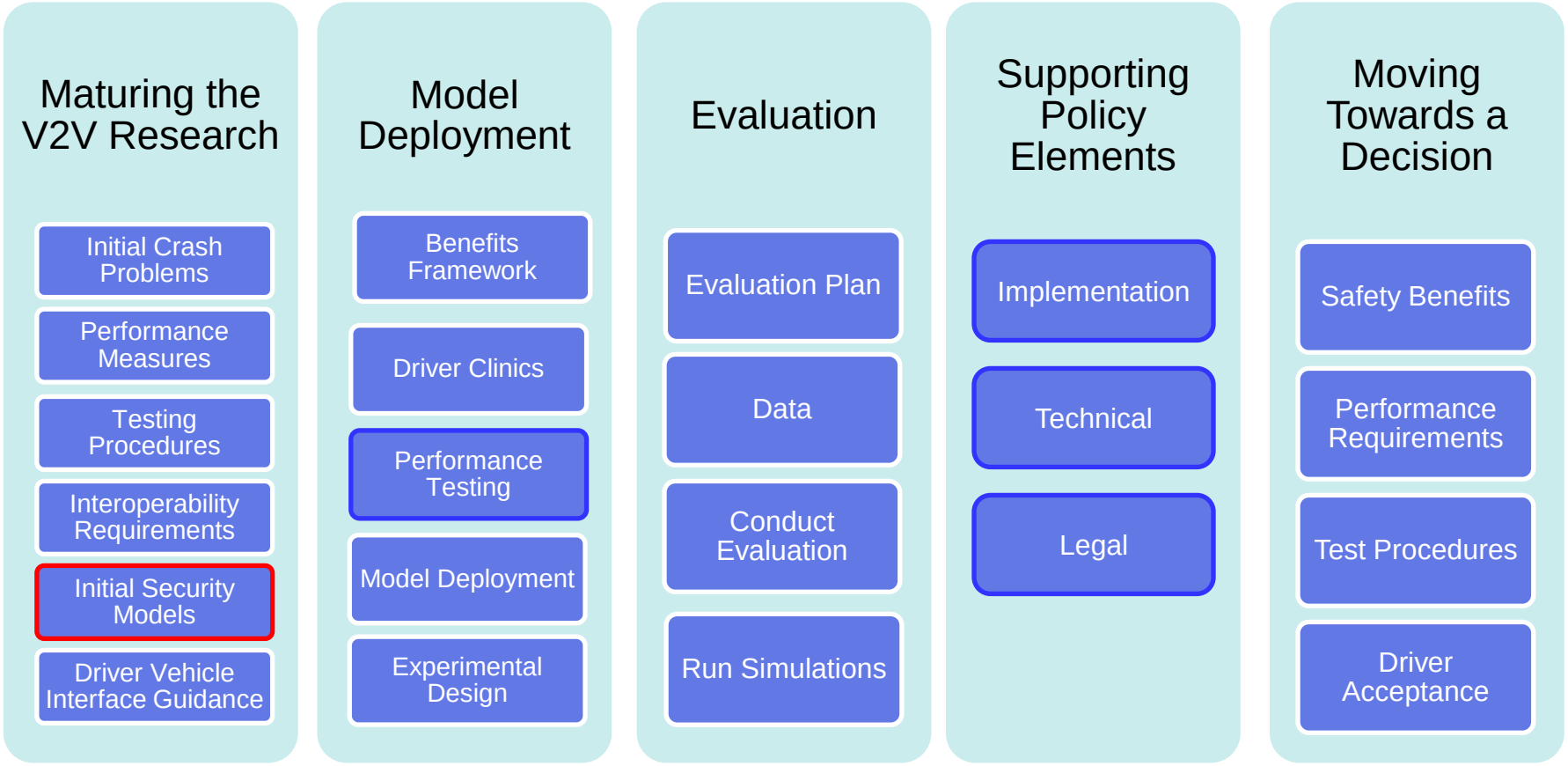
V2V Communications Security Project Update

USDOT ITS Connected Vehicle Workshop

Mike Shulman, Ford / CAMP VSC3

V2V Safety Framework



Key Messages

A team of OEMs, US DOT personnel, automotive suppliers and security experts have examined the technical feasibility and risks associated with a security system for V2V warning-only applications, under a certain set of assumptions.

