CAMP

Vehicle Safety Communications 3

Mercedes-Benz Research & Development North America, Inc.

GM

TOYOTA

HONDA Honda R&D Americas

Ford

NISSAN

HYUNDAI·KIA MOTORS Hyundai·Kia America Technical Center, Inc.

VOLKSWAGEN GROUP OF AMERICA

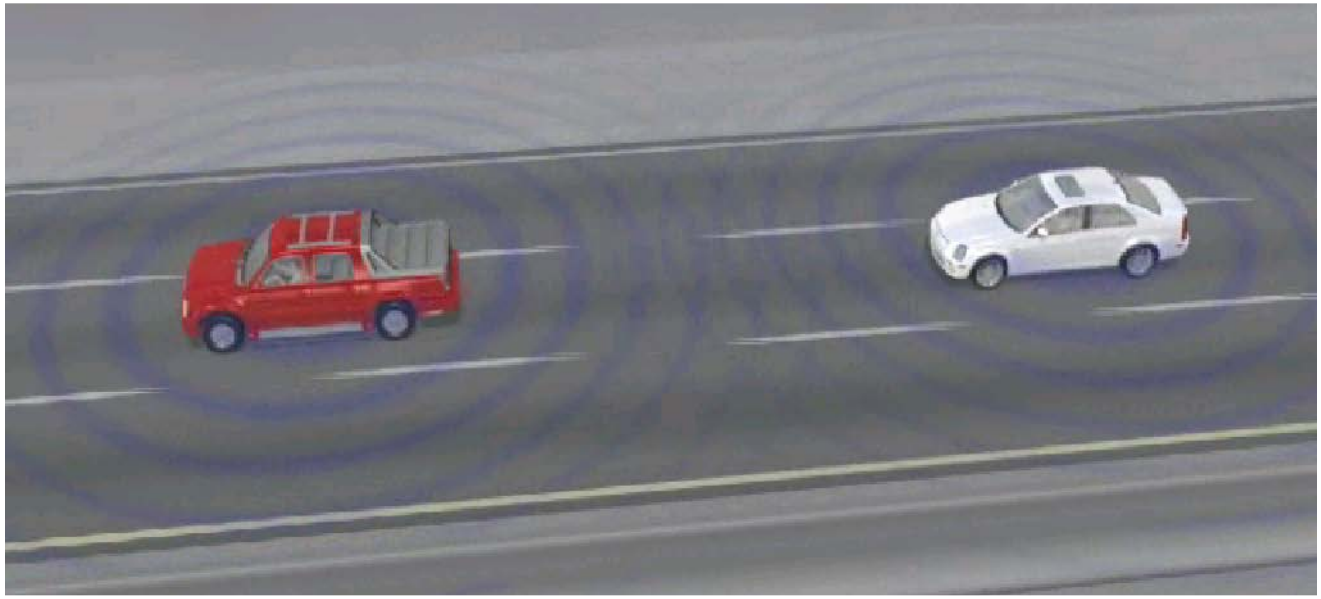
Intelligent Transportation Systems

V2V Communications Security Project Update

ITS Advisory Committee Update

Mike Shulman, Ford / CAMP VSC3

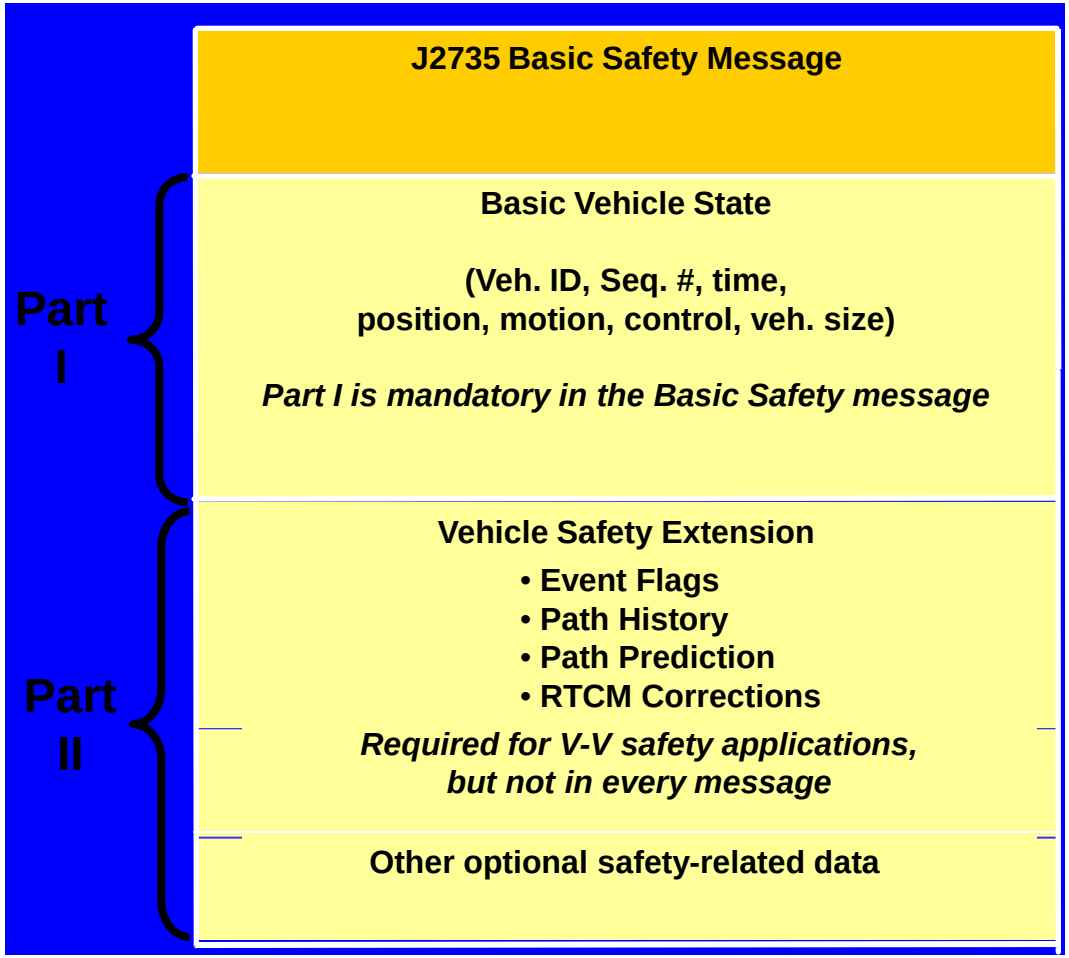
Vehicle Communications + GPS: A New Safety Sensor



- Offers new features not possible with existing obstacle detection-based driver assistance systems
