

CAMP LLC

Vehicle Safety Communications 5 (VSC5)

HONDA
Honda R&D Americas



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



mazda

NISSAN

VOLKSWAGEN
GROUP OF AMERICA

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! 😊



establish trust

Photo Source: [Núria I. JC](#) via Flickr



**Sign messages & verify
signature**

Photo Source [Wiertz Sébastien](#) via Flickr

Ensure privacy

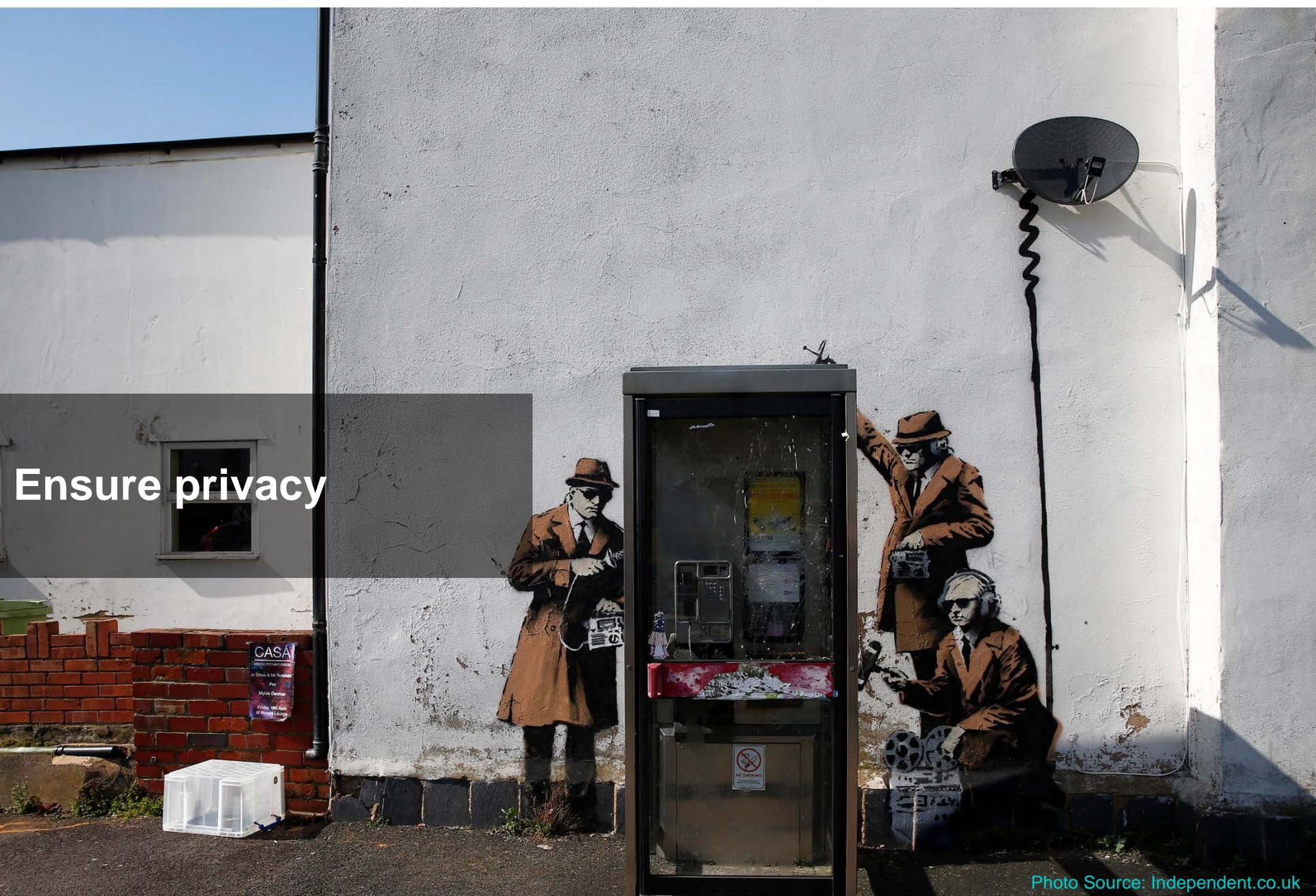


Photo Source: Independent.co.uk

A scroll of aged parchment with the word "CERTIFICATE" written in gold, serif capital letters across the top. The scroll is partially unrolled, showing two wooden rollers with red rings. A red wax seal with a decorative pattern is visible on the right side of the parchment. The parchment has a slightly textured, yellowish-brown appearance with some staining and irregular edges.

