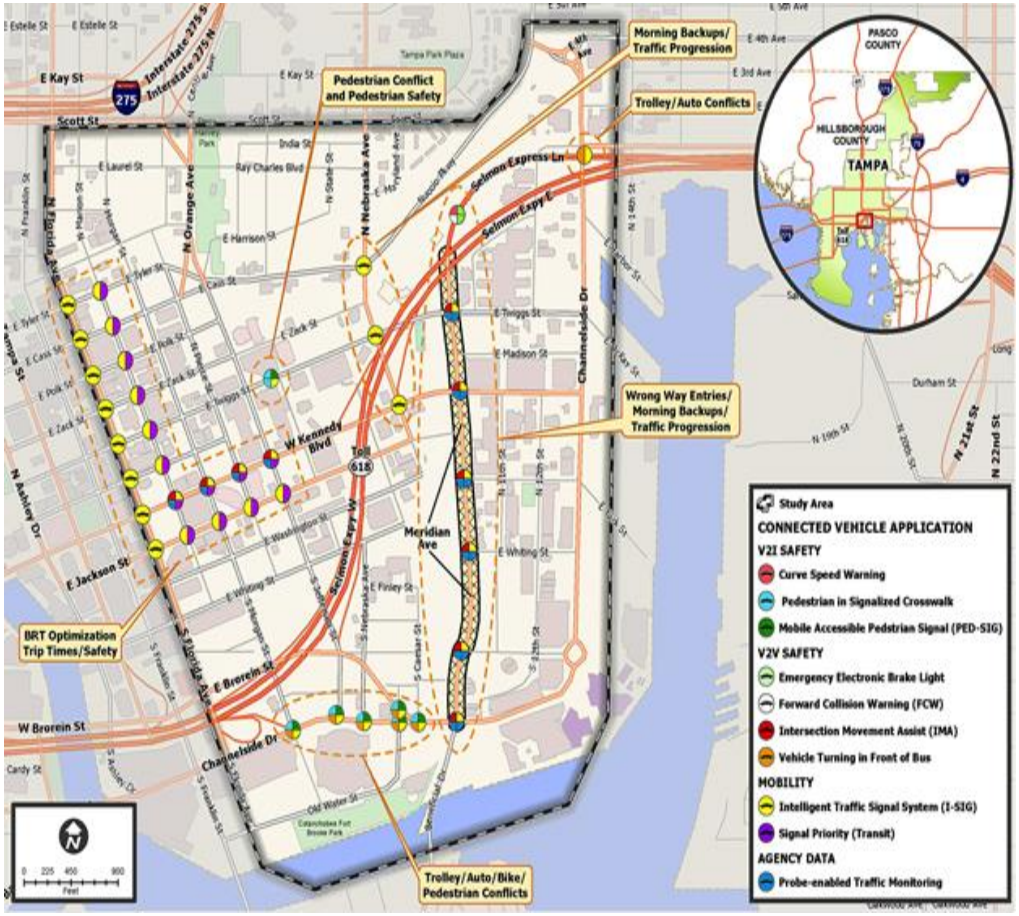


Table 1. Tampa (THEA) Pilot Site Proposed CV Applications

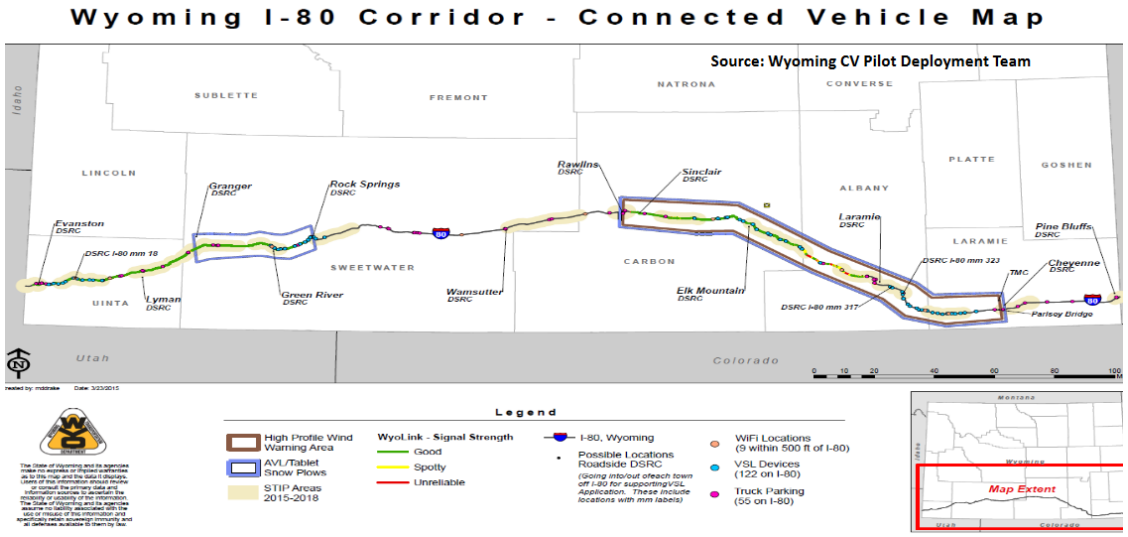
ID	Category	Tampa (THEA) – CV Application
1	V2I Safety	End of Ramp Deceleration Warning (ERDW)
2		Pedestrian in Signalized Crosswalk Warning (PED-X)
3		Wrong Way Entry (WWE)
4	V2V Safety	Emergency Electronic Brake Lights (EEBL)
5		Forward Collision Warning (FCW)
6		Intersection Movement Assist (IMA)
7		Vehicle Turning Right in Front of a Transit Vehicle (VTRFTV)
8	Mobility	Mobile Accessible Pedestrian Signal System (PED-SIG)
9		Intelligent Traffic Signal System (I-SIG)
10		Transit Signal Priority (TSP)
11	Agency Data	Probe-enabled Data Monitoring (PeDM)

Table 2. Tampa (THEA) Pilot Site Proposed CV Devices

Tampa (THEA) – Devices	Estimated Number
Roadside Unit (RSU) at Intersection	40
Vehicle Equipped with On-Board Unit (OBU)	1,600
Pedestrian Equipped with App in Smartphone	500
HART Transit Bus Equipped with OBU	10
TECO Line Street Car Equipped with OBU	10
Total Equipped Vehicles	1,620

Tampa-Hillsborough Expressway Authority (THEA) owns and operates the Selmon Reversible Express Lanes (REL), which is a first-of-its-kind facility to address urban congestion. The REL morning commute endpoint intersection is on major routes into and out of the downtown Tampa commercial business district. Drivers experience significant delay during the morning peak hour resulting in, and often caused by, a correspondingly large number of rear-end crashes and red light running collisions. Because the lanes are reversible, wrong way entry is possible.The THEA CV Pilot will employ Dedicated Short Range Communication (DSRC) to enable transmissions among approximately 1,600 cars, 10 buses, 10 trolleys, 500 pedestrians with smartphone applications, and approximately 40 roadside units.

Wyoming (WY) DOT Connected Car Pilot



Wyoming is an important freight corridor that plays a critical role in the movement of goods across the country and between the United States, Canada, and Mexico. As shown in the figure below, Interstate 80 (I-80) in southern Wyoming which is above 6000 feet is a major corridor for east/west freight movement and moves more than 32 million tons of freight per year. During winter seasons when wind speeds and wind gusts exceed 30 mph and 65 mph respectively, crash rates on I-80 have been found to be 3 to 5 times as high as summer crash rates. This resulted in 200 truck blowovers within 4 years and often led to road closures.

Table 1. WYDOT Pilot Site Proposed CV Applications

ID	Category	ICF/WYDOT – CV Application
1	V2V Safety	Forward Collision Warning (FCW)
2	V2I/I2V Safety	I2V Situational Awareness*
3		Work Zone Warnings (WZW)*
4		Spot Weather Impact Warning (SWIW)*
5	V2I and V2V Safety	Distress Notification (DN)

Table 2. WYDOT Pilot Site Proposed CV Devices

ICF/WYDOT – Devices	Estimated Number
Roadside Unit (RSU)	75
WYDOT Fleet Subsystem On-Board Unit (OBU)	100
Integrated Commercial Truck Subsystem OBU	150
Retrofit Vehicle Subsystem OBU	25
Basic Vehicle Subsystem OBU	125
Total Equipped Vehicles	400

WYDOT will develop systems that support the use of CV Technology along the 402 miles of I-80 in Wyoming. As listed in Table 2, approximately 75 roadside units (RSUs) that can receive and broadcast message using Dedicated Short Range Communication (DSRC) will be deployed along various sections of I-80. WYDOT will equip around 400 vehicles, a combination of fleet vehicles and commercial trucks with on-board units (OBUs). Of the 400 vehicles, at least 150 would be heavy trucks that are expected to be regular users of I-80. In addition, of the 400 equipped-vehicles, 100 WYDOT fleet vehicles, snowplows and highway patrol vehicles, will be equipped with OBUs and mobile weather sensors. units along city streets

New York City (NYC) Connected Car Pilot

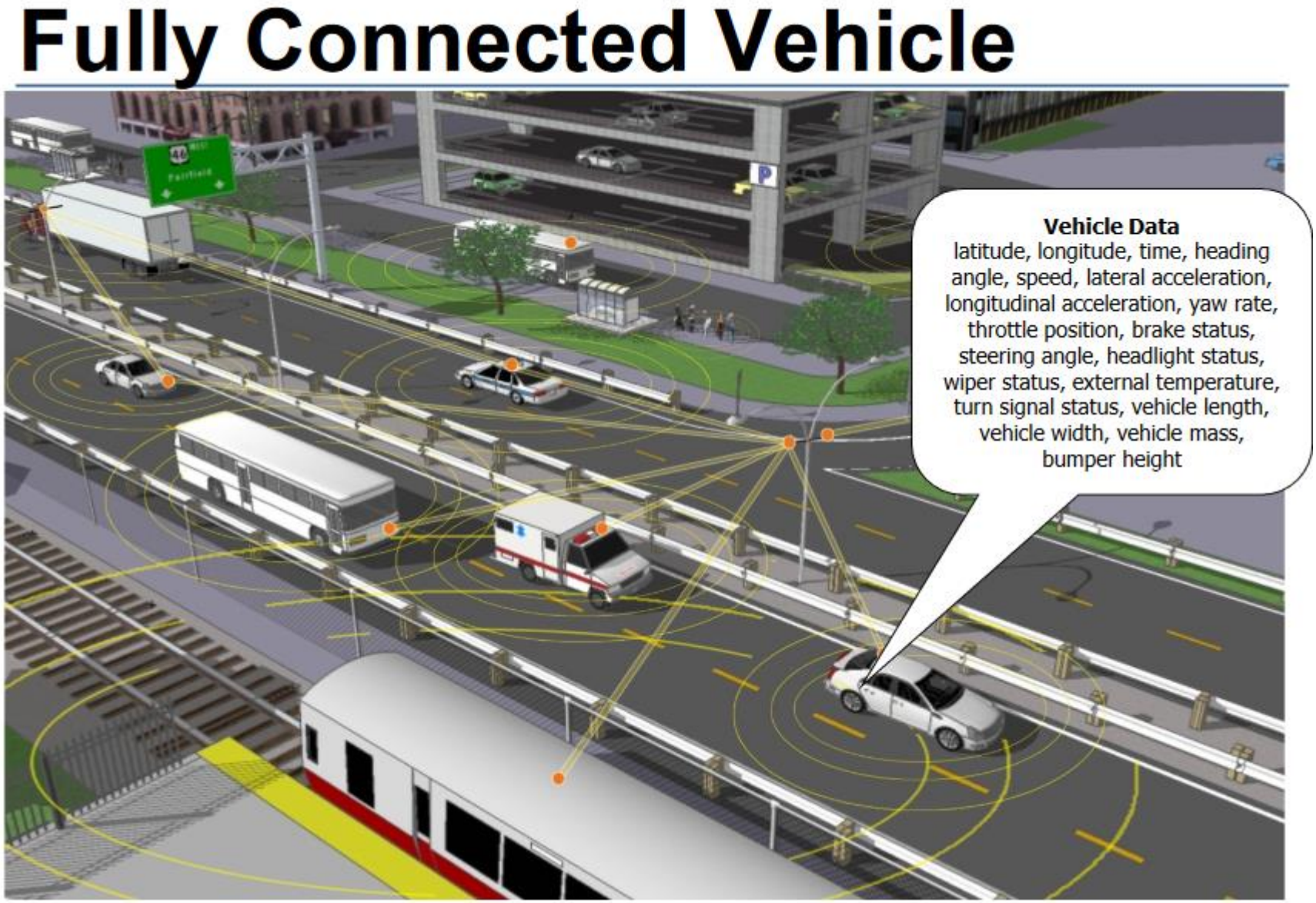
The NYCDOT leads the New York City Pilot, which aims to improve the safety of travelers and pedestrians in the city through the deployment of V2V and V2I connected vehicle technologies. This objective directly aligns with the city's Vision Zero initiative. In 2014, NYC began its *Vision Zero* program to reduce the number of fatalities and injuries resulting from traffic crashes

ID	Category	NYCDOT – CV Application
1	V2I/I2V Safety	Speed Compliance
2		Curve Speed Compliance
3		Speed Compliance/Work Zone
4		Red Light Violation Warning
5		Oversize Vehicle Compliance
6		Emergency Communications and Evacuation Information
7	V2V Safety	Forward Crash Warning (FCW)
8		Emergency Electronics Brake Lights (EEBL)
9		Blind Spot Warning (BSW)
10		Lane Change Warning/Assist (LCA)
11		Intersection Movement Assist (IMA)
12		Vehicle Turning Right in Front of Bus Warning
13	V2I/I2V Pedestrian	Pedestrian in Signalized Crosswalk
14		Mobile Accessible Pedestrian Signal System (PED-SIG)
15	Mobility	Intelligent Traffic Signal System (I-SIGCVDATA)

NYCDOT – Devices	Estimated Number
Roadside Unit (RSU) at Manhattan and Brooklyn Intersections and FDR Drive	353
Taxi Equipped with Aftermarket Safety Device (ASD)*	5,850
MTA Fleet Equipped with ASD*	1,250
UPS Truck Equipped with ASD*	400
NYCDOT Fleet Equipped with ASD*	250
DSNY Fleet Equipped with ASD*	250
Vulnerable Road User (Pedestrians/Bicyclists) Device	100
PED Detection System	10 + 1 spare
Total Equipped Vehicles	8,000

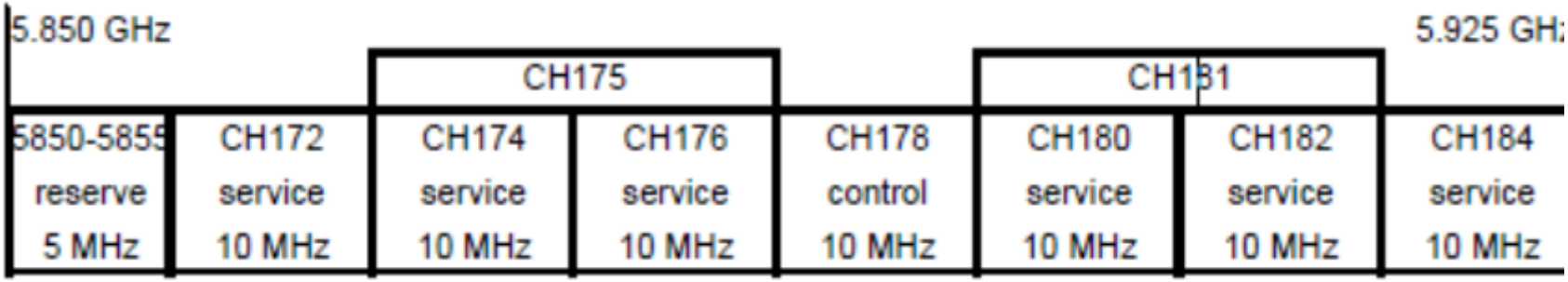
The NYCDOT CV Pilot Deployment project area encompasses three distinct areas in the boroughs of Manhattan and Brooklyn (see the figure below). The first area includes a 4-mile segment of Franklin D. Roosevelt (FDR) Drive in the Upper East Side and East Harlem neighborhoods of Manhattan. The second area includes four one-way corridors in Manhattan. The third area covers a 1.6-mile segment of Flatbush Avenue in Brooklyn. As shown in Table 2, approximately 5,800 cabs, 1,250 MTA buses, 400 commercial fleet delivery trucks, and 500 City vehicles will be fit with CV technology.