- Enhances existing obstacle detection-based driver assistance systems
- However, only works when the vehicles in conflict are equipped

Interoperable Communication: SAE J2735 Message Set

- Periodic safety message broadcast (10 times per second)
- Event-driven safety message broadcast (immediate on event occurrence)



Why we need security

- The receiver of a message is not able to determine, without additional mechanisms, whether

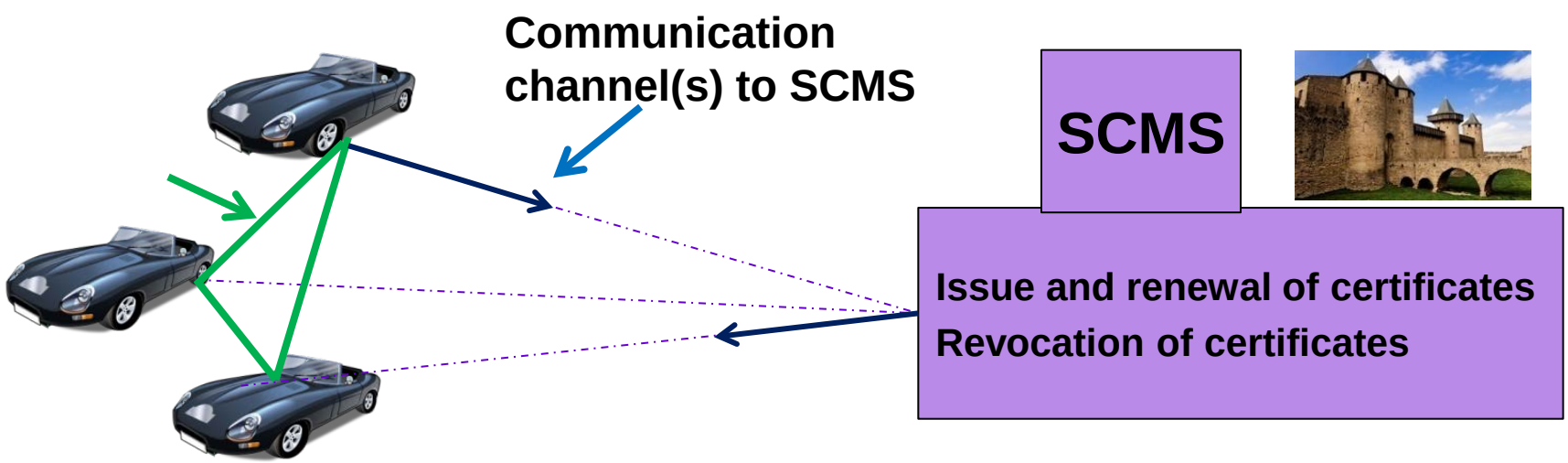
  1. a message originates from a trustworthy and legitimate device, and whether

