V2V: vehicles exchange BSMs with security credentials
Basic Safety Message Structure

Vehicle A  BSMs  Vehicle B

<table>
<thead>
<tr>
<th>Basic Safety Message</th>
<th>Message Content</th>
<th>Digital Signature</th>
<th>Pseudonym Certificate</th>
<th>Timestamp</th>
</tr>
</thead>
</table>
|                      | • Speed  
                      • Position  
                      • Heading  
                      • Acceleration | • 64 byte number created with the private key of an associated pseudonym certificate issued by CA | • Public key that corresponds to the private key used for signature  
• Validity interval  
• CA signature | • Date / Time in UTC |
V2X Public Key Infrastructure Overview

1. Device generates private, public key-pair

2. Device authenticates itself, and sends its public key to CA

3. CA verifies requesting device is authorized and generates a certificate

4. CA sends certificate back to device

Common entity in chain of trust

Other Vehicles & infrastructure

Infrastructure

Exchange Messages

Private Key

Device ID

Public Key

Validity Date

CA Signature

Certificate Authority

Vehicle

Public Key

2. Device authenticates itself, and sends its public key to CA

4. CA sends certificate back to device

3. CA verifies requesting device is authorized and generates a certificate
V2X SCMS Architecture
# SCMS POC Roadmap

## Security Credential Management System – Roadmap

<table>
<thead>
<tr>
<th>Year</th>
<th>2015</th>
<th>2016</th>
<th>2017</th>
<th>2018</th>
<th>2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCMS POC Refinement</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Develop Enrollment &amp; Provisioning Functionality</td>
<td></td>
<td></td>
<td>SCMS Poc System v1.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Integrate Global Misbehavior Detection Functionality</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Prototype Misbehavior Detection Methods</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCMS POC IT Operations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Deploy QA / Test Environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Deploy Operational Environment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SCMS POC Management</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Conduct POC Management Activities</td>
<td></td>
</tr>
</tbody>
</table>
SCMS Software Environments

Diagram showing the process flow of fixing bugs, finding root causes, deploying bug fixes, and releasing new system versions across different environments:

- Development Environment
  - Component Testing
  - Integration Testing
- QA/Test Environment
- Operational Environment
  - CV Pilot Operations

Certificate Authority Hierarchy

- QA and Operational Environments will have different roots
- However, CA hierarchy will look similar between the two environments

- For CV Pilots, there will be a dedicated ICA and PCA to supply security credential materials
- Other ICAs will be authorized as necessary to support early deployments of CV technology
## SCMS POC Certificate Types

<table>
<thead>
<tr>
<th>Issued To</th>
<th>Name</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>OBU / ASD</td>
<td>Enrollment</td>
<td>Initialize the OBU to allow communication with the SCMS</td>
</tr>
<tr>
<td>OBU / ASD</td>
<td>Pseudonym</td>
<td>Used to sign all BSMs generated by an OBU</td>
</tr>
<tr>
<td>OBU</td>
<td>Authorization</td>
<td>Used to identify public sector vehicles for specific apps</td>
</tr>
<tr>
<td>RSU</td>
<td>Enrollment</td>
<td>Initialize the RSU to allow communication with SCMS</td>
</tr>
<tr>
<td>RSU</td>
<td>Application</td>
<td>Used to sign application messages generated by RSU (TIM, SPaT, etc.)</td>
</tr>
</tbody>
</table>
EE Requirements and Specification

- Documentation is publicly available
  - Version 1.0 – Released in January 2016
  - Version 1.1 – Released in May 2016

- All use cases relevant to OBUs/RSUs are listed in the document

- Document contains links to ASN.1 code open to public on CAMP wiki:
General EE Requirements

1. Generate Public/Private Key Pairs
   - SCMS will not generate key-pairs for devices
   - Devices/DCM must generate keys for bootstrapping
   - Devices will need to generate future keys for provisioning

2. Secure Storage of Cryptographic Materials
   - Certificates and private keys need to be stored in secure, tamper evident module in the system
   - Minimum requirements are equivalent to FIPS 140 Level 2
   - Requirements available in 1.1 Release of Interface Documentation

3. Definition of Time
   - SCMS POC will utilize TAI as the time basis according to IEEE 1609.2
UC 2: Bootstrapping

- Manual process will be utilized for initial deployment
- Later versions of the system will implement an automated process

**CV Pilot Bootstrapping Process**

1. Create Bootstrap Request
2. Review Request
3. Verify Certification Results
4. Request Approved?
   - Yes
     - 5. Generate Initialization & Enrollment Data
     - 6. Create Bootstrap ZIP File & encrypt
   - No
     - 7. Decrypt & Unzip Bootstrap File
     - 8. Upload Bootstrap Data to Devices
     - 9. Request pseudonym certificates
At a high level, this use case can be divided into 5 steps as follows.

1. Check for policy updates
2. Request for Pseudonym Certificates
3. Pseudonym Certificate Generation
4. Download of Pseudonym Certificates
5. Generate subsequent batch of Pseudonym Certificates
Stay Connected

Visit our website for information on:
• Webinars
• Events
• Publications
• News

Twitter: @ITSJPODirector
Facebook: https://www.facebook.com/DOTRITA
Website: http://www.its.dot.gov

Kevin Gay, PMP
Chief – ITS Policy, Architecture and Knowledge Transfer
Kevin.Gay@dot.gov