US DOT Model


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

Basics of Dedicated Short Range Radio (DSRC)

https://www.its.dot.gov/presentations/world_congress2016/Leonard_DSRC_Spectrum2016.pdf



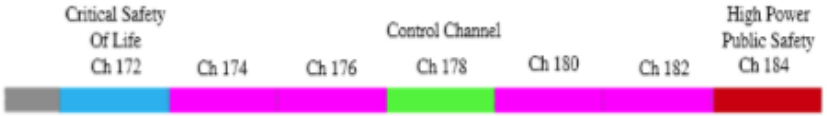
Source: FCC Report and Order FCC 03-324

- **Packet-based** medium based on **IEEE 802.11** specifications for lower-layer definition
- Additional **network** layer definitions and a **cryptographic** process for establishing trust and protecting confidentiality given in **IEEE 1609 family**
- **Payload** definitions and performance requirements for common data units established in **SAE standards**
- General **IP transport** available with certain **priority** requirements and packet **size** limitations

SAE Connected Vehicle Standards (J. Misener)

http://www.sae.org/events/ces/2016/attend/program/presentations/misener.pdf

Dedicated Short Range Communications (DSRC) for V2V Safety Applications



DSRC was designed for the 5.9GHz ITS band

Licensed under FCC Part 90 and 95

Uses "communication outside the context of a BSS" defined in 802.11p

FCC designates certain channels, e.g. V2V safety, control, public safety

V2V Standards

- IEEE 802.11 (PHY/MAC) →
- IEEE 1609.2-4 (message protocol and security services) →
- SAE J2735 (data dictionary / message sets: Vehicle Safety Extension) →
- SAE J2945/1 (on-board performance requirements)

DSRC V2V Use Cases (USDOT, OEMs) – These were tested at the Ann Arbor Safety Pilot

Emergency Electronic Brake Lights (EEBL)

- Brake "on" from several cars ahead sent to subject vehicle

Forward Collision Warning (FCW)

- Alert to elicit hard braking to prevent rear-end crash

Blind Spot Warning/Lane Change Warning (BSW/LCW)

- Alerts of fast-approaching cars from behind (and in adjoining lanes)

Do Not Pass Warning (DNPW)

- Alerts for head-on crashes during passing maneuver

Intersection Movement Assist (IMA)

Left Turn Assist (LTA)

Basic Safety Messages (BSM)

Fundamentals

- Connected V2V safety applications are built around the SAE J2735 BSM, which has two parts
  - BSM Part 1:
    - Contains the core data elements (vehicle size, position, speed, heading acceleration, brake system status)
    - Transmitted approximately 10x per second
  - BSM Part 2:
    - Added to part 1 depending upon events (e.g., ABS activated)
    - Contains a variable set of data elements drawn from many optional data elements (availability by vehicle model varies)
    - Transmitted less frequently
  - No on-vehicle BSM storage of BSM data

Test Bed Data Systems

- Example: Safety Pilot (26 RSEs and <3000 vehicles):
  - SPaT Data (6 sites): 28,821,437 messages per day
  - MAP Data (6 sites): 2,510,384 messages per day
  - TIM (3 sites): 227,766 messages per day
  - BSM (26 sites): 16,740,785 messages per day
  - Total data per month: 18.4 TB

BSMs are one of the primary building blocks for V2V communications. They provide situational awareness information to individual vehicles regarding traffic and safety. BSMs are broadcast ten times per second by a vehicle to all neighboring vehicles and are designed to warn the drivers of those vehicles of crash imminent situations.

Basic Vehicle State

(Veh. ID, Seq. #, time, position, motion, control, veh. size)

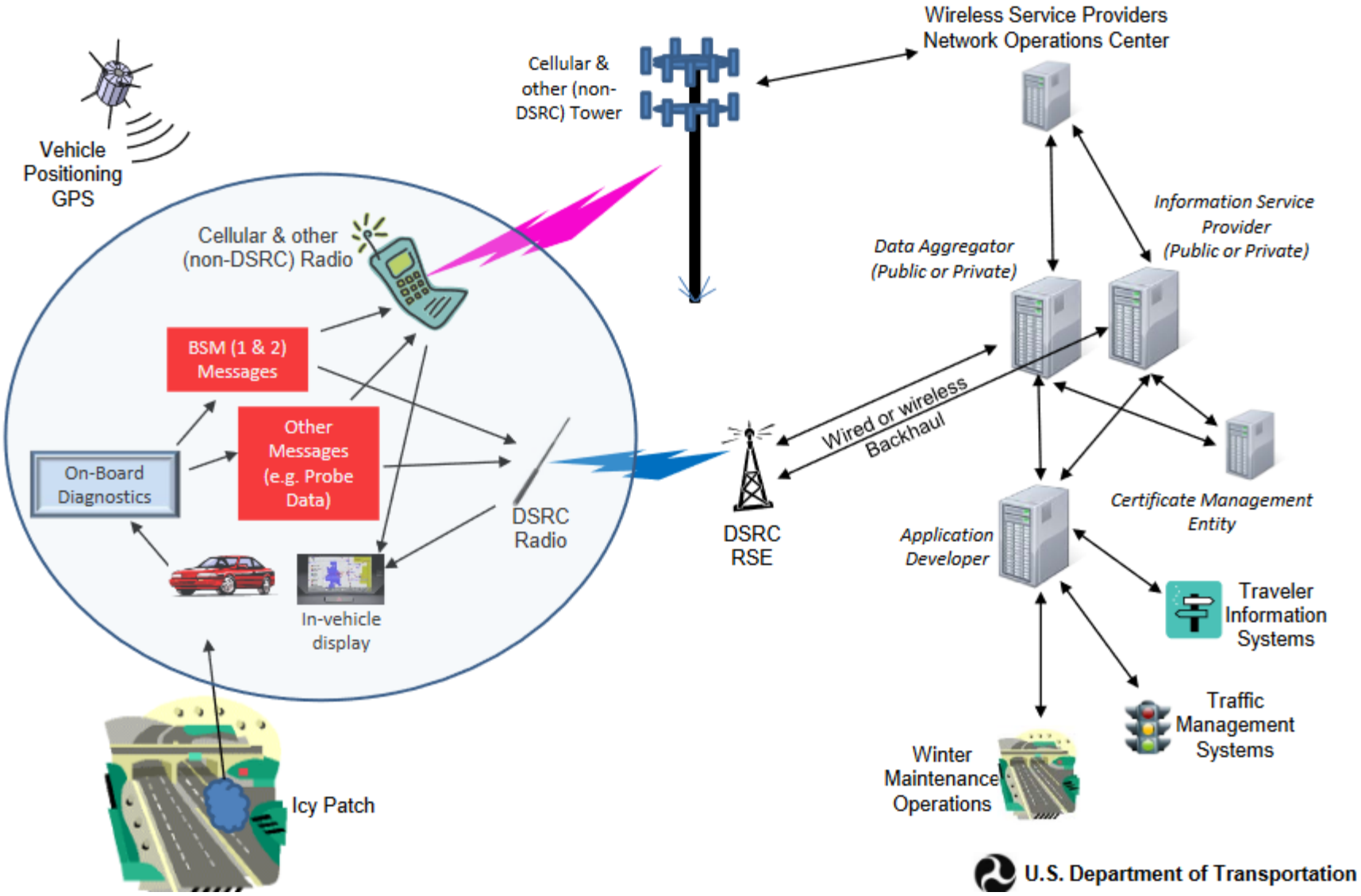
Part I is mandatory in the Basic Safety message

Vehicle Safety Extension

- **Event Flags**
- **Path History**
- **Path Prediction**
- **RTCM Corrections**

Required for V-V safety applications, but not in every message

Private Vehicles Receiving BSMs from DSRC and non-DSRC Sources



J2735 Message Priorities (2009)

.

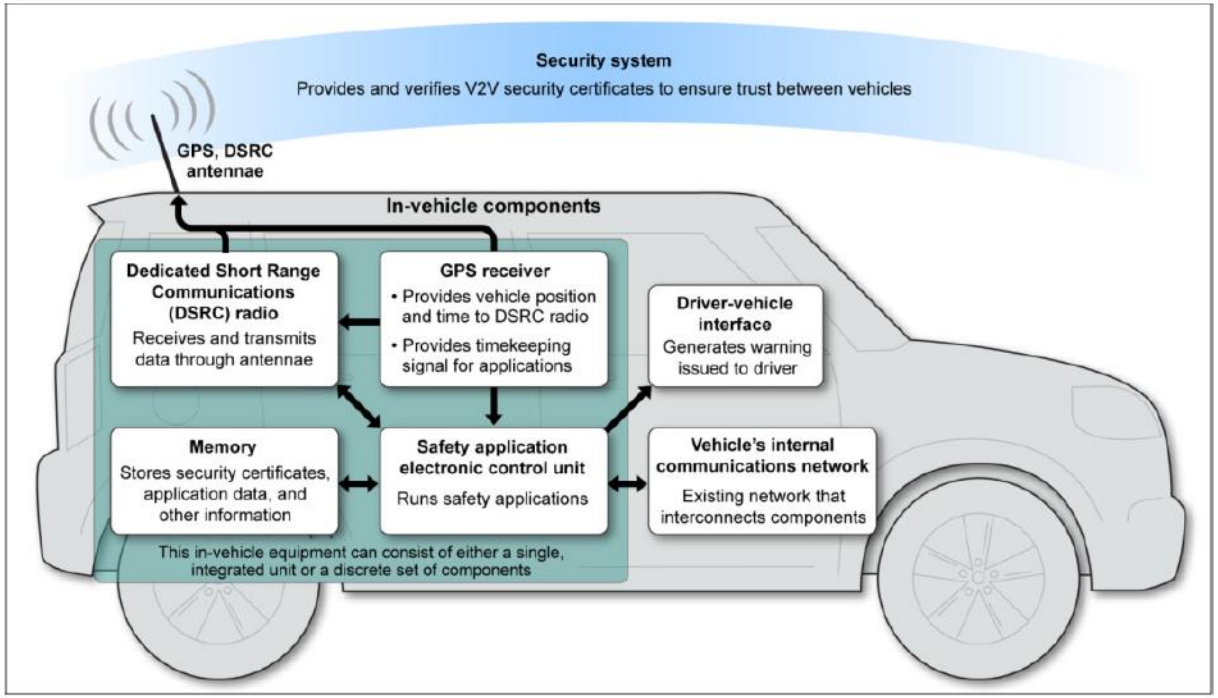
Safety of Life Messages

Public Safety Messages

Non-Priority Communications

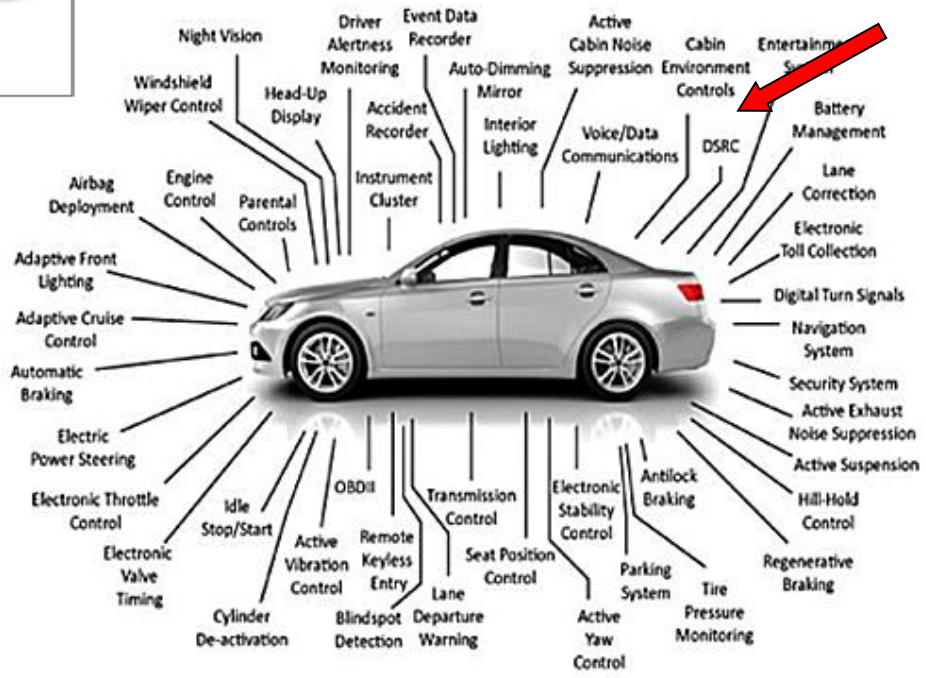
Importance Level from USA FCC Policy	Description (When to apply a specific urgency level)	Latency for Reception (Urgency)	J2735 Message Sets and Example(s)	Default Message Priority
1 = Safety of Life Applies to those Messages and Message Sets associated with societal and/or safety impact related to human life.	Emergency Impact mitigation and injury avoidance/mitigation	< 10 ms	Crash-Pending Notification (Example)	7
	Emergency Potential-event impact and/or injury mitigation and avoidance	< 10 ms	Pre-Crash (Example)	7
	Urgent Warning Events (using Event Flags)	< 10 ms	Basic Safety + Hard-Brake (Collision Warning, EEBL, Anti - Lock, etc.)	7
	Periodic public safety status information	10 to 20 ms	Basic Safety Message	5
	Urgent warning of impending local situation	10 to 20 ms	Emergency Vehicle Alert	5
	Situation-based status information of uninvolved local interest	10 to 20 ms	ATIS Roadside Alerts (e.g. Accident)	5
	Potential-situation information of uninvolved local interest	> 20 ms	ATIS Probable-situation (e.g. Rapidly deteriorating dangerous conditions)	3
2 = Public Safety (Safety not in 1) Applies to Road Side Units (RSU) and On-Board Units (OBUs) operated by state or local governmental entities presumptively engaged in public safety priority communications. (Includes Mobility and Traffic Management Features)	Urgent public safety downloads (Intersection Information)	< 10 ms	SPAT (Signal Phase and Timing)	6
	Public safety data transactions, exchanges	< 10 ms	Electronic Toll Collection (Example)	6
	Public safety geospatial context information	10 to 20 ms	GID message (Geospatial Context)	4
	Semi-urgent public safety link establishment	10 to 20 ms	Lane Coordination; Cooperative ACC (Example)	4
	Public safety RTCM GPS correction information	10 to 20 ms	RTCM GPSC (GPS Correction)	4
	Semi-urgent public safety data and application enabler	> 20 ms	Services Table, Digital Map Download (Example)	3
	Important Traffic Management status information enabler	> 20 ms	ATIS Alerts (e.g. Highway Closed Ahead)	3
	Important Announcement of Services	> 20 ms	WSA message (Wave Service Announcement*)	3
	Non-urgent Traffic Management Foundational Data	> 20 ms	Probe Messages, Localized warning zones update	3
3 = Non-Priority Communications (Not in 1 or 2) Applies to Fleet Management, Traveler Information Services and Private Systems.	Urgent, private mobility message	< 10 ms	On-Board Navigation Reroute Instructions	2
	Urgent, private and commercial electronic transactions	< 10 ms	Electronic Payments	2
	Semi-Urgent, private mobility data and electronic transactions	10 to 20 ms	Commercial applications (e.g., GPS driving instructions)	1
	Important, private and commercial electronic transactions	10 to 20 ms	Large commercial transactions (E-Commerce)	1
	Background, private mobility data downloads and upgrades	> 20 ms	Area map or database download or upgrade	1