CERTIFICATE

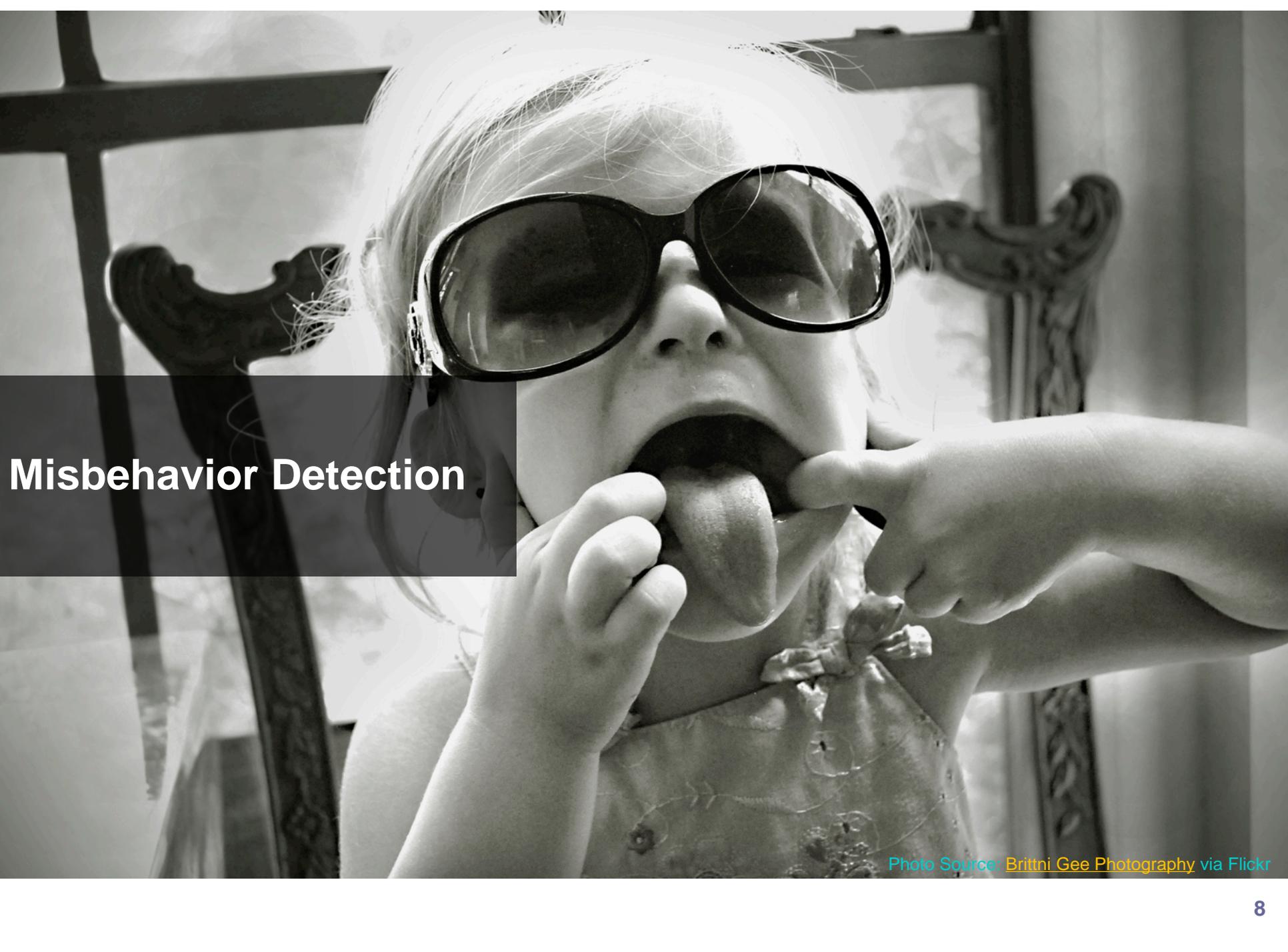
**Long-term certificate
used in interactions
with SCMS**