  2. the message was modified between sender and receiver.

What is a PKI?

Vehicle A
Public Key
Validity Date
CA Signature
Vehicle A
1. Issue certificate and private key
Vehicle A
Public Key
Validity Date
CA Signature
Message
Signature
2. Sign message (using private key) and send message, signature & certificate
Security Credential Management System
3. Verify certificate (using CA's public key) and verify message (using certificate's public key)

V2V Security Communications



- **Communication Channel from Vehicles to SCMS**
  - **Send misbehavior reports (messages that led to warnings, messages flagged by local misbehavior detection and casual reports**

- **Communication Channel from SCMS to Vehicles**
  - **Issue New Certificates**
  - **Update Vehicles with Certificate Revocation List**

Initial Deployment Model

Security Credential Management System (SCMS)	On-Board Elements (OBE)	Communications between OBE & SCMS

• SCMS structure with:
  • Certificate Authority (CA)
  • Registration Authority (RA)
  • 2 Linkage Authorities (LAs)
  • Preliminary Misbehavior Authority, etc.
• Capability to generate and provide certificates valid for use for three (3) years from initial deployment
  • Option 1: re-useable, non-overlapping, 5 minute certificates valid for 3 years
  • Option 2: re-useable, overlapping certificates valid for 1 week for each week for 3 years
	• OBE requirements:
	  • FIPS 140 Level 2 or equivalent security processor
	  • Encrypted storage of certificates on-board
	• Capability to:
	  • Option 1: initially load 3000 non-overlapping certificates, re-use for 3 years, 5 minute duration each use – 300kB certificate storage
	  • Option 2: initially load 7 - 40 overlapping certificates per week, sufficient for 3 years (~6000), re-use during week if necessary, change at OEM discretion – max. 600kB certificate storage
		• Communications required after 3 years for:
		  • New certificate request
		  • Certificate Revocation List
		  • Misbehavior reporting
		• Also possible more frequently, if supported by opt-in connections

• **SCMS risk mitigation techniques are well-known from similar implementations**	• **OBE requirements are technically feasible** • **Security portion < 20% of total OBE cost**	• **Connectivity not required for the first 3 years**

Full Deployment Model

Security Credential Management System (SCMS)	On-Board Elements (OBE)	Communications between OBE & SCMS

• SCMS structure with:
  • Certificate Authority (CA)
  • Registration Authority (RA)
  • 2 Linkage Authorities (LAs)
  • Misbehavior Authority, etc.
• Capability to generate and provide certificates valid for use for <3 years from certificate request:
  • Option 1: re-useable, non-overlapping, 5 minute certificates valid for <3 years
  • Option 2: re-useable, overlapping certificates valid for 1 week for each week for <3 years
	• OBE requirements:
	  • FIPS 140 Level 2 or equivalent security processor
	  • Encrypted storage of certificates on-board
	• Capability to:
	  • Option 1: request and load 3000 non-overlapping certificates, re-use for < 3 years, 5 minute duration each use – 300kB certificate storage
	  • Option 2: request and load 7 - 80 overlapping certificates per week, sufficient for <3 years (~6000), re-use during week if necessary, change at OEM discretion – max. 600kB certificate storage
		• Communications required for:
		  • New certificate request
		  • Certificate Revocation List
		  • Misbehavior reports
		• Connectivity required:
		  • Likely more frequently than every 3 years
		  • Depends upon:
		  • number of attackers
		  • magnitude of the attacks
		  • Difficult to estimate without actual operational experience