The proposed security model developed needs to be built and tested to validate the conclusions from this study.

Key Messages

A team of OEMs, US DOT personnel, automotive suppliers and security experts have examined the technical feasibility and risks associated with a security system for V2V warning-only applications, under a certain set of assumptions. The proposed security model developed needs to be built and tested to validate the conclusions from this study.

1. Technical solutions for the initial and full security deployment models have been identified that the DOT and the OEMs believe are feasible.

Key Messages

A team of OEMs, US DOT personnel, automotive suppliers and security experts have examined the technical feasibility and risks associated with a security system for V2V warning-only applications, under a certain set of assumptions. The proposed security model developed needs to be built and tested to validate the conclusions from this study.

1. Technical solutions for the initial and full security deployment models have been identified that the DOT and the OEMs believe are feasible..

2. The on-board system will require additional special hardware for security, which is technically feasible and is not expected to considerably increase the cost.

Key Messages

A team of OEMs, US DOT personnel, automotive suppliers and security experts have examined the technical feasibility and risks associated with a security system for V2V warning-only applications, under a certain set of assumptions. The proposed security model developed needs to be built and tested to validate the conclusions from this study.

1. Technical solutions for the initial and full security deployment models have been identified that the DOT and the OEMs believe are feasible..

2. The on-board system will require additional special hardware for security, which is technically feasible and is not expected to considerably increase the cost.

3. The team believes that connectivity will not be required for the first three years. After that, more frequent connectivity is likely to be required, but is increasingly difficult to estimate. Connectivity options are being examined in a follow-on study.

Key Messages

A team of OEMs, US DOT personnel, automotive suppliers and security experts have examined the technical feasibility and risks associated with a security system for V2V warning-only applications, under a certain set of assumptions. The proposed security model developed needs to be built and tested to validate the conclusions from this study.

1. Technical solutions for the initial and full security deployment models have been identified that the DOT and the OEMs believe are feasible..

2. The on-board system will require additional special hardware for security, which is technically feasible and is not expected to considerably increase the cost.

3. The team believes that connectivity will not be required for the first three years. After that, more frequent connectivity is likely to be required, but is increasingly difficult to estimate. Connectivity options are being examined in a follow-on study.

4. SCMS (Security Certificate Management System) technical risks are well-understood from implementations of similar systems, although the V2V PKI is considerably larger than any previous system. SCMS costs, funding and organization are being examined in a follow-on study.

Key Messages

A team of OEMs, US DOT personnel, automotive suppliers and security experts have examined the technical feasibility and risks associated with a security system for V2V warning-only applications, under a certain set of assumptions. The proposed security model developed needs to be built and tested to validate the conclusions from this study.

1. Technical solutions for the initial and full security deployment models have been identified that DOT and the OEMs believe are feasible..

