Security and privacy for a connected vehicle environment

SCMS Overview
End Entity Requirements and Interfaces
Dean Therriault - GM/CAMP
Benedikt Brecht – VWGoA/CAMP
CAMP built/provides the SCMS “box” mentioned by Ariel! 😊
Sign messages & verify signature
Ensure privacy
Long-term certificate used in interactions with SCMS

Where does it come from?
How does the EE get it?
Pseudonym certificate batch
Misbehavior Detection
Penalty / device revocation

Device should no longer be trusted - MA revokes certificates via Certificate Revocation List (CRL)
SCMS PoC Environment

SCMS POC Governmental Management
- Operation Protocols
- Set Policies
- End Entity User Group

SCMS POC Development
- New Requirements (if necessary)
- New/Alternative Functions/Fixes
- Maintain Source Code
- Fix Bugs
- Develop New System Capabilities

Policies/Protocols/Basic Procedures
- Technical Procedures
- Software Releases

Connected Vehicle Support Services
- General Support
- Support Registration
- End User Interface

SCMS Technical Management
- Develop Technical Procedures
- Implement New Functions
- Support Incident Studies
- Establish Technical Operations
- Generate Credentials
- Provide SCMS Tech Support

SCMS Operation QA & Production
- Support System Evaluation

Certification Services
- End Entity Security Requirements
- Procedures, Configurations & Certificates

Deployment Sites
- NYC
- Tampa
- Wyoming
- Ann Arbor
- Future Sites

Device Suppliers
- Certified Devices
- Devices
- For Testing
- Develop OBUs
- Develop ASDs
- Develop RSUs

System Documentation

Certification Services
- Test Devices
- Certify Devices

End User & SCMS Technical Liaison

End User & SCMS Technical Liaison

SCMS POC USDOT Management & Policy Task Force

National Prototype Policy Development
- Analysis of PoC Policies
- Adapt & Additional Prototype Policies
- USDOT SCMS Policy Statement

SCMS Operation QA & Production
- Establish Technical Operations
- Generate Credentials
- Provide SCMS Tech Support

Policies & Organizational Protocols

SCMS PoC Governmental Management
- Operation Protocols
- Set Policies
- End Entity User Group
SCMS “Operations” - Environments

- **CAMP Dev Stage** (part of SoW)
- **QA Stage** (based on existing hardware – part of the SoW)
- **Production Stage** (part of the SoW)

**Process Flow:***
- Bug fixed
- Fix bug
- Root cause found
- Report bug
- Deploy bug-fix
- Deploy bug-fix
- Deploy bug-fix

- **Bug-fix component test**
- **Bug-fix integration / system test**
- **CV pilot use**
End Entity Basics

EE basics and interfaces
End Entity Basics

Enroll
Get Pseudonyms
Communicate
<Repeat>
Enroll

Enrollment is the EEs entry point to the SCMS

- Enrollment Certificate = long term (life of device)
  - Ticket for admission to SCMS
- Every EE must be provisioned with an Enrollment Certificate
  - part of bootstrap process
  - Expected to cover the lifetime of EE (OBE, RSE/U)
  - OEM specific/proprietary
- Enrollment environment governed by SCMS Manager policy

More OBE: [wiki.campllc.org/display/SCP/Step+2.2%3A+OBE+Enrollment](wiki.campllc.org/display/SCP/Step+2.2%3A+OBE+Enrollment)
More RSE: [wiki.campllc.org/display/SCP/Step+12.2%3A+RSE+Enrollment](wiki.campllc.org/display/SCP/Step+12.2%3A+RSE+Enrollment)
Manual Enrollment Process

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

### CV Pilot Bootstrapping Process

<table>
<thead>
<tr>
<th>Phase</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Create Bootstrap Request</td>
</tr>
<tr>
<td>2.</td>
<td>Review Request</td>
</tr>
<tr>
<td>3.</td>
<td>Verify Certification Results</td>
</tr>
<tr>
<td>4.</td>
<td>Request Approved?</td>
</tr>
<tr>
<td>5.</td>
<td>Generate Initialization &amp; Enrollment Data</td>
</tr>
<tr>
<td>6.</td>
<td>Create Bootstrap ZIP File &amp; encrypt</td>
</tr>
<tr>
<td>7.</td>
<td>Decrypt &amp; Unzip Bootstrap File</td>
</tr>
<tr>
<td>8.</td>
<td>Upload Bootstrap Data to Devices</td>
</tr>
<tr>
<td>9.</td>
<td>Request pseudonym certificates</td>
</tr>
</tbody>
</table>

- **No**
- **Yes**
DCM – Secure Environment

- ECA provides a one-time, long term enrollment certificate
- OEM can design and implement into existing mfg. processes
- No “interface” to the SCMS
Secure Environment for Enrollment

- A documented procedure for performing the enrollment process
- A physically secure location where the enrollment will take place
- One or more authorized devices (computers) for managing the enrollment process
- An activity log or recording of the enrollment operations that were performed
  - wiki.campllc.org/display/SCP/Secure+Environment+for+Device+Enrollment
Get Pseudonym certs

- Pseudonym certs are short lived
  - Used for BSM authentication and MB reporting
  - i-Period = 10140 minutes (1 week + 1 hour)
  - j-Value = 20 certs/i-Period (currently could change)
- EE-RA <---> PCA-RA