• **Graceful evolution from initial deployment model**	• **OBE full deployment requirements supported by initial deployment vehicles**	• **Connectivity options, both default and opt-in, must expand by full deployment**

Connectivity Requirements
For Different Penetration Levels and Attack Rates

Attack Rate → Penetration Levels ↓	Benign Case: up to 100 devices/year cert extraction	Severe Case: up to 1000 devices/year cert extraction	Extreme Case: up to 10,000 devices/year cert extraction
1%	3 years	3 years	1 year
10%	3 years	3 years	4 months
50%	3 years	1 year	6 weeks
100%	3 years	6 months	3 weeks

Modeling target is less than one false alarm per week per equipped vehicle from intentional attacks. This may change as system matures and there is a better understanding about user acceptance of false alarms.

Summary of Highest Risk Levels for Privacy and Tracking Attacks

Type of Attack	Initial	Full	Mitigation	After Mitigation
Tracking	* - US DOT technical team rankings are lower			
Tracking Vehicles using 1-Day Certificates by Funded Private Organizations	Medium to High	Medium to High	Use shorter duration for certificates, to make this attack more difficult, such as 5-minute certificates which are now assumed for initial and full CAMP models	Medium
Find and Track Vehicles by Government Organizations Assumptions: certificates are linked to VIN, a subpoena/warrant is not required & full RSE network deployed	Low	High*	Public SCMS: Do not link certificates to VIN and/or require legal process Private SCMS: Require legal process	Medium
Law Enforcement				
Traffic Law Enforcement. Assumptions: using BSM information is advantageous as compared to current automated traffic enforcement systems and data would hold up in a court of law*	High*	High*	Under these assumptions, a technical mitigation for this risk has not yet been identified. Further technical and policy study is required.	TBD

Summary

1. The OBE requirements are technically feasible, but automotive hardware for the security components is not yet available. Suppliers estimate that the cost for the security portion is less than 20% of the total cost for the OBE.

2. With secure hardware, the team believes that connectivity is not required for the first three years. After that, more frequent connectivity is likely to be required but is increasingly difficult to estimate, since it depends upon the number of attackers and the magnitude of the attacks.

3. Mitigations for SCMS technical risks are well-understood from similar implementations. SCMS costs, funding and organization are being examined in a follow-on study.

4. Privacy and tracking attacks can most likely be addressed by using short-duration certificates. Having the appropriate policies and procedures in place will help prevent the perception that the system will be used for “big brother” tracking. Concerns about the use of this system for traffic enforcement need further technical and policy study.

Next Step: Analyze alternative connectivity options

Next Step: Analyze SCMS architectures and potential OEM roles

Assessment of Wireless Technology for Vehicle/Device Communication with Security Credential Management System (SCMS)

Main Discussion Topics

- Long-term technical stability
- Ability to support alternatives to user-paid subscriptions
- Technical capabilities to support privacy goals