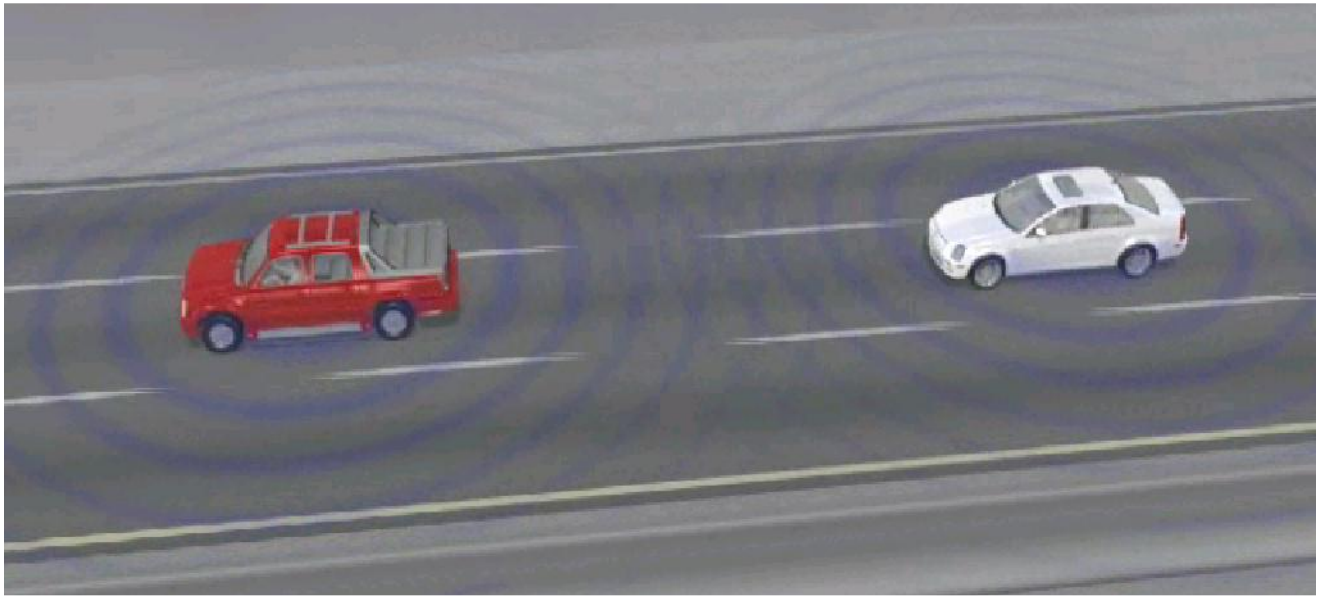
2. The on-board system will require additional special hardware for security, which is technically feasible and is not expected to considerably increase the cost.

3. The team believes that connectivity will not be required for the first three years. After that, more frequent connectivity is likely to be required, but is increasingly difficult to estimate. Connectivity options will be examined in a follow-on study.

4. SCMS (Security Certificate Management System) technical risks are well-understood from implementations of similar systems, although the V2V PKI is considerably larger than any previous system. SCMS costs, funding and organization are being examined in a follow-on study.

5. OEMs believe that privacy and tracking risks will likely require a combination of technical and policy solutions.

Vehicle Communications + GPS: A New Safety Sensor



- Lower cost enables deployment to all market segments, not just luxury
- Offers new features not possible with existing obstacle detection-based driver assistance systems
- Enhances existing obstacle detection-based driver assistance systems

Opportunity for Safer Driving

- **Greater situational awareness**

  Your vehicle can “see” nearby vehicles

Reduce or even eliminate crashes thru:

Driver Advisories

Driver Warnings

Adobe Acrobat Document

V2V systems have the potential to address 81% of light vehicle crash scenarios involving unimpaired drivers