Requirements & process description:
wiki.campllc.org/display/SCP/Use+Case+3%3A+OBE+Pseudonym+Certificates+Provisioning
Request doc: wiki.campllc.org/display/SCP/RA+-+Request+Pseudonym+Certificate+Batch+Provisioning
Download doc: wiki.campllc.org/display/SCP/RA+-+Download+Pseudonym+Certificate+Batch
Additional:
- wiki.campllc.org/display/SCP/RA+-+Download+.info+file
- wiki.campllc.org/display/SCP/RA+-+Download+Local+Policy+File
- wiki.campllc.org/display/SCP/RA+-+Download+Local+Certificate+Chain+File
Get Application Cert

- Application certs are short lived
  - NO Pseudonymity constraints required
  - Validity period can vary (i-period)
  - One-to-one mapping of PSID and SSP to enrollment cert
  - 1 valid application certificate per application valid at a time
- EE-RA <---> PCA-RA

Requirements & process description:
wiki.campllc.org/display/SCP/Use+Case+13%3A+RSE+Application+Certificate+Provisioning
Request doc: wiki.campllc.org/display/SCP/RA+-+Request+Application+Certificate+Provisioning
Download doc: wiki.campllc.org/display/SCP/RA+-+Download+Application+Certificate
Additional:
- wiki.campllc.org/display/SCP/RA+-+Download+.info+file
- wiki.campllc.org/display/SCP/RA+-+Download+Local+Policy+File
- wiki.campllc.org/display/SCP/RA+-+Download+Local+Certificate+Chain+File
Get Identification Cert

- Identification certs are short lived
  - NO Pseudonymity constraints required
  - Validity period can vary (i-period)
  - One-to-one mapping of PSID and SSP to enrollment cert
  - 1 valid identity certificate per application valid at a time
- EE-RA <--> PCA-RA

Requirements & process description:
wiki.campllc.org/display/SCP/UseCase19%OBE%Identification+Certificate+Provisioning

Request doc: wiki.campllc.org/display/SCP/RA+-+Request+Identification+Certificate+Provisioning
Download doc: wiki.campllc.org/display/SCP/RA+-+Download+Identification+Certificate

Additional:
- wiki.campllc.org/display/SCP/RA+-+Download+_.info+file
- wiki.campllc.org/display/SCP/RA+-+Download+Local+Policy+File
- wiki.campllc.org/display/SCP/RA+-+Download+Local+Certificate+Chain+File
Communicate – How?

The foundation of V2V safety is based on BSM
- J2945/1 - “how to send a BSM”
  - Frequency every 100ms using DSRC
In the device

- Certificate management in the device
  - Send BSMs → as defined in J2945/1
    - BSM every 100ms
    - Change/rotate pseudo cert every 5mins
  - Download and store new batches when possible
    - DSRC, WiFi, Cellular, etc
Hardware, OS, and Software

- [link](https://wiki.campllc.org/display/SPFR/Hardware%2C+Software+and+OS+Security+Requirements) (work in progress → eventual standard??)

- Have an HSM (FIPS 140-2 Level 2 [good])
  - FIPS 140-2 Level 3 [better] (yes more costly)
- Differentiate between (un)privileged applications
EE interface details

• End Entity Requirements Release 1.1 are here: www.its.dot.gov/pilots/pdf/SCMS_POC_EE_Requirements.pdf
  “SHOW OF HANDS IF YOU’VE SEEN THIS DOCUMENT!”

• End Entity Requirements Release 1.2 will be here (published soon): wiki.campllc.org/display/SCP/SCMS+CV+Pilots+Documentation

• ASN.1 repository is here: stash.campllc.org/projects/SCMS/repos/scms-asn/browse
CV Pilot validity

- CV Pilots supported by “SCMS Operations” project
  - 5 year duration
  - All EE CV pilot certs will expire at end of project duration
    - All private keys to be destroyed
  - EE certificate type
    - Section 2.1.2.4 of EE Requirements
  - RootCA – 70 years / useable for 20
    - Component CA certs short enough to exercise rollover
    - Section 2.1.2.6.2 of EE Requirements
  - Every EE must conform to J2945/1 when sending BSMs

More: https://wiki.campllc.org/display/SCP/CV+Pilot+Certificate+Expiration+Timelines
Revocation handling

• Use Case 5: Misbehavior Reporting –
  wiki.campllc.org/display/SCP/Use+Case+5%3A+Misbehavior+Reporting
  wiki.campllc.org/display/SCP/RA+-+Submit+Misbehavior+Report

• Use Case 6: CRL Download –
  wiki.campllc.org/display/SCP/Use+Case+6%3A+CRL+Download
  wiki.campllc.org/display/SCP/MA+-+Download+CRL

• Use Case 8: OBE CRL Check –
  wiki.campllc.org/display/SCP/Step+8.4%3A+OBE+CRL+Check

• Use Case 16: RSE CRL Check –
  wiki.campllc.org/display/SCP/Step+16.4%3A+RSE+CRL+Check
THANK YOU
Sources:

- USDOT Smart City Challenge: [https://www.transportation.gov/smartcity](https://www.transportation.gov/smartcity)
- SAE J2945/1: [http://standards.sae.org/j2945/1_201603/](http://standards.sae.org/j2945/1_201603/)
SCMS Trust Relationship

Root CA

Intermediate CA

Pseudonym CA

Registration Authority

Location Obscurer Proxy

Enrollment CA

Device Config. Manager

OBEs

RSEs

ASDs
pseudonym certificate