Discussions with Industry Participants

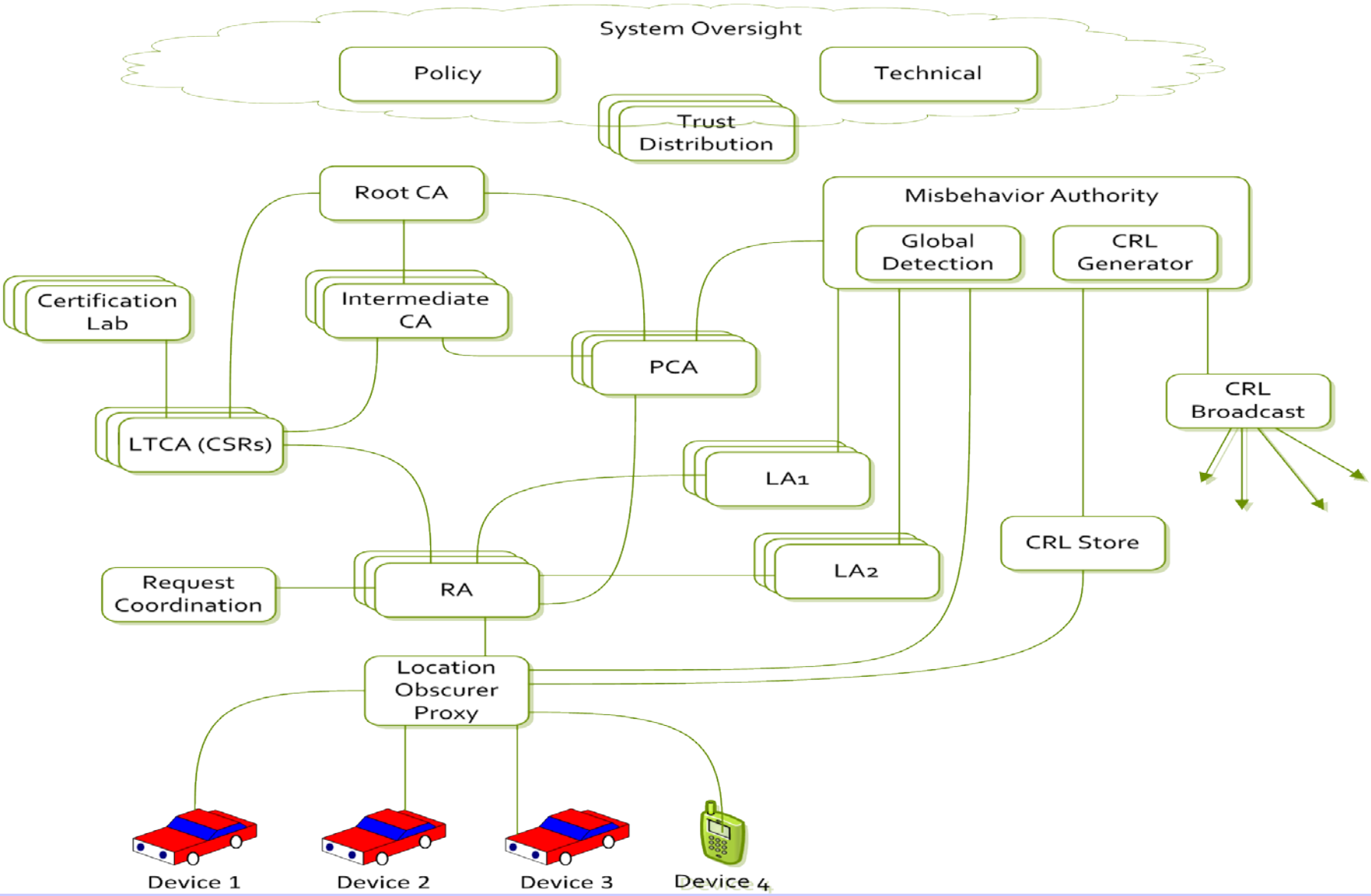
- Cellular Carriers
- Wireless Device Manufacturers
- Wireless Technology Developers
- Satellite Radio Operators
- IEEE 802.22 Working Group

Assessment of Wireless Technology for Vehicle/Device Communication with Security Credential Management System (SCMS)

Preliminary Conclusions

- Long Term Evolution (LTE) is integrating previously diverse technology developments and is expected to continue on an evolutionary development path within a 5-10 year horizon
- Cellular network management systems are becoming more flexible in terms of support for non-traditional billing arrangements
- Satellite Radio may offer better-than-expected capabilities for Certificate Revocation List (CRL) distribution to vehicles

SCMS Design


System Oversight
Policy
Technical
Trust Distribution
Root CA
Misbehavior Authority
Global Detection
CRL Generator
Certification Lab
Intermediate CA
PCA
CRL Broadcast
LTCA (CSRs)
LA1
CRL Store
LA2
Request Coordination
RA
Location Obscurer Proxy
Device 1
Device 2
Device 3
Device 4