Smart vehicle are *unsecure robots*



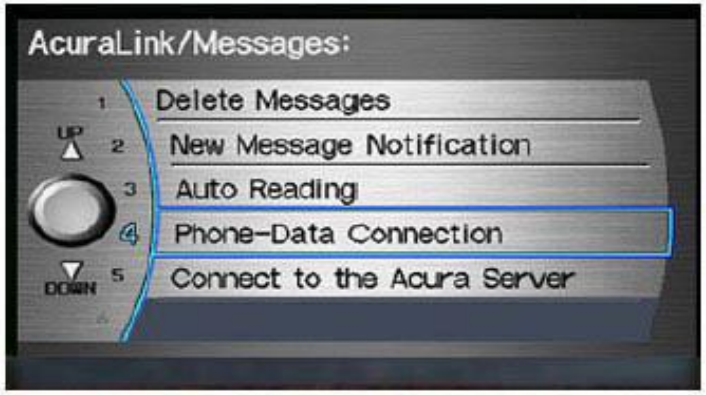
NHTSA also foresees the potential for V2V safety systems to be integrated into an existing electronic control unit(s) during large-scale production of vehicles equipped with these systems. Figure (left) illustrates the vehicle-based components needed for an integrated V2V system that uses integrated vehicle devices. (A V2V system with ASDs would only differ in its lack of connection to the vehicle's internal communications network.)

Modern cars include: more than 80 ECUs many logically interacting subsystems …sensors, actuators, and their intelligent interconnection



ITS Security and Privacy – Data You Can Trust

Privacy



Confidentiality

Availability

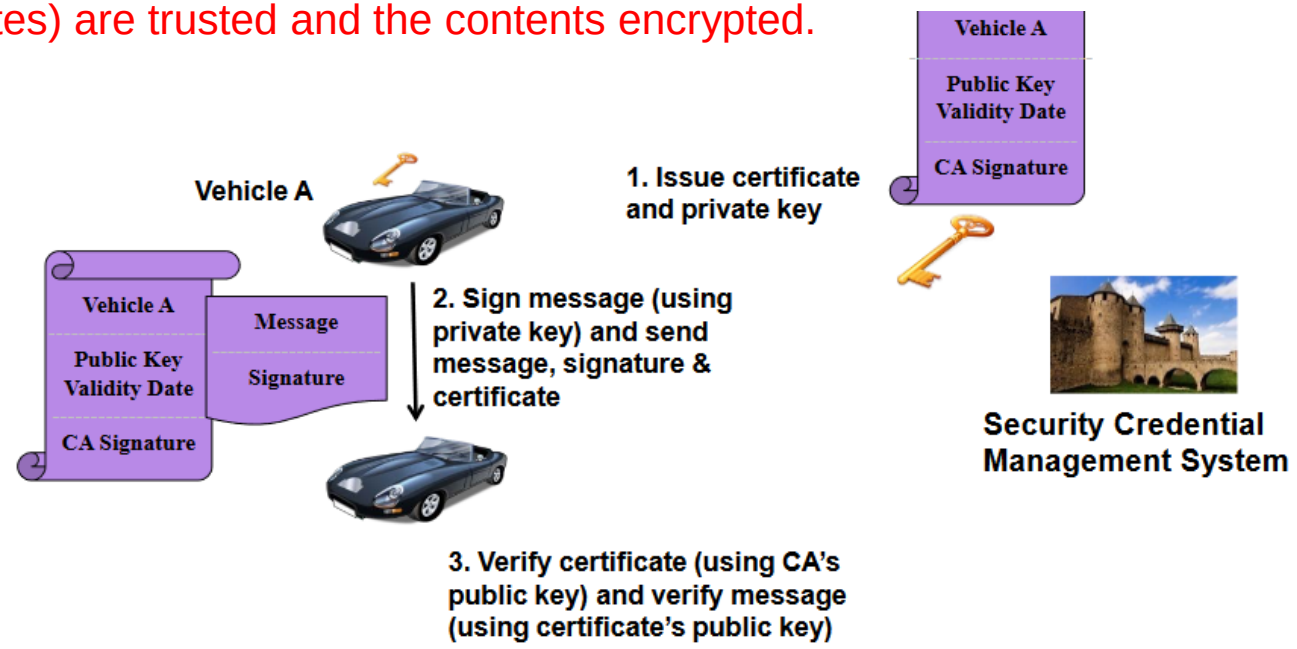
Integrity

Table of Contents

Vehicular Public Key Infrastructure (VPKI)

V2V communications consists of two types of messages: safety messages and certificate exchange messages. The safety messages are used to support the safety applications, and the certificate exchange messages ensure that the safety message is from a trusted source. The safety messages are transmitted in a standardized format so that they can be read by all other vehicles participating in the network.

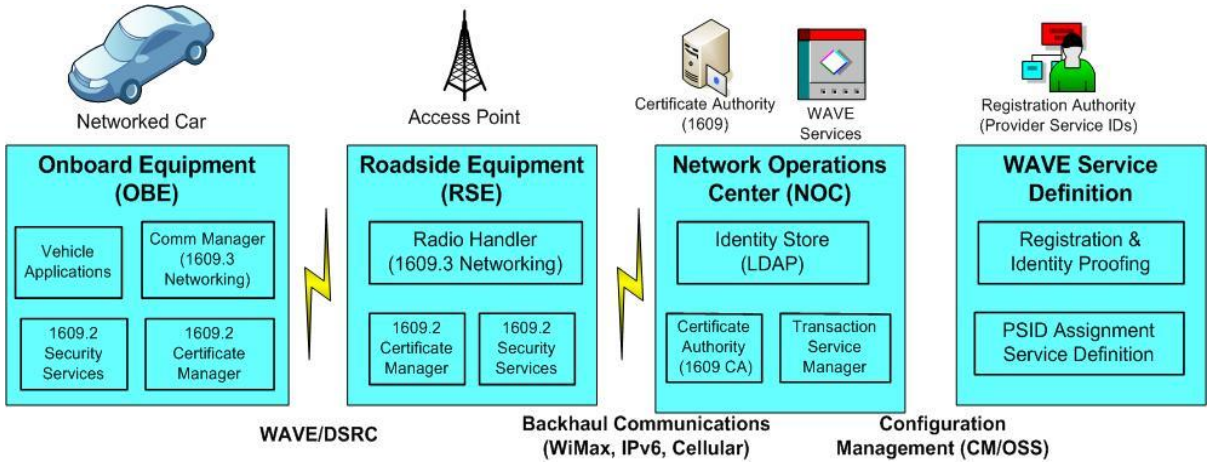
NHTSA's current research is based on the assumption that the V2V system will use a Public Key Infrastructure (PKI) to authenticate messages, so that other vehicles will trust the message. PKI uses certificates to inform a receiving device that the message is from a trusted source, and it uses cryptography to send encrypted message content. For V2V communications, BSM messages are trusted but not encrypted, while messages that contain security information (e.g., certificates) are trusted and the contents encrypted.

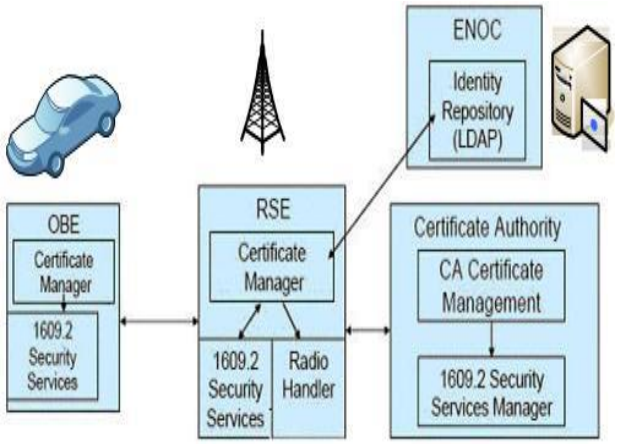


IEEE 1609.2 – Practical Internet of Things Security (Brian Russell)

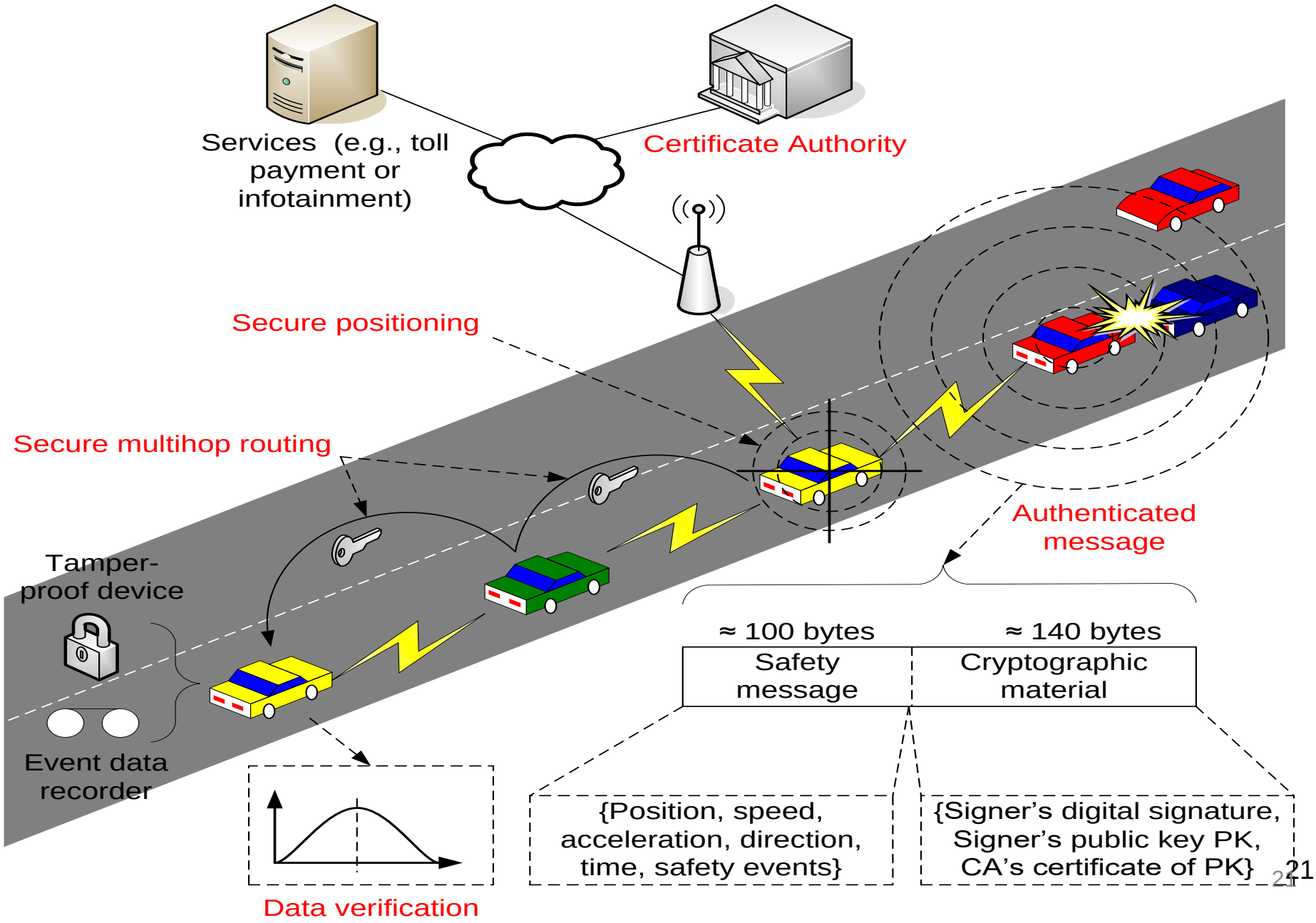
The US Dept Transportation (USDOT), and academia have been developing CV technology for many years and it will make its commercial debut in the 2017 Cadillac. In a few years, it is likely that most new US vehicles will be outfitted with the technology. ***The dedicated short range communications (DSRC) wireless protocol (based on IEEE 802.11p) is limited to a narrow set of channels in the 5 GHz frequency band. To accommodate so many vehicles and maintain security, it was necessary to 1) secure the communications using cryptography (to reduce malicious spoofing or eavesdropping attacks) and 2) minimize the security overhead within connected vehicle BSM transmissions.*** The industry resolved to use a new, slimmer and sleeker digital certificate design.