**Where does it come from?
How does the EE get it?**

**Pseudonym certificate
batch**



Photo Source: REUTERS/Ricardo Mo



Misbehavior Detection

Photo Source: [Brittni Gee Photography](#) via Flickr

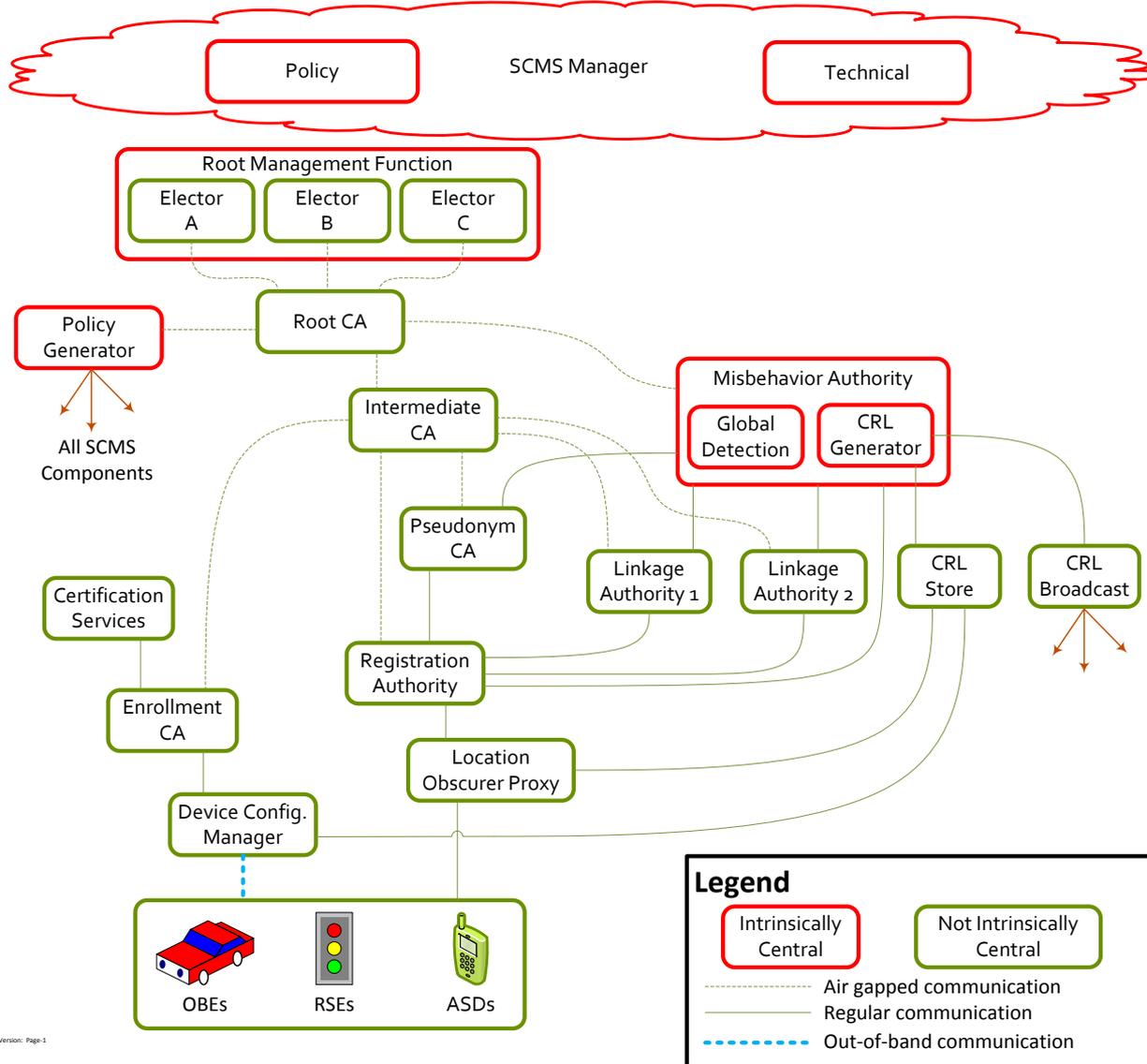


Penalty / device revocation

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

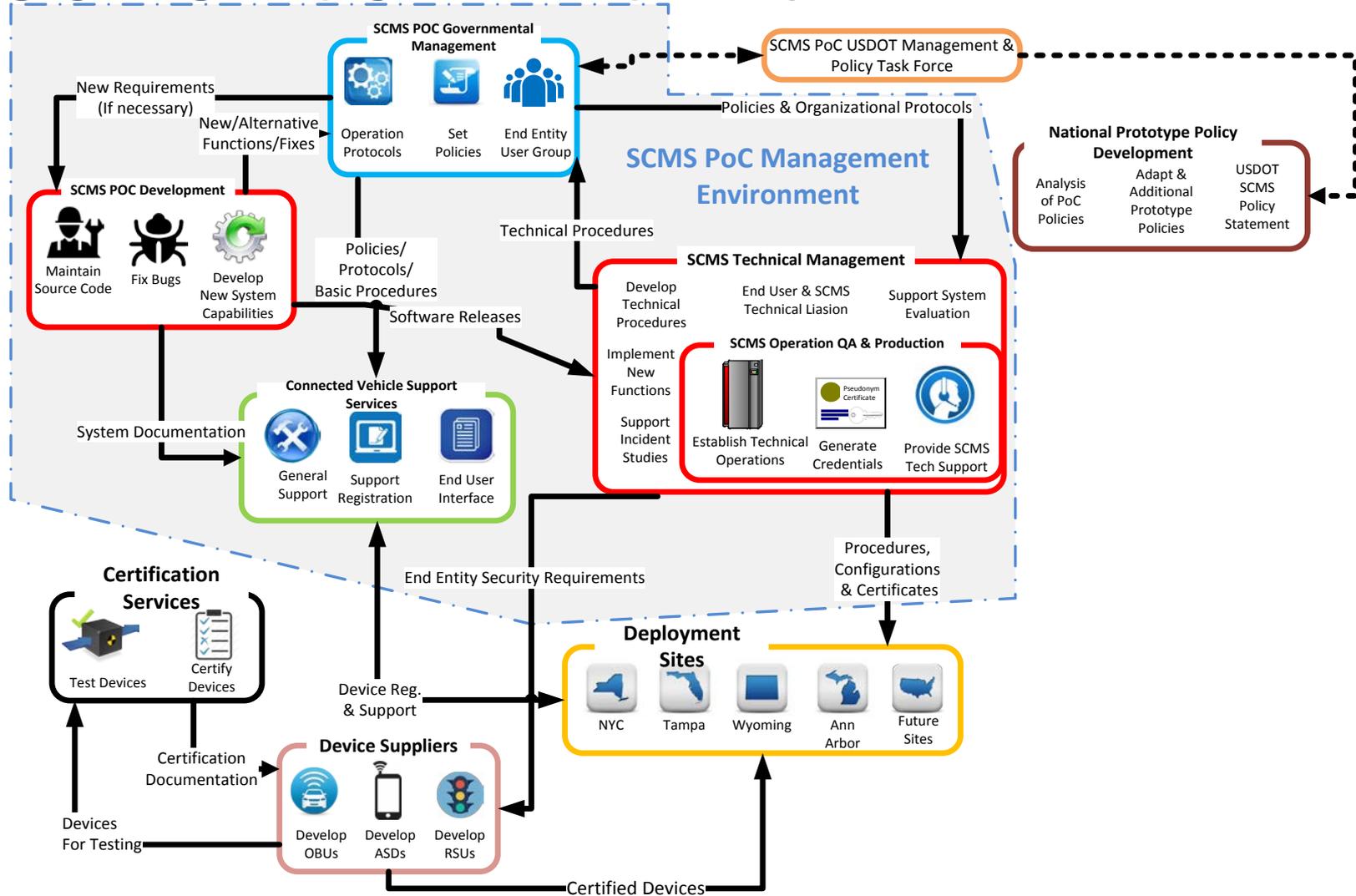
Photo Source: [Andy Devlin/NHLI](#) via [Getty Images](#)