Safety Applications *vs.* Crash Scenarios Mapping

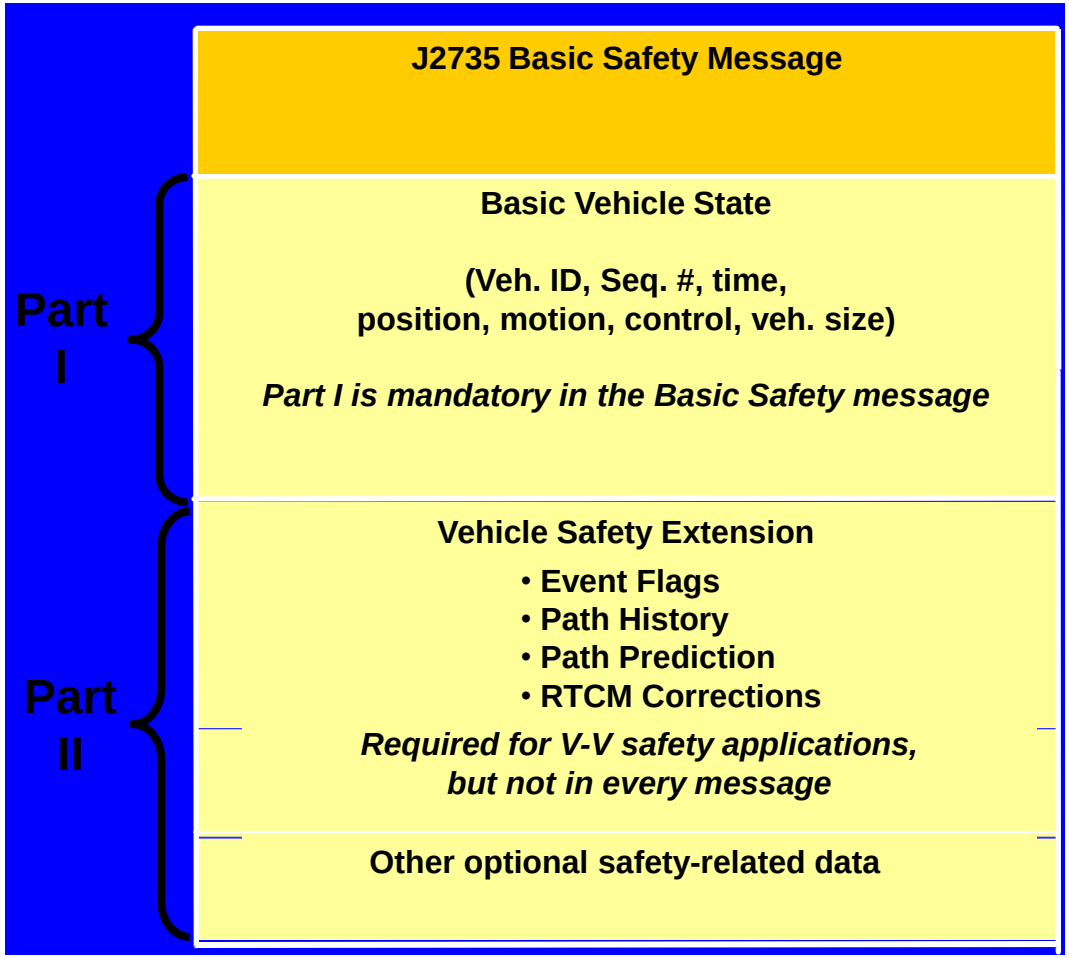
	V2V Safety Applications → / Crash Scenarios ↓	EEBL	FCW	BSW	LCW	DNPW	IMA	CLW
1	Lead Vehicle Stopped		✓					
2	Control Loss without Prior Vehicle Action							✓
3	Vehicle(s) Turning at Non-Signalized Junctions						✓	
4	Straight Crossing Paths at Non-Signalized Junctions						✓	
5	Lead Vehicle Decelerating	✓	✓					
6	Vehicle(s) Not Making a Maneuver – Opposite Direction					✓		
7	Vehicle(s) Changing Lanes – Same Direction			✓	✓			
8	LTAP/OD at Non-Signalized Junctions						✓	

Note: Crash Scenario reference: "VSC-A Applications_NHTSA-CAMP Comparison v2" document, USDOT, May 2 2007. Selected based on 2004 General Estimates System (GES) data and Top Composite Ranking (High Freq., High Cost and High Functional Years lost).