The 1609.2 certificate format is advantageous in that it is approximately half the size of a typical X. 509 certificate *while still using* ***strong, elliptic curve cryptographic algorithms (ECDSA and ECDH)****. The certificate is also useful for general machine-to-machine communication through its unique attributes, including explicit application identifier (SSID) and credential holder permission (SSP) fields*. These attributes can allow IoT applications to make explicit access control decisions without having to internally or externally query for the credential holder's permissions. ***They're embedded right in the certificate during the secure, integrated bootstrapping and enrollment process with the PKI***. The reduced size of these credentials also makes them attractive for other, bandwidth-constrained wireless protocol

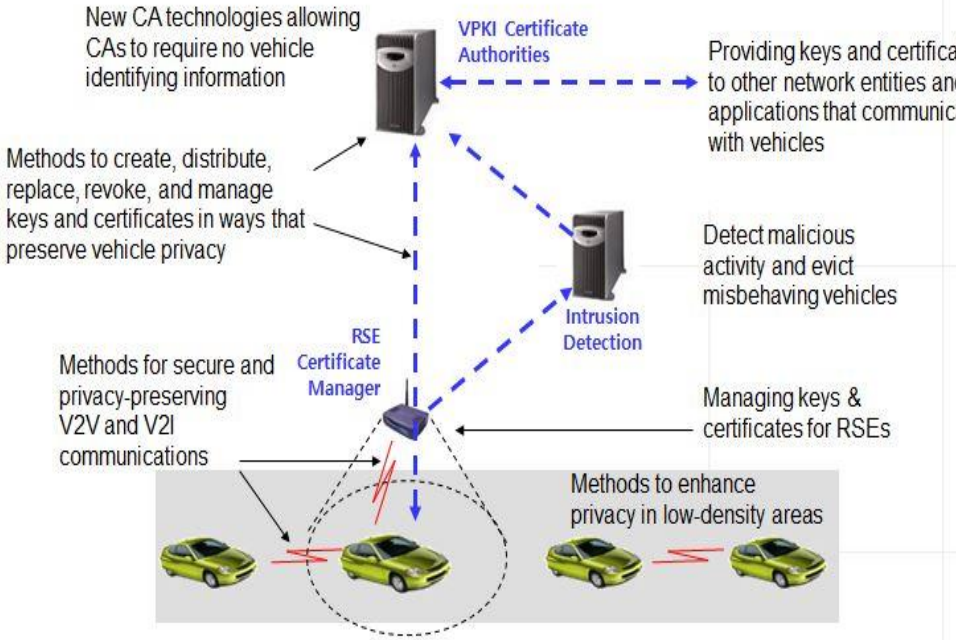


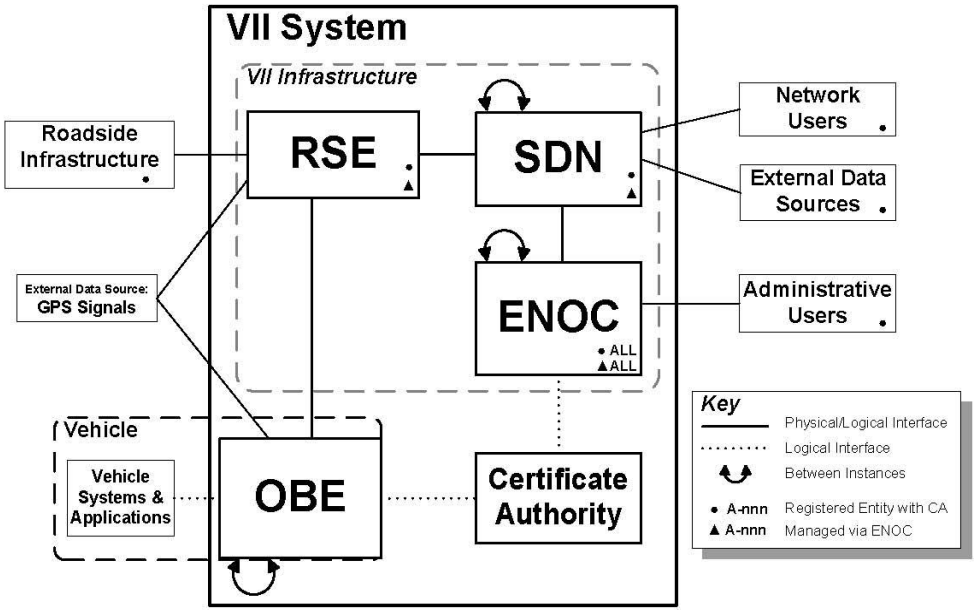


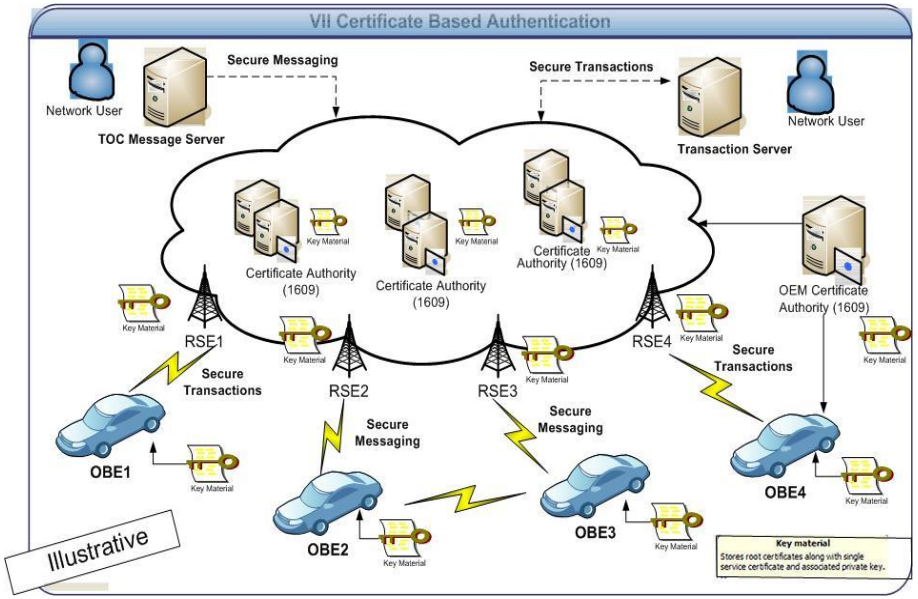
Security Architecture (EPFL V-PKI – J.Hubaux et. al.)

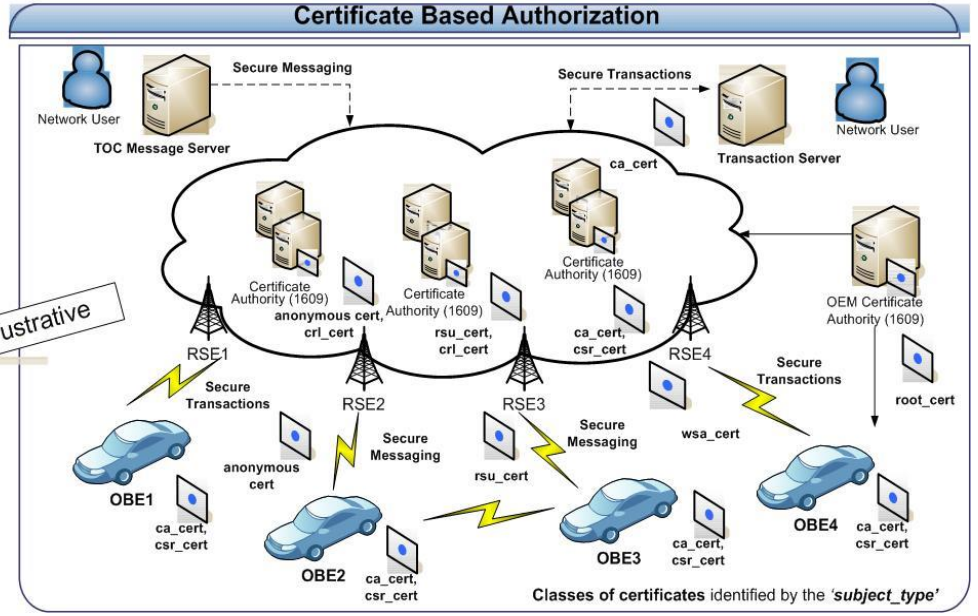


A quick look at VPKI for US DOT Pilots (10 year span)









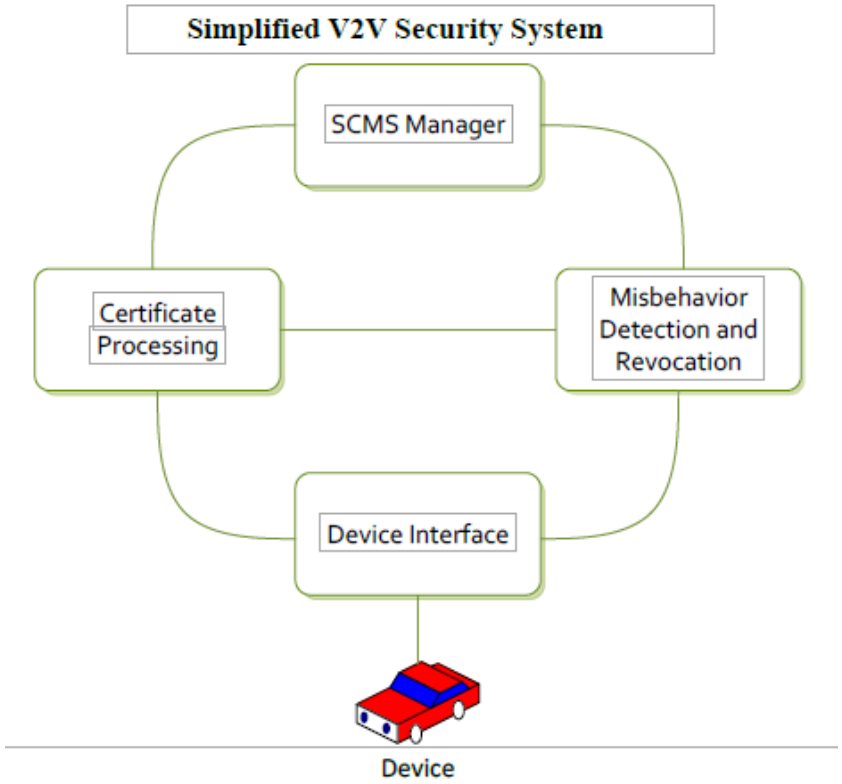
V2V Communications Security Research 2002 – 2015 (Booz Allen 2014 Report

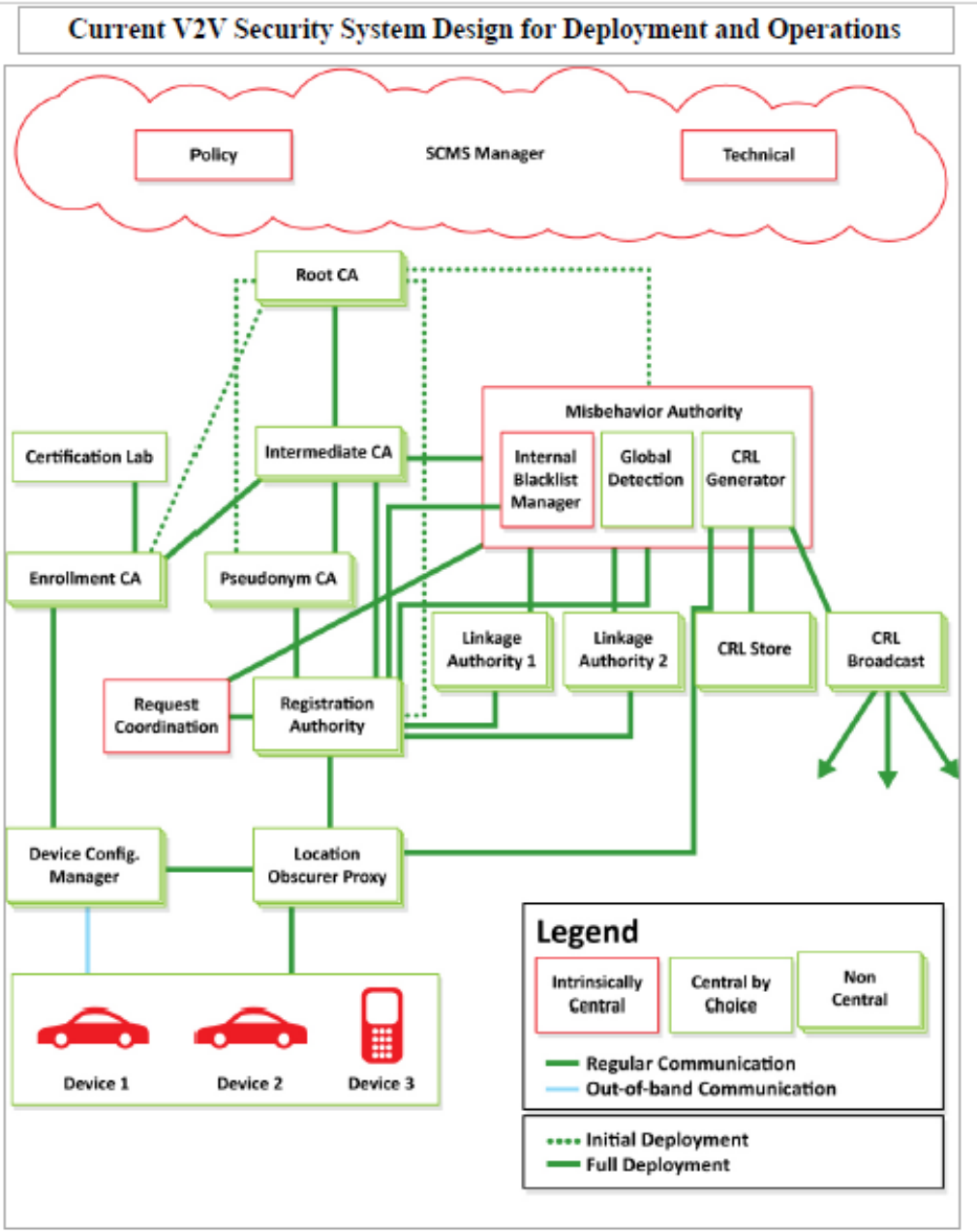
Research Project	Time Period	Research Focus
Vehicle Safety Communications (VSC)	2002-2005	Secure communications that included identifying options for: • Trust mechanisms • ID misbehaving devices • PKI architecture
Review by the National Institute of Standards and Technology (NIST)	2004	NIST reviewed the security options alternatives analysis, agreed with the security approach chosen (PKI), reviewed the emerging PKI configuration for V2V, and identified concerns that the research team would need to address as development moved forward.
Vehicle Safety Communications – Applications (VSC-A)	2006-2010	Development of high-level security design that covered: • Over-the-air performance of an authentication scheme • Identification of privacy mechanisms • Analysis of channel options for security • Refinement of the attacker model • Initial development of misbehavior detection schemes

Research Project	Time Period	Research Focus
Vehicle-to-Vehicle-Communications Security (V2V-CS)	2010-2012	Research Objectives included: • Determined security requirements and derived communication channel requirements. • Delivered a simplified initial and final deployment security model that identified the 3000/year certificate model with no infrastructure required for the first three years. • Performed a system-based risk assessment using the proposed initial and full deployment models. Assessment identified both privacy and security risks. • Began definition of the SCMS to understand the organizational and operational requirements; identified a need to research ownership/operations from a centralized versus non-centralized perspective. • This version of the SCMS formed the basis for the Safety Pilot Model Deployment prototype.
Vehicle-to-Vehicle-Interoperability, Phase 1 (V2V-I)	2010-2012	Research objectives for defining interoperability included further research into security from an operational perspective. The research covered: • Definition of a concept of operations for a V2V security; tested the operations with 200 vehicles to observe channel congestion using both cellular and DSRC. • Definition of a process of certificate management and an initial process for misbehavior detection. • Publication of design specifications on IP.com and licensing of the operational design for use in the Safety Pilot Model Deployment.
Oak Ridge National Laboratories (ONRL)	2012	Before the launch of the Safety Pilot Model Deployment, ORNL tested the prototype security system.

Research Project	Time Period	Research Focus
Safety Pilot Model Deployment (SPMD)	2012-2013	Implementation of a prototype that included: • Support for device initialization • Pre-load of certificates onto devices • Over-the-air certificate reload • Testing of the certificate revocation list • Testing of misbehavior reporting function
Vehicle-to-Vehicle-Vehicle Safety Communications Security Studies (V2V-VSCS)	2012-2014	Research is underway and includes: • Finalization of the SCMS design with a focus on simplifying and optimizing operations • Cost analysis of the SCMS with a sensitivity analysis on the assumptions associated with the current design concept. • Identification of optional methods to link batches of on-board equipment devices to enrollment certificates
V2V Interoperability Project/Phase 2 (V2V-I/Phase 2)	2012-2014	Research is underway and is focused on misbehavior detection and reporting – the algorithms and operational requirements needed to ensure that this function works under real-world conditions that will lead to development of a deployment use case.
Independent Evaluation of V2V Security System Design	2014-2015	To better understand the state of the current design, the DOT needs an independent entity's assessment to inform the DOT of the status of the design and provide a basis for future policy and technical decisions.