V2X SCMS Architecture

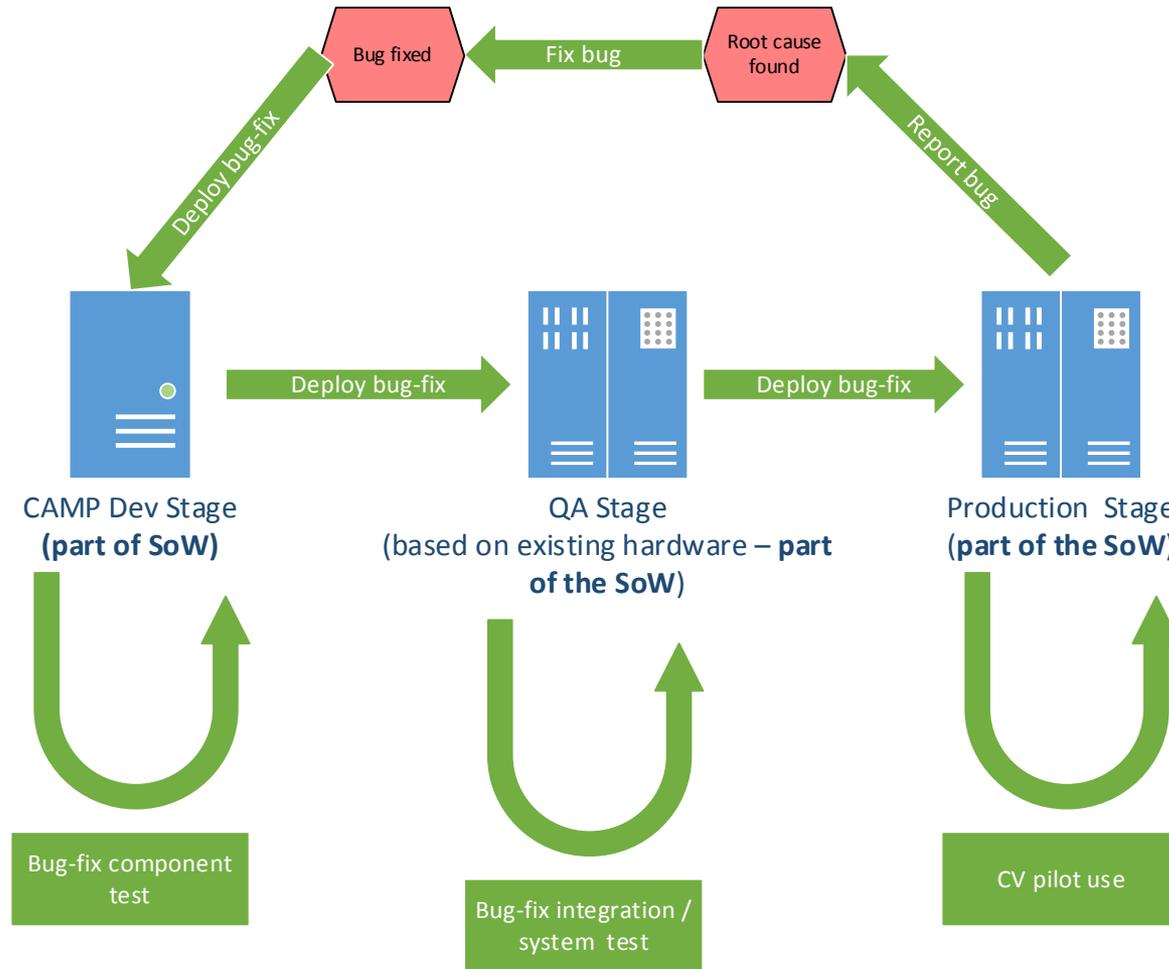


Version: Page-1

SCMS PoC Environment



SCMS “Operations” - Environments



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

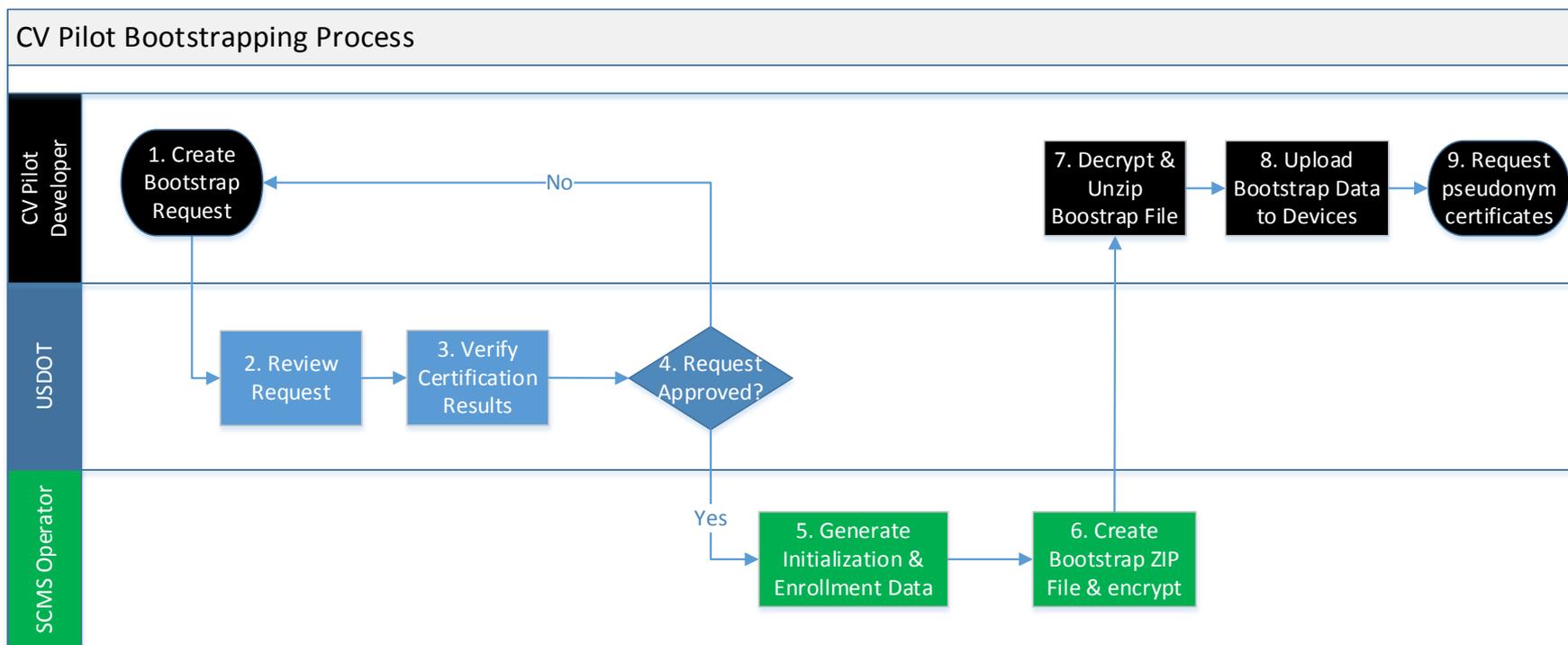
- Enrollment Certificate = long term (life of device)
 - Ticket for admission to SCMS
- Every EE must be provisioned with an Enrollment Certificate
 - part of bootstrap process
 - Expected to cover the lifetime of EE (OBE, RSE/U)
 - OEM specific/proprietary