EEBL: Emergency Electronic Brake Lights
FCW: Forward Collision Warning
BSW: Blind Spot Warning
LCW: Lane Change Warning
DNPW: Do Not Pass Warning
IMA: Intersection Movement Assist
CLW: Control Loss Warning

Interoperable Communication: SAE J2735 Message Set

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



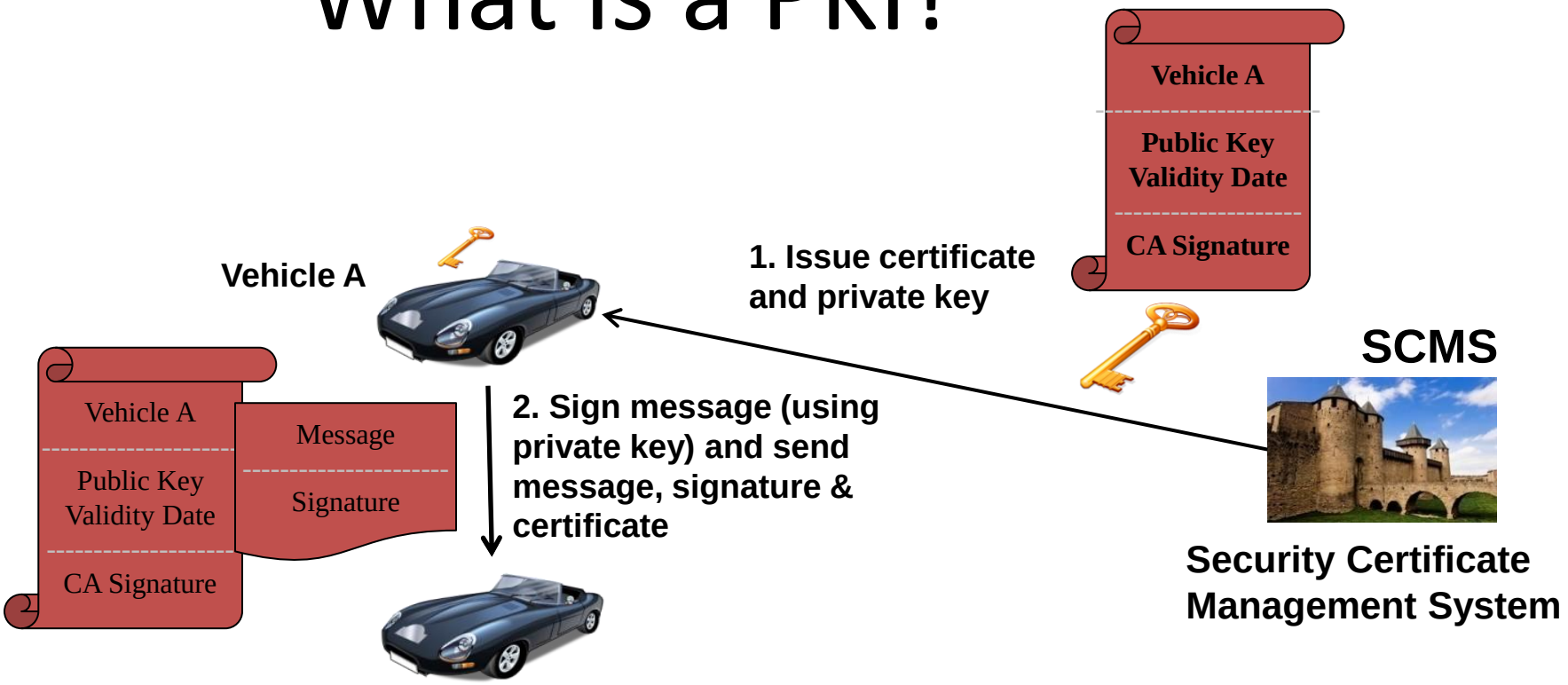
Why we need security

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

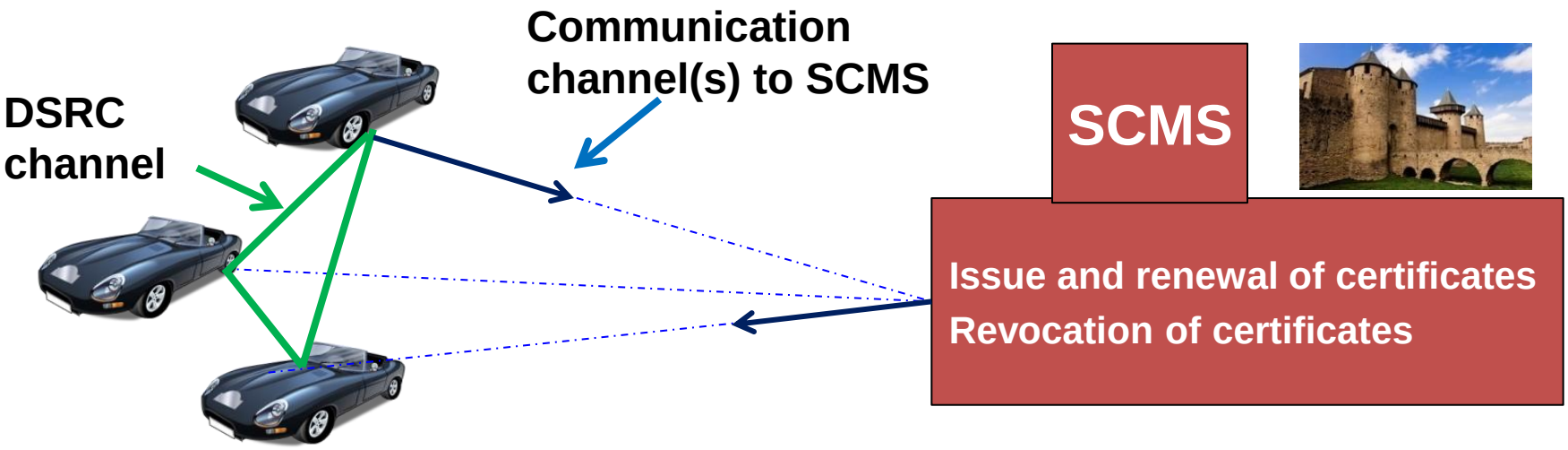
  1. a message originates from a trustworthy and legitimate device, and whether

  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
SCMS
Vehicle A
Public Key
Validity Date
CA Signature
Message
Signature
2. Sign message (using
private key) and send
message, signature &
certificate
Security Certificate
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**

Assumptions and Goals

- The system being considered is for V2V warning-only applications.

Assumptions and Goals

- The system being considered is for V2V warning-only applications.
- To the extent possible, the V2V crash avoidance security system design should support a balanced approach to safety, security and privacy

Assumptions and Goals

- The system being considered is for V2V warning-only applications.
- To the extent possible, the V2V crash avoidance security system design should support a balanced approach to safety, security and privacy

- A trust relationship must exist among all participants in the V2V crash avoidance security system

Assumptions and Goals

- The system being considered is for V2V warning-only applications.
- To the extent possible, the V2V crash avoidance security system design should support a balanced approach to safety, security and privacy
- A trust relationship must exist among all participants in the V2V crash avoidance security system

- The V2V safety system must be interoperable between vehicles from different manufacturers and other devices, throughout all geographic regions of the US

Assumptions and Goals

- The system being considered is for V2V warning-only applications.
- To the extent possible, the V2V crash avoidance security system design should support a balanced approach to safety, security and privacy
- A trust relationship must exist among all participants in the V2V crash avoidance security system
- The V2V safety system must be interoperable between vehicles from different manufacturers and other devices, throughout all geographic regions of the US

- No information should be available in mandatory vehicle transmissions to identify the driver or other occupants of the vehicle

Assumptions and Goals

- The system being considered is for V2V warning-only applications.
- To the extent possible, the V2V crash avoidance security system design should support a balanced approach to safety, security and privacy
- A trust relationship must exist among all participants in the V2V crash avoidance security system
- The V2V safety system must be interoperable between vehicles from different manufacturers and other devices, throughout all geographic regions of the US
- No information should be available in mandatory vehicle transmissions to identify the driver or other occupants of the vehicle

- User acceptance is important for the V2V crash avoidance system in order to realize the potential safety benefits