Introducing the Security Credential Management Systems (VPKI)



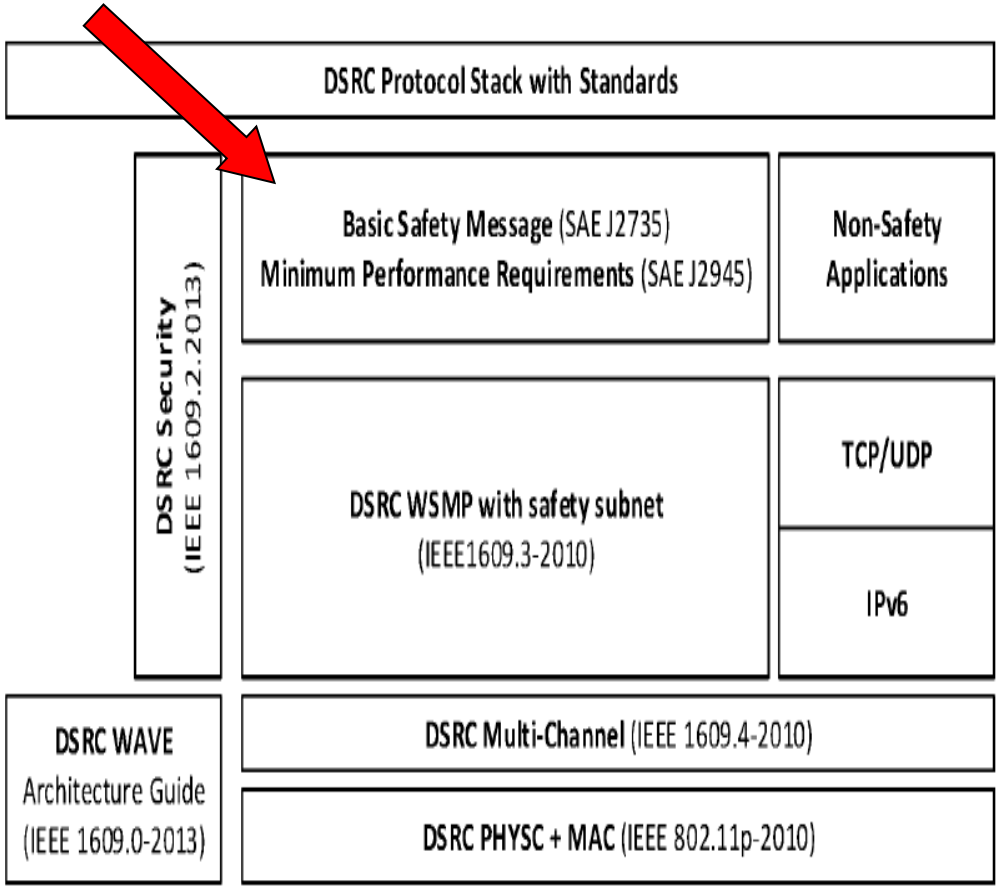


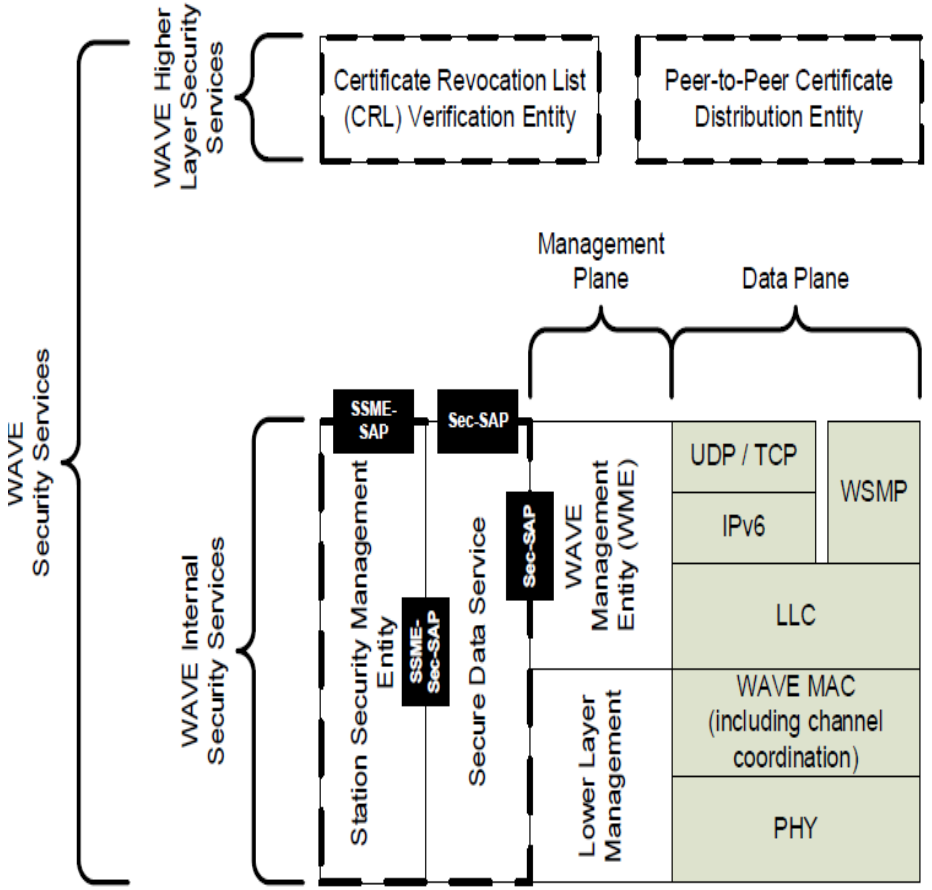
This image presents both an initial deployment model as well as a full deployment model. Note that this diagram shows the initial deployment model where there is no Intermediate CA and the Root CA talks to the MA, PCA, and ECA (dotted lines). In the full deployment model, these entities communicate with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

SCMS Component Functions

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	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

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



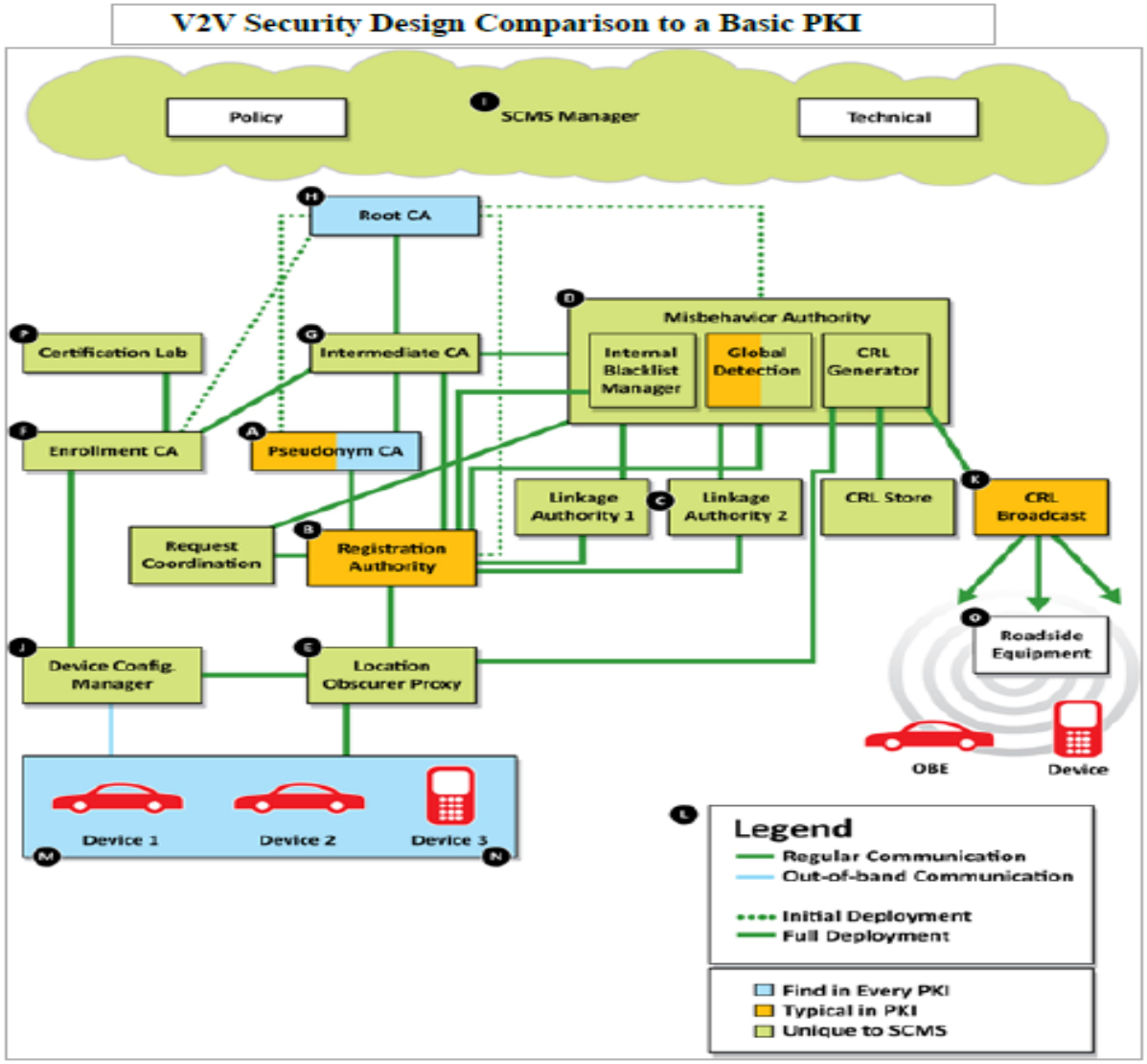


WAVE Security Services for Applications and Management Messages (1609.2)

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 subet 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

Table of Contents

SCMS vs Traditional PKI Models



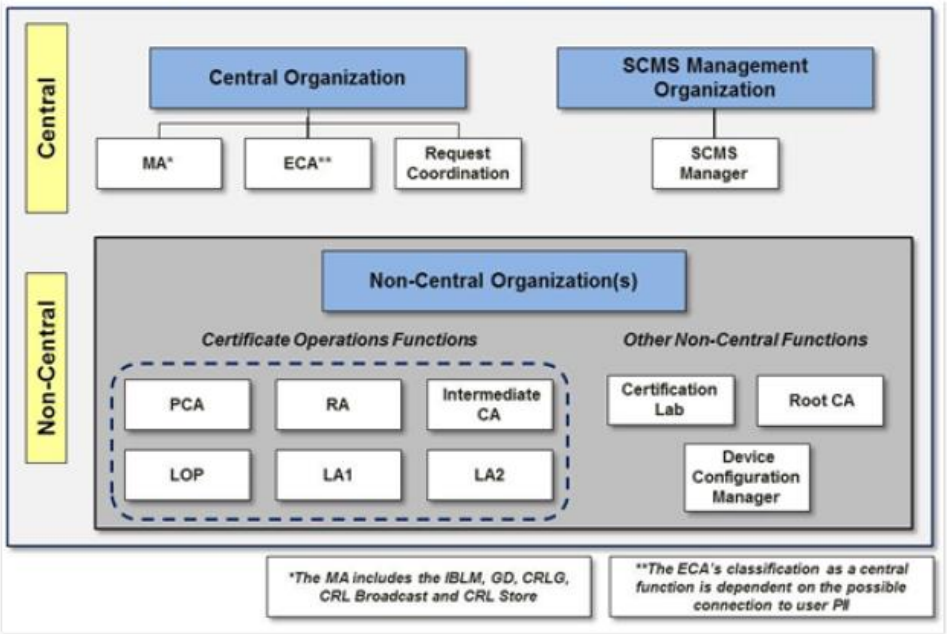
SCMS is a tailored public key infrastructure (PKI) that is designed to provision PKI certificates to vehicles and infrastructure.The SCMS employs components such as location obscurer proxies (LOPs) that shield vehicle identities from PKI components and by extension operators. Vehicles themselves employ a concept of rotating certificates taken from a pool, and then used to digitally sign messages.

SCMS implements a PKI with some additional new features. This SCMS is currently the leading candidate design for the V2V security backend design in the US, It is distinguished from a traditional PKI in several aspects, the two most important ones being its size (i.e., the number of vehicles that it supports) and the balance among security, privacy, and efficiency. At its full capacity, assuming 300 million vehicles, it will issue approximately 300 billion certificates per year1. The largest current PKI, deployed by the US Department of Defense, is several orders of magnitude smaller and issues under 10 million certificates per year.

SCMS design is significantly different from any previously implemented PKI due to the underlying security objectives and size, however, it is somewhat similar to the design of the European V2X PKI [2]. The main differences to [2] include an increased focus on privacy against attacksf rom SCMS insiders, efficient handling of revocation, and an efficient method for updating certificates based on the butterfly key expansion algorithm.

SCMS vs Traditional PKI Models (BAH Conceptual Diagram)

Security Certificate Management System Organizational Model



Function name	Activities
Certification Lab	Tests OBE and informs ECA that units of a particular type are eligible for enrollment certificates.
Device Configuration Manager	Coordinates initial distribution with OBE and enables OBE to request certificates from RA.
Enrollment Certificate Authority	Activates OBE and credentials users.
Intermediate Certificate Authority	Shields Root CA from system and provides more flexibility for trust management.
Linkage Authority	Each pair of LAs communicates with the RA to provide linkage values necessary for certificate production, and assists the MA in misbehavior processes.
Location Obscurer Proxy	Obscures the locations of requesting devices (e.g., OBE requesting certificates) from other functions, such as the RA.
Misbehavior Authority	Collects misbehavior reports from OBE and analyzes system-wide misbehavior. Coordinates with PCA and RA to produce CRL. Other activities include CRL generation, broadcast, and store; internal blacklist manager (IBLM); and global detection.
Pseudonym Certificate Authority	Generates and signs short-lived certificates.
Registration Authority	Coordinates certificate production with other functions; sends certificates to OBE (during full deployment).
Request Coordination	Coordinates certificate requests from OBE to RA.
Root Certificate Authority	Provides system-wide confidence through CME certificates issued to all CMEs; represents the basis of confidence in the system.
Security Credentials Management System Manager.	Defines and oversees standards and practices for the SCMS, related to both technical and policy issues.

The CAMP SCMS design features a CA hierarchy, with:

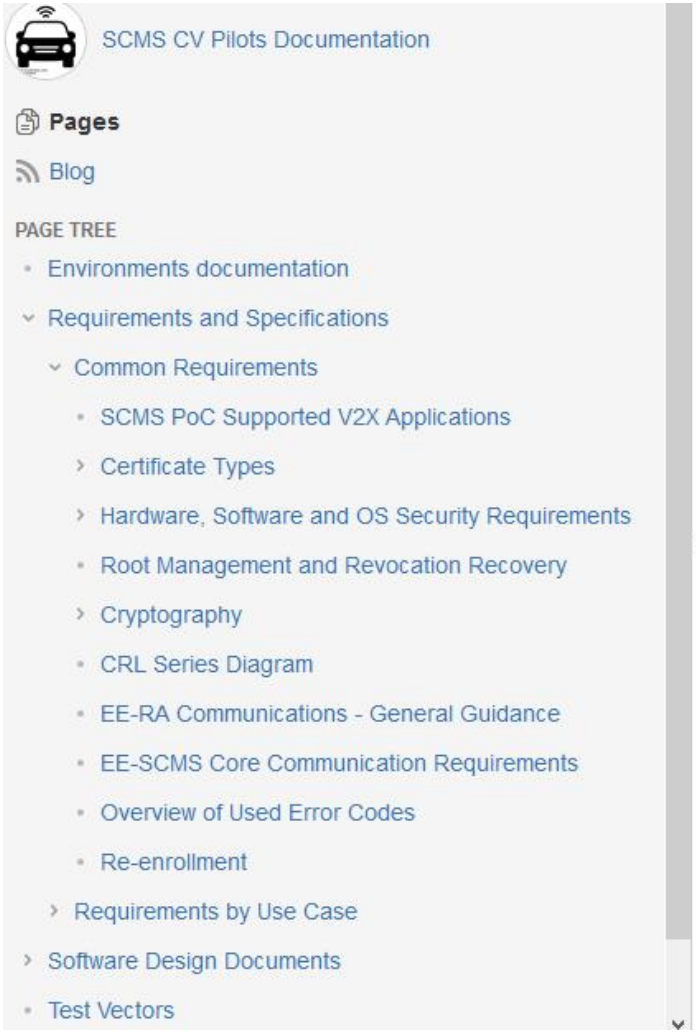
- A root CA that issues certificates for other CAs but not for vehicles or other end-entities
- Optionally, intermediate CAs (ICAs), which obtain their certificates from other CAs above them and also issue certificates for other CAs rather than end-entities. The advantage of using intermediate CAs is that if an intermediate CA is compromised, it is less catastrophic than if the root CA is compromised, so this gives the system more flexibility to introduce new CAs without running the risks incurred by using the root CA key. It is possible to use intermediate CAs in a cascade, so an intermediate CA is either validated by the root CA or the intermediate CA above it.
- Enrollment authorities that issue enrollment certificates (long-term certificate signing requests) for the end-entities. These enrollment certificates are used only to communicate with the SCMS, not with other vehicles or end-entities**. Note: the lifetime of the certificate is currently assumed to be the lifetime of a car (e.g., 30 years). However, this still needs discussion as it influences the size of the internal blacklist and is hence a cost issue**. Note: the certificate lifetime and the lifetime of the actual CA do not have to be equal.
- Pseudonym CAs that issue certificates for the applications on the cars

The CAMP SCMS also distinguishes between the CA, which actually signs the certificate and the RA, which approves certificate requests.

Table of Contents

SCMS CV Pilots Documentation Online

https://wiki.campllc.org/display/SCP/SCMS+CV+Pilots+Documentation



SCMS Requirements by Use Case

https://wiki.campllc.org/pages/viewpage.action?pageId=58589462

Use Case 3: OBE Pseudonym Certificates Provisioning

Created by Benedikt Brecht, last modified by Roger Motz on Mar 27, 2017

Target release	Release 0.1
Document owner	@Virendra Kumar
Reviewer	@Roger Motz, @Benedikt Brecht

Goals

The goal is to provide a freshly bootstrapped OBE with the very first batch of pseudonym certificates that it can use in applications like Basic Safety Message (BSM).

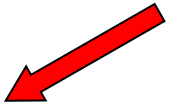
Background and Strategic Fit

The initial provisioning of pseudonym certificates is the process by which an OBE receives its very first batch of pseudonym certificates. This use case also acts as a trigger for subsequent provisioning of pseudonym certificates. The OBE does not need to make any more requests, the RA automatically does everything necessary (such as doing the butterfly key expansion, getting pre-linkage values from the LAs, making individual certificate requests to the PCA, etc.) for the next batches of certificates.

Due to the time constraints imposed by the OEMs, shuffling requirements for the initial provisioning may be relaxed.

This use case involves the following SCMS components:

- Linkage Authorities (LAs)
- Location Obscurer Proxy (LOP)
- Pseudonym Certificate Authority (PCA)
- Registration Authority (RA)



At the start of this use case, the OBE has no pseudonym certificates. At the end of this use case, the OBE has three years worth of pseudonym certificates, and the RA has everything it needs from the OBE for generating and providing subsequent pseudonym certificate batches for the OBE.

SCMS Certificate Types

https://wiki.campllc.org/display/SCP/Certificate+Types

On-Board Equipment (OBE)

OBE Enrollment

An enrollment certificate is like a passport for the OBE in that it uses the enrollment certificate to request other certificates: pseudonym and identification certificates. It does not have an encryption key. It is provided to the OBE during its **bootstrap** process.

Pseudonym

Pseudonym certificates are used by an OBE primarily for BSM authentication and misbehavior reporting and do not have encryption keys.

Identification

Identification certificates are used by an OBE primarily for authorization in V2I applications.

Road-Side Equipment (RSE)

RSE Enrollment

An enrollment certificate is like a passport for the RSE in that it uses the enrollment certificate to request application certificates.

Application

Application certificates are used by an RSE for authentication and encryption; therefore, they might have **encryption keys**. As there are no privacy constraints for RSEs, an RSE has **only one** application certificate valid at a time for a given application.

The V2X system uses several types of certificates. SCMS components generate these and in many cases can also revoke them. All the EE certificates are of **implicit** type to save storage space and over-the-air bytes. All the SCMS component certificates are of **explicit** type.

A certificate is expected to be 117 bytes. The number of unique certs/year * size of **one certificate. (103680 * 117 = *12.13MB for one vehicle for one year). *300 million vehicles = 3,639,168,000,000,000. Or 3.6 exabytes*.**

SCMS Component

The elector, root CA, PCA, and ICA certificates are of explicit type to support P2P distribution, There are no privacy constraints for any of the SCMS component certificates.

Electors

Elector certificates are not part of the PKI hierarchy of the SCMS, i.e., verifying a certificate chain in the system does not involve verifying elector certificates. They are used primarily for root CA certificate management, including adding and removing a root CA.

Root CA

The root CA certificate is different from all other types of certificates in many ways:

1. It is the end of trust chain, i.e., verification of any certificate in the system ends at verifying this certificate
2. The signature on the root CA certificate does not have any cryptographic value as the signature is by the root CA itself, and, therefore, the trust in a root CA certificate is established through out-of-band means
3. Usually the root CA certificate has a long lifetime, as changing a root CA certificate is a time consuming, and potentially expensive operation
4. Only a quorum of electors can issue root management messages and add them to a CRL to revoke a root CA certificate

ICA

ICA certificates can be used to only issue certificates to other SCMS components and nothing else. Only the root CA or the ICA can issue, or authorize someone to issue, a CRL to revoke an ICA certificate.

A root CA certificate does not have an encryption key as the root CA is mostly offline and does not accept any incoming messages, whether encrypted or not. The root CA certificate needs to be made available to everyone in the system. The initial provisioning of the root CA certificate is done through out-of-band means in a secure environment during enrollment

SCMS Certificate Types and EE Certificate Type Features

https://wiki.campllc.org/display/SCP/Certificate+Types

EE Certificate Type Features

The following table provides an overview of the EE certificate types. 'X' describes mandatory features, and '(x)' describes optional features. The table provides a comprehensive overview. The following are assumptions for the POC:

- All RSEs have regular connectivity. Hence, case 5.b is not implemented
- The response by the PCA is not encrypted for case 3 and case 5

	OBE Enrollment Certificate	OBE Pseudonym Certificate	OBE Identification Certificate	RSE Enrollment Certificate	RSE Application Certificate	
					RSE with Connectivity	RSE without Connectivity
Provisioning	1 per EE per PSID category	20 per week, up to 3 years, top-up refresh using butterfly keys	1 per time period, only issue very small number of certificates at a time, top-up refresh using butterfly keys	1 per EE per PSID category	1 per time period, only issue for short time periods, require frequent renewal. RSE generates public/private key pair and provides public-key to RA	1 per time period, issue longer time periods. RSE generates public/private key pair and provides public-key to RA
Revocation	RA blacklist	leverage linkage values	add certificate digests of all issued certificates (can be more than one)	RA blacklist	Cannot renew certificates, due to RA blacklist of enrollment certificate	Add certificate digest of all issued certificates (can be more than one)

Table 1. Certificate types for testing.

Issued to	Certificate name	Purpose
OBU*/ASD	Enrollment	Initializes the OBU to allow communication with the SCMS
OBU/ASD	Pseudonym	Used to sign all basic safety messages generated by an OBU
OBU	Authorization	Used to identify public sector vehicles for specific apps
RSU	Enrollment	Initializes the RSU to allow communication with SCMS
RSU	Application	Used to sign messages generated by the RSU

**OBU: onboard unit; ASD: aftermarket safety device; RSU: roadside unit; SCMS: Security Credential Management System*

SCMS Component

ECA

As mentioned above, ECA certificates are of **explicit** type as they do not need to be distributed through P2P distribution. ECA certificates can be used to only issue certificates to end-entities including OBEs and RSEs.

PCA

PCA certificates can be used to only issue certificates to end-entities including OBEs and RSEs.

CRL Generator

CRL generator certificates are issued by the root CA and can be used only to sign CRLs, and nothing else. As revocation of CRL generator certificates is difficult (i.e., can be done by either root CA or ICA), the validity period of the CRL generator certificates is kept as low as possible.

Policy Generator

Policy generator certificates are issued by the root CA and can be used only to sign the global policy configuration files that are distributed to SCMS components. The policies around validity are the same as for CRL generator certificates.

LA Certificates

Can be short as LAs do not interact with end-entities.

RA Certificates

Must be long enough so that end-entities can successfully make a certificate provisioning request after being bootstrapped.

MA Certificates

Needs to be long so that end-entities do not need to retrieve these certificates very often.

SCMS POC Supported V2X Applications and PSIDs

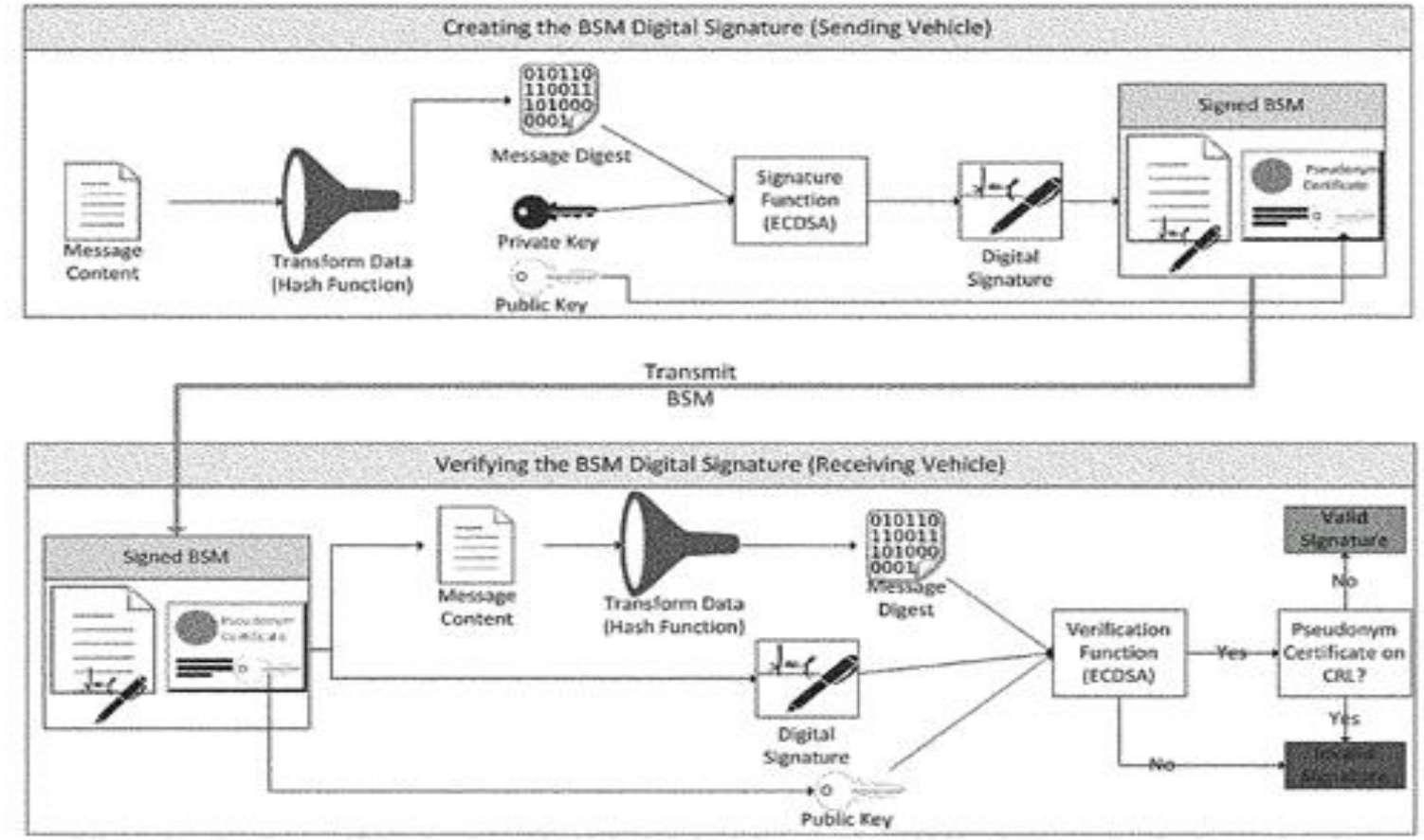
https://wiki.campllc.org/display/SCP/SCMS+PoC+Supported+V2X+Applications

Application	Application Category	PSID Decimal
Basic Safety Message (BSM)	BSM inputs	32
Vehicle Turning Right in Front of Bus Warning	BSM inputs	32
Intelligent Traffic Signal System (I-SIG) In-Vehicle Information Potential	BSM inputs	32
Forward Collision Warning (FCW)	BSM inputs	32
Emergency Electronic Brake Light (EEBL)	BSM inputs	32
Blind Spot Warning (BSW)	BSM inputs	32
Lane Change Warning/Assist (LCA)	BSM inputs	32
Intersection Movement Assist	BSM inputs	32
Stationary Vehicle Ahead (SVA)	BSM inputs	32
Do Not Pass Warning	BSM inputs	32
Probe Enabled Traffic Monitoring	BSM inputs	32

Application	Application Category	PSID Decimal
CV-enabled Weather-Responsive Variable Speed Limits	9 - Temporary Situation Warning	131
Road Weather Advisories for Trucks and Vehicles	9 - Temporary Situation Warning	131
Emergency Communications and Evacuation (EVAC)	9 - Temporary Situation Warning	131
WAVE Service Advertisement	Support	135
Certificate Revocation List Application	Support	256
CV Pilot Application 1		2,113,672
CV Pilot Application 2		2,113,673
CV Pilot Application 3		2,113,674
CV Pilot Application 4		2,113,675
CV Pilot Application 5		2,113,676

Application	Application Category	PSID Decim
Misbehavior Reporting for Common Applications	Support	38
Differential GPS Corrections, Uncompressed	Support	128
Differential GPS Corrections, Compressed	Support	129
Red Light Violation Warning/RSE	3 - Signal Violation Warning	130
Pedestrian in Signalized Crosswalk Warning/RSE	16 - Pedestrian Warnings	130
Mobile Accessible Pedestrian Signal System (PED-SIG)	16 - Pedestrian Warnings	130
Transit Signal Priority/ Special Vehicles	1 - Signal Pre-emption/Priority	130
Modified Eco-Speed Harmonization/RSE	2 - Speed Harmonization	131
Modified Eco-Speed Harmonization/TMC	2 - Speed Harmonization	131
Curve Speed Warning	8 - Curve Speed Warning	131
Reduced Speed/Work Zone Warning/RSE	9 - Temporary Situation Warning	131
Reduced Speed/Work Zone Warning/TMC	9 - Temporary Situation Warning	131
Spot Specific Weather Warnings/RSE	9 - Temporary Situation Warning	131
Spot Specific Weather Warnings/TMC	9 - Temporary Situation Warning	131
Variable Speed Limits/RSE	10 - Speed Zone	131
Variable Speed Limits/TMC	10 - Speed Zone	131
Speed Harmonization/RSE	2 - Speed Harmonization	131
Speed Harmonization/TMC	2 - Speed Harmonization	131
Work Zone Alerts/RSE	9 - Temporary Situation Warning	131
Work Zone Alerts/TMC	9 - Temporary Situation Warning	131
Truck Restrictions/RSE	11 - Special Vehicle Warning	131
Truck Restrictions/TMC	11 - Special Vehicle Warning	131
Automatic Alerts for First Responders	11 - Special Vehicle Warning	131

SCMS Cryptographic Methods (NHSTA NPRM pg 3908)
Transmitting a digitally signed Basic Safety Message



The V2V device generates the private key & public keys. The public key is sent to the SCMS to incorporate into a certificate that is signed by the PCA. The private key is always kept secret with the V2V device. The private key is vital to the signing process and must be kept secured at all times.