Assumptions and Goals

- The system being considered is for V2V warning-only applications.
- To the extent possible, the V2V crash avoidance security system design should support a balanced approach to safety, security and privacy
- A trust relationship must exist among all participants in the V2V crash avoidance security system
- The V2V safety system must be interoperable between vehicles from different manufacturers and other devices, throughout all geographic regions of the US
- No information should be available in mandatory vehicle transmissions to identify the driver or other occupants of the vehicle
- User acceptance is important for the V2V crash avoidance system in order to realize the potential safety benefits

- The system should be designed so that a vehicle is not able to be tracked, in order to gain user acceptance

Assumptions and Goals

- The system being considered is for V2V warning-only applications.
- To the extent possible, the V2V crash avoidance security system design should support a balanced approach to safety, security and privacy
- A trust relationship must exist among all participants in the V2V crash avoidance security system
- The V2V safety system must be interoperable between vehicles from different manufacturers and other devices, throughout all geographic regions of the US
- No information should be available in mandatory vehicle transmissions to identify the driver or other occupants of the vehicle
- User acceptance is important for the V2V crash avoidance system in order to realize the potential safety benefits
- The system should be designed so that a vehicle is not able to be tracked in order to gain user acceptance

- DSRC and/or other communications technologies may be used to provide communications between vehicles and off-board security functions, without any subscription fees for mandatory services

Assumptions and Goals

- The system being considered is for V2V warning-only applications.
- To the extent possible, the V2V crash avoidance security system design should support a balanced approach to safety, security and privacy
- A trust relationship must exist among all participants in the V2V crash avoidance security system
- The V2V safety system must be interoperable between vehicles from different manufacturers and other devices, throughout all geographic regions of the US
- No information should be available in mandatory vehicle transmissions to identify the driver or other occupants of the vehicle
- User acceptance is important for the V2V crash avoidance system in order to realize the potential safety benefits
- The system should be designed so that a vehicle is not able to be tracked in order to gain user acceptance
- DSRC and/or other communications technologies may be used to provide communications between vehicles and off-board security functions, without any subscription fees for mandatory services
- The system should be able to withstand attacks and effectively recover from the effects of attacks

Initial Deployment Model

Security Credential Management System (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

• SCMS risk mitigation techniques are well-known from similar implementations

On-Board Elements (OBE)

- 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

• OBE requirements are technically feasible
• Security portion < 20% of total OBE cost

Communications between OBE & SCMS

- Communications required after 3 years for:
  - New certificate request
  - Certificate Revocation List
  - Misbehavior reporting
- Also possible more frequently, if supported by opt-in connections

• Connectivity not required for the first 3 years

Full Deployment Model

Security Credential Management System (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

On-Board Elements (OBE)

- 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 between OBE & SCMS

- 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**

Risk Analysis

- Risk analysis was performed for various attack/attacker combinations and scenarios. Analysis done for 24 attacks, 11 attackers, and 3 scenarios, so overall a total of 792 risk assessments.

- Expert judgment and a NIST-like model were used to find likelihood and impact levels, and finally risk levels.
  - Risk levels are low, medium and high. A high risk level may, for example, mean frequent false warnings that may deter user acceptance.

- Assuming connectivity only every 3 years, Sybil attacks on the OBEs in the full deployment model showed up as high risk.
  - This risk can be mitigated by having more frequent connectivity. Connectivity requirements analysis results are on the next slide.

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 SCMS-Directed Attacks

Type of Attack	Initial	Full	Mitigation	After Mitigation
SCMS - Root CA Compromise	**High**	**High**	Policy (see below)	**High (Very Low Probability)**
SCMS - Intermediate CA Compromise	**High**	**High**	Policy (see below)	**High (Very Low Probability)**
Trust Management Compromise	**High**	**High**	Policy (see below)	**High (Very Low Probability)**

- The likelihood of each attack can be reduced by implementing appropriate policy, process and procedures, as is done with similar systems. This would include separation of duties and multiple layers of security.

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.

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.

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-up study.

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.

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