SCMS Cryptographic Test Vectors

https://stash.campllc.org/projects/SCMS/repos/crypto-test-vectors

Linkage Values - To support efficient revocation, end-entity certificates contain a linkage value (LV), which is derived from (cryptographic) linkage seed material. Publication of the seed is sufficient to revoke all certificates belonging to the revoked device, but without the seed an eavesdropper cannot tell which certificates belong to a particular device.

Butterfly Expansion Function - Butterfly Keys are a novel cryptographic construction that allow a device to request an arbitrary number of certificates, each with different signing keys and each encrypted with a different encryption key, using a request that contains only one verification public key seed and one encryption public key seed and two “expansion functions.

Key Derivation Function, **KDF2 with SHA-256** - test vectors of HMAC-SHA-256

Message Authentication Code, MAC1 (HMAC) with SHA-256 - **Message Authentication Code (MAC)** is a short piece of information used to authenticate a message and to provide integrity and authenticity assurances on the message.

AES-CCM-128 Symmetric Authenticated Encryption [IEEE-1609.2] - **Advanced Encryption Standard** (**AES**), also known as Rijndael (its original name), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001

ECDH Key Agreement - Elliptic Curve Diffie-Hellman is a public-key primitive where two parties can compute a shared secret by exchanging public keys and employing them and the corresponding private keys in the computation

ECIES Public-Key Encryption [IEEE-1609.2] - **Elliptic Curve Integrated Encryption Scheme**, or **ECIES**, is a hybrid encryption system proposed by Victor Shoup in 2001. ECIES combines a Key Encapsulation Mechanism (KEM) with a Data Encapsulation Mechanism (DEM). The system independently derives a bulk encryption key and a MAC key from a common secret. Data is first encrypted under a symmetric cipher, and then the cipher text is MAC'd under an authentication scheme. Finally, the common secret is encrypted under the public part of a public/private key pair

Implicit Certificate Generation and Public/Private Keys Reconstruction - Implicit certificates are employed for pseudonym certificates, enrollment certificates, etc. They do not contain the subject's public key and are not signed by the issuer, as is the case with explicit certificates, rather they contain a public key reconstruction point that is used to reconstruct the public key of the subject knowing the public key of the issuer

Table of Contents

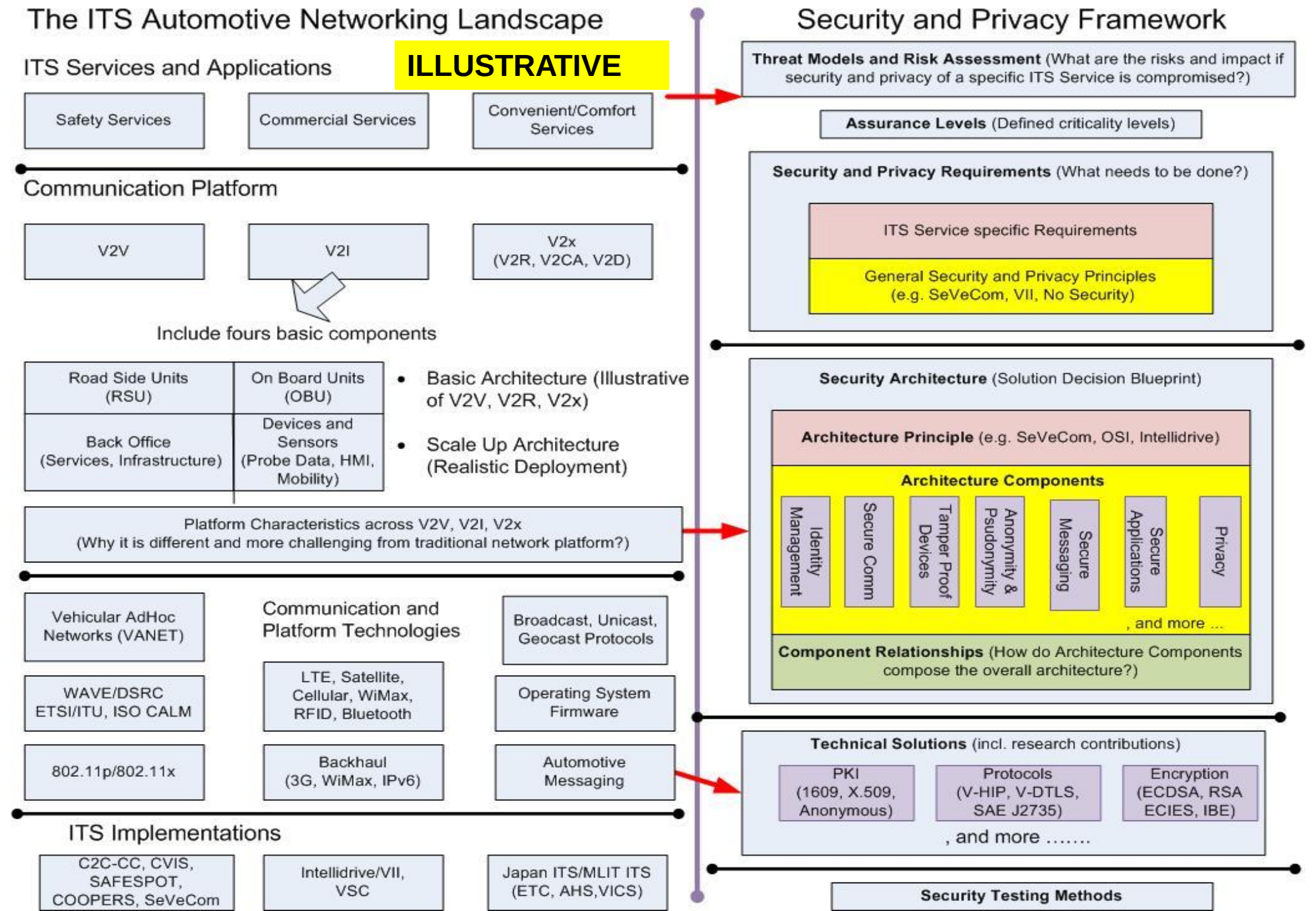

The ITS Automotive Networking Landscape
ILLUSTRATIVE
ITS Services and Applications
Safety Services
Commercial Services
Convenient/Comfort Services
Communication Platform
V2V
V2I
V2x (V2R, V2CA, V2D)
Include fours basic components
Road Side Units (RSU)
On Board Units (OBU)
Back Office (Services, Infrastructure)
Devices and Sensors (Probe Data, HMI, Mobility)
Basic Architecture (Illustrative of V2V, V2R, V2x)
Scale Up Architecture (Realistic Deployment)
Platform Characteristics across V2V, V2I, V2x (Why it is different and more challenging from traditional network platform?)
Vehicular AdHoc Networks (VANET)
WAVE/DSRC ETSI/ITU, ISO CALM
802.11p/802.11x
Communication and Platform Technologies
LTE, Satellite, Cellular, WiMax, RFID, Bluetooth
Backhaul (3G, WiMax, IPv6)
Broadcast, Unicast, Geocast Protocols
Operating System Firmware
Automotive Messaging
ITS Implementations
C2C-CC, CVIS, SAFESPOT, COOPERS, SeVeCom
Intellidrive/VII, VSC
Japan ITS/MLIT ITS (ETC, AHS,VICS)
Security and Privacy Framework
Threat Models and Risk Assessment (What are the risks and impact if security and privacy of a specific ITS Service is compromised?)
Assurance Levels (Defined criticality levels)
Security and Privacy Requirements (What needs to be done?)
ITS Service specific Requirements
General Security and Privacy Principles (e.g. SeVeCom, VII, No Security)
Security Architecture (Solution Decision Blueprint)
Architecture Principle (e.g. SeVeCom, OSI, Intellidrive)
Architecture Components
Identity Management
Secure Comm
Tamper Proof Devices
Anonymity & Psudonymity
Secure Messaging
Secure Applications
Privacy
, and more ...
Component Relationships (How do Architecture Components compose the overall architecture?)
Technical Solutions (incl. research contributions)
PKI (1609, X.509, Anonymous)
Protocols (V-HIP, V-DTLS, SAE J2735)
Encryption (ECDSA, RSA ECIES, IBE)
, and more .....
Security Testing Methods

Table of Contents

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

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

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

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

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

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

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

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

How are Provider Service IDs (PSIDs) Provisioned and Deployed?

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

Applications Supported by PSID

SPaT & MAP
Red Light Violation Warning
Pedestrian in Signalized Crosswalk Warning
Mobile Accessible Pedestrian Signal System

Basic Safety Message
Probe Enabled Traffic Monitoring
Intelligent Traffic Signal System In-Vehicle Information Potential
Vehicle Turning Right in Front of Bus Warning
Forward Collision Warning
Emergency Electronic Brake Light
Blind Spot Warning
Lane Change Warning / Assist
Intersection Movement Assist
Stationary Vehicle Ahead
Do Not Pass Warning

Traffic Signal Preemption
Transit Signal Priority / Special Vehicles

Speed Harmonization
Modified Eco-Speed Harmonization
Speed Harmonization

Basic Information Message
Curve Speed Warning
Reduced Speed / Work Zone
Spot Specific Weather Warning
Variable Speed Limits
Work Zone Alerts
Truck Restrictions

Provider Service Identifiers (PSIDs) & SCMS

- PSID values are included in the security certificates generated by the SCMS
- PSID values indicate which applications a message is authorized to support
- PSIDs are described in IEEE1609 standards

Applications by Connected Vehicle Test Bed

ICF/Wyoming
Work Zone Warnings
Spot Weather Impact Warning
Situational Awareness
Freight-Specific Dynamic Travel Planning
Automatic Alerts for Emergency Responders
CV-enabled Weather-Responsive Variable Speed Limits
Road Weather Advisories for Trucks and Vehicles
Truck Parking Availability for Freight Carriers

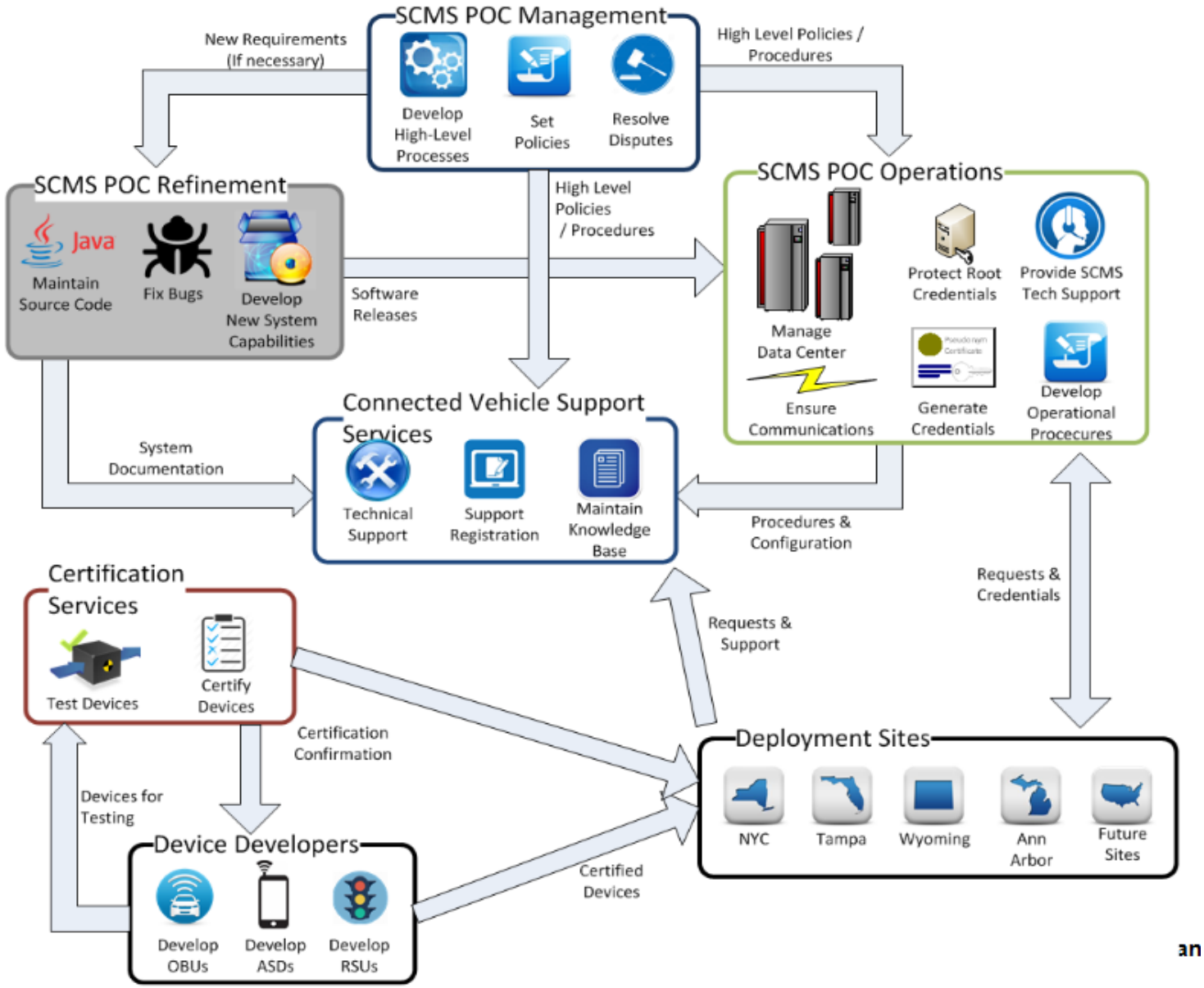
Tampa (THEA)
Curve Speed Warning
Pedestrian in Signalized Crosswalk Warning (Transit)
Emergency Electronic Brake Lights (EEBL)
Forward Collision Warning (FCW)
Intersection Movement Assist (IMA)
Vehicle Turning Right in Front of Bus Warning (Transit)
Intelligent Traffic Signal System (I-SIG)
Mobile Accessible Pedestrian Signal System (PED-SIG)
Transit Signal Priority (TSP)
Probe-enabled Traffic Monitoring

New York City (NYC)
Curve Speed Warning
Pedestrian in Signalized Crosswalk Warning (Transit)
Red Light Violation Warning
Reduced Speed/Work Zone Warning
Blind Spot Warning (BSW) *
Emergency Electronic Brake Lights (EEBL) *
Forward Crash Warning *
Intersection Movement Assist (IMA) *
Lane Change Assist (LCA) *
Stationary Vehicle Ahead (SVA) *
Vehicle Turning Right in Front of Bus Warning (Transit)
Advanced Traveler Information System
Emergency Communications and Evacuation (EVAC)
Freight-Specific Dynamic Travel Planning and Performance Measurement (F-ATIS)
Intelligent Traffic Signal System (I-SIG)
Mobile Accessible Pedestrian Signal System (PED-SIG)
Eco-Speed Harmonization

- **Deployment of applications is dependent upon Final ConOps and funding*

What do SCMS Management and Operations Look Like?

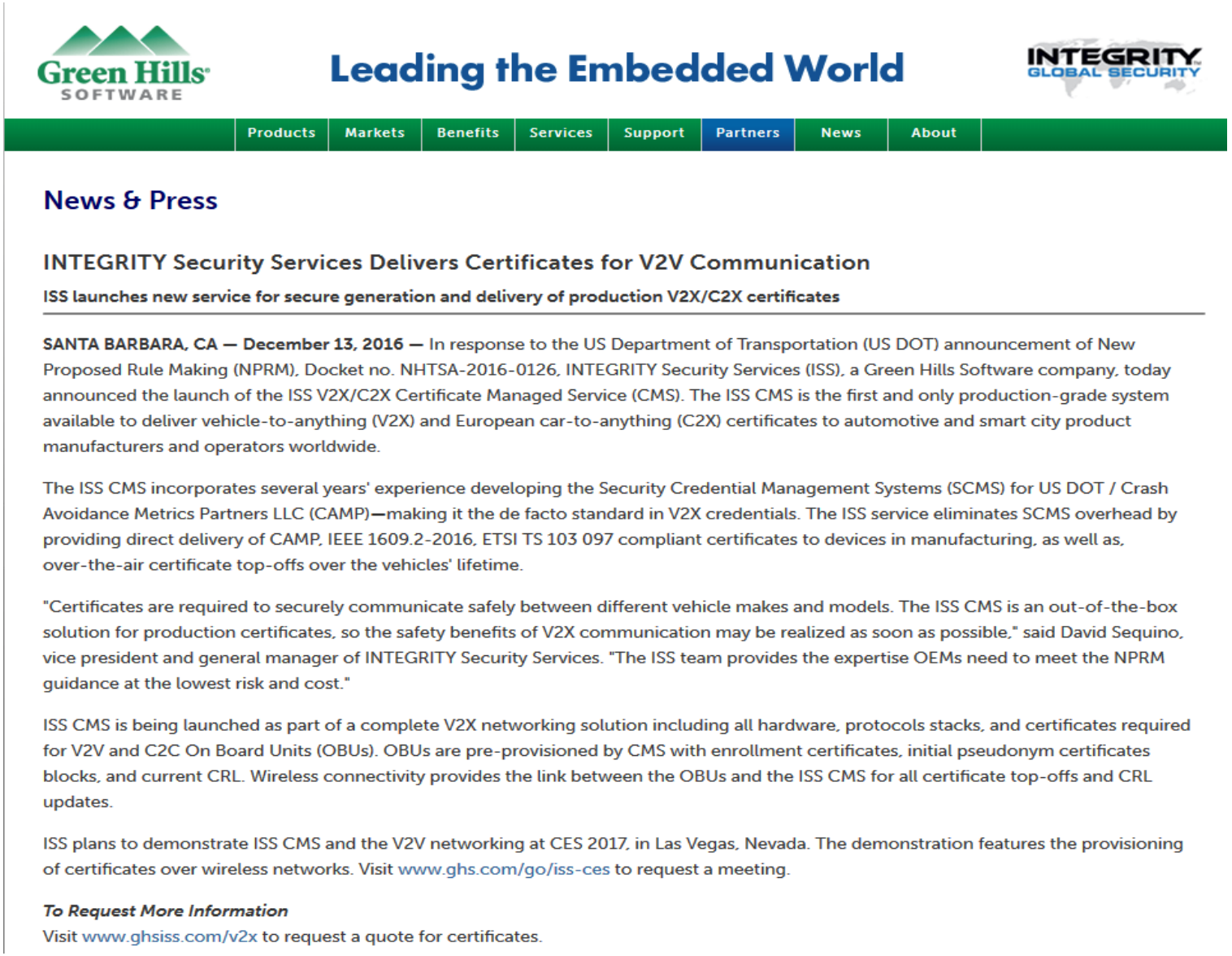
https://www.its.dot.gov/pilots/pdf/TechAssistWebinar_Template_SCMSIIv4.pdf



If they build it, will they come?

Green Hills Software Integrity Security Services (ISS)

http://www.ghs.com/go/iss-ces



Green Hills SOFTWARE

Leading the Embedded World

INTEGRITY GLOBAL SECURITY

Products | Markets | Benefits | Services | Support | Partners | News | About

News & Press

INTEGRITY Security Services Delivers Certificates for V2V Communication

ISS launches new service for secure generation and delivery of production V2X/C2X certificates

SANTA BARBARA, CA — December 13, 2016 — In response to the US Department of Transportation (US DOT) announcement of New Proposed Rule Making (NPRM), Docket no. NHTSA-2016-0126, INTEGRITY Security Services (ISS), a Green Hills Software company, today announced the launch of the ISS V2X/C2X Certificate Managed Service (CMS). The ISS CMS is the first and only production-grade system available to deliver vehicle-to-anything (V2X) and European car-to-anything (C2X) certificates to automotive and smart city product manufacturers and operators worldwide.

The ISS CMS incorporates several years' experience developing the Security Credential Management Systems (SCMS) for US DOT / Crash Avoidance Metrics Partners LLC (CAMP)—making it the de facto standard in V2X credentials. The ISS service eliminates SCMS overhead by providing direct delivery of CAMP, IEEE 1609.2-2016, ETSI TS 103 097 compliant certificates to devices in manufacturing, as well as, over-the-air certificate top-offs over the vehicles' lifetime.

"Certificates are required to securely communicate safely between different vehicle makes and models. The ISS CMS is an out-of-the-box solution for production certificates, so the safety benefits of V2X communication may be realized as soon as possible," said David Sequino, vice president and general manager of INTEGRITY Security Services. "The ISS team provides the expertise OEMs need to meet the NPRM guidance at the lowest risk and cost."

ISS CMS is being launched as part of a complete V2X networking solution including all hardware, protocols stacks, and certificates required for V2V and C2C On Board Units (OBUs). OBUs are pre-provisioned by CMS with enrollment certificates, initial pseudonym certificates blocks, and current CRL. Wireless connectivity provides the link between the OBUs and the ISS CMS for all certificate top-offs and CRL updates.

ISS plans to demonstrate ISS CMS and the V2V networking at CES 2017, in Las Vegas, Nevada. The demonstration features the provisioning of certificates over wireless networks. Visit www.ghs.com/go/iss-ces to request a meeting.

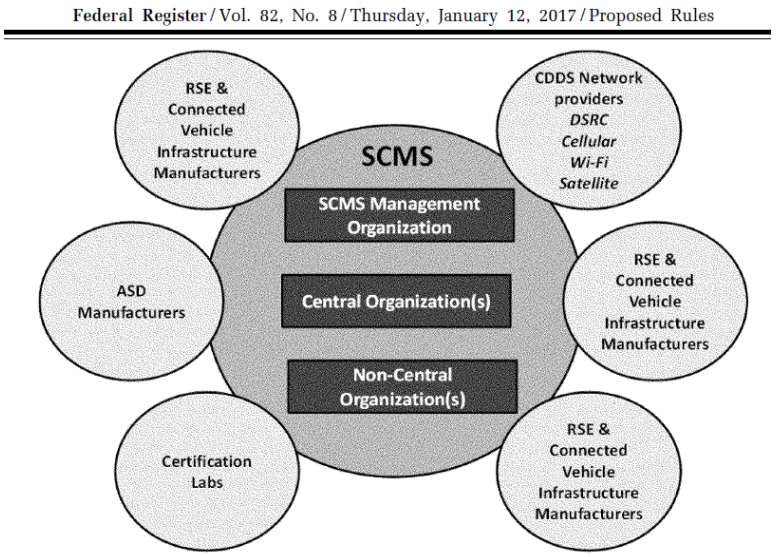
To Request More Information

Visit www.ghsiss.com/v2x to request a quote for certificates.

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

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

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




SecurityFeeds LLC
Information Assurance for the Enterprise Network
Tim Weil - CISSP/CCSP, CISA, PMP
Principal
PO Box 18385
Denver, CO 80218
Phone: 301.452.3641 (m)
Fax: 240.337.1305
Email: tweil@securityfeeds.com
Website: http://securityfeeds.com

Thank you for joining us!

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

References Used in This Presentation

- T.Weil, VPKI Hits the Highway: Security Communication for the Connected Vehicle Program, IT Professional Magazine, Volume 19, Issue 1, January 2017, pg 59-63
- IEEE 1609 Standards for Wireless Access in Vehicular Environments (WAVE), online available (fee based) - https://standards.ieee.org/develop/wg/1609_WG.html
- 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
- Harding, J., Powell, G., R., Yoon, R., Fikentscher, J., Doyle, C., Sade, D., Lukuc, M., Simons, J., & Wang, J. (2014, August). *Vehicle-to-vehicle communications: Readiness of V2V technology for application.* (Report No. DOT HS 812 014). Washington, DC: National Highway Traffic Safety Administration, online available - https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/readiness-of-v2v-technology-for-application-812014.pdf
- W. Whyte et al., "A Security Credential Management System for V2V Communications," Proc. IEEE Vehicular Networking Conf. (VNC), 2013; http://ieeexplore.ieee.org/document/6737583
- Security Credential Management System (SCMS) Connected Vehicle Pilot Documentation, Crash Avoidance Metrics Partnership (CAMP) Wiki - https://wiki.campllc.org/display/SCP
- US Department of Transportation, Intelligent Transportation Systems Joint Program Office, Connected Vehicle Pilot Deployment Program, online available - https://www.its.dot.gov/pilots/index.htm

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

WAVE Advertisement – Communication with a service (1609.0)

A WAVE service is supported by time and frequency (channel) resources allocated at some set of participating devices within communication range, in support of one or more applications. The service is initiated at the request of the application at one device (the provider), and announced on the CCH.

Applications offering services to potential user applications are announced on the air interface via an advertisement inside a WAVE management frame.

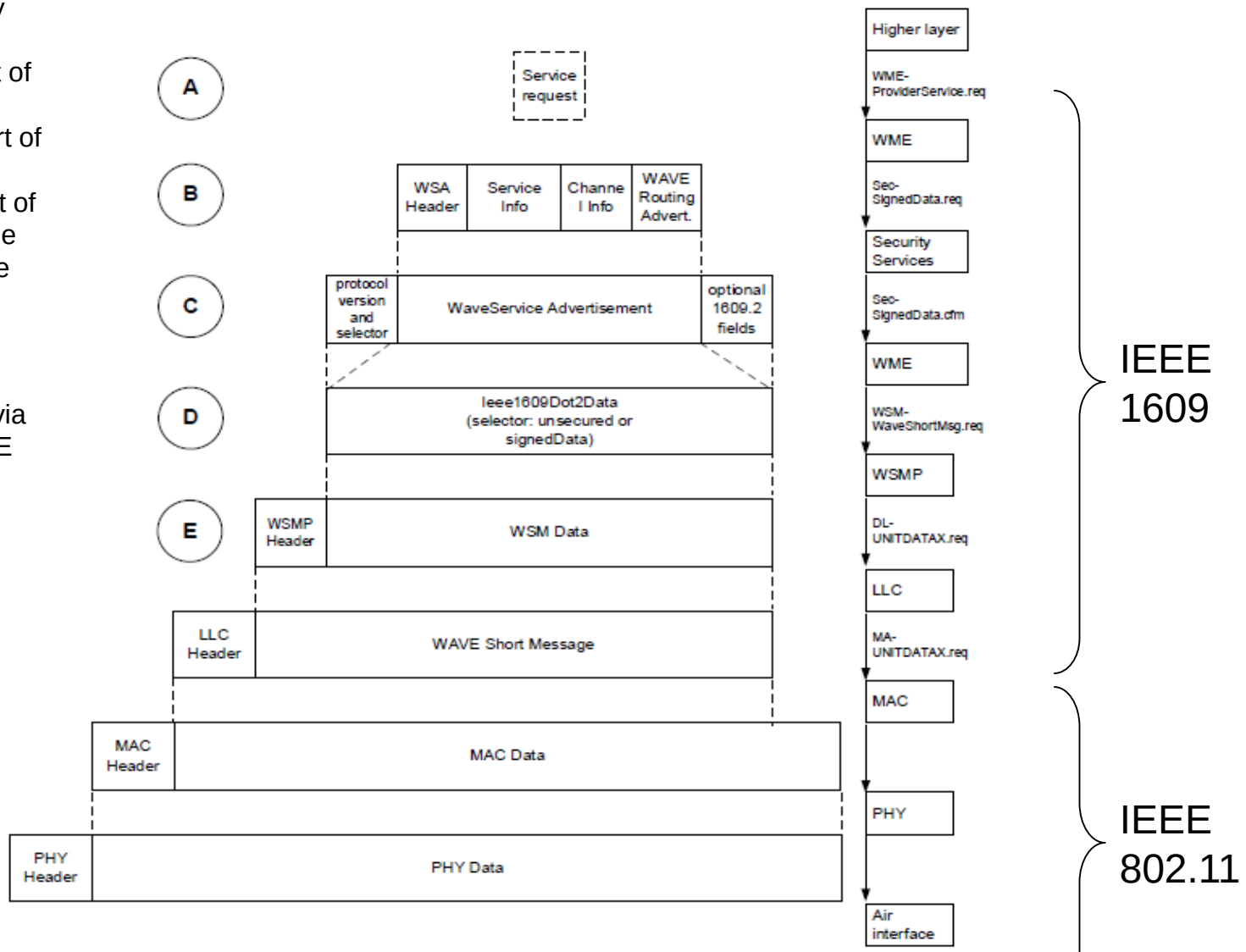


Figure 13— Building the WSA

WAVE Networking Services – WAVE Service Advertisement (new format)

Streamlines message. Makes more consistent use of WAVE Element IDs and Extension (optional) fields.