- Enrollment environment governed by SCMS Manager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

More OBE: wiki.campllc.org/display/SCP/Step+2.2%3A+OBE+Enrollment

More RSE: 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





CERTIFICATE

DCM – Secure Environment

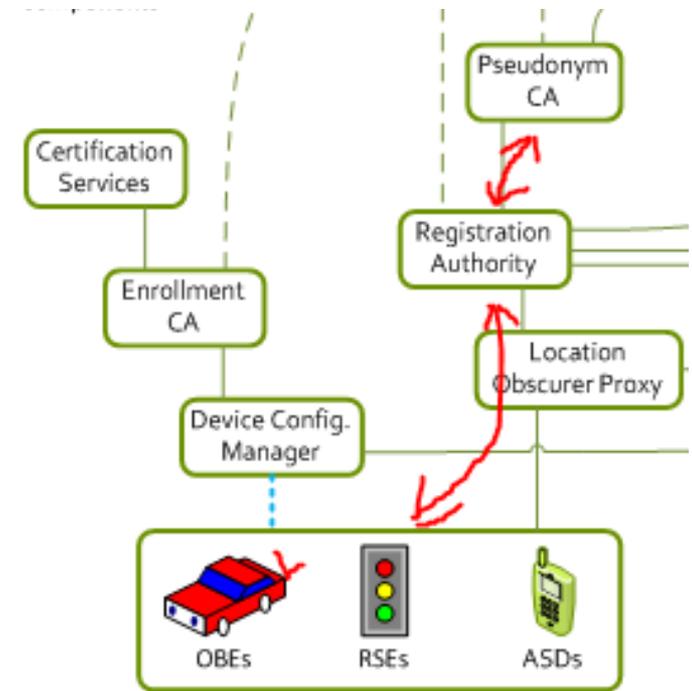
- ECA provides a one-time, long term enrollment certificate
- OEM can design and implement into existing mfg. processes
- No “interface” to the SCMS

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 (1week+1hour)
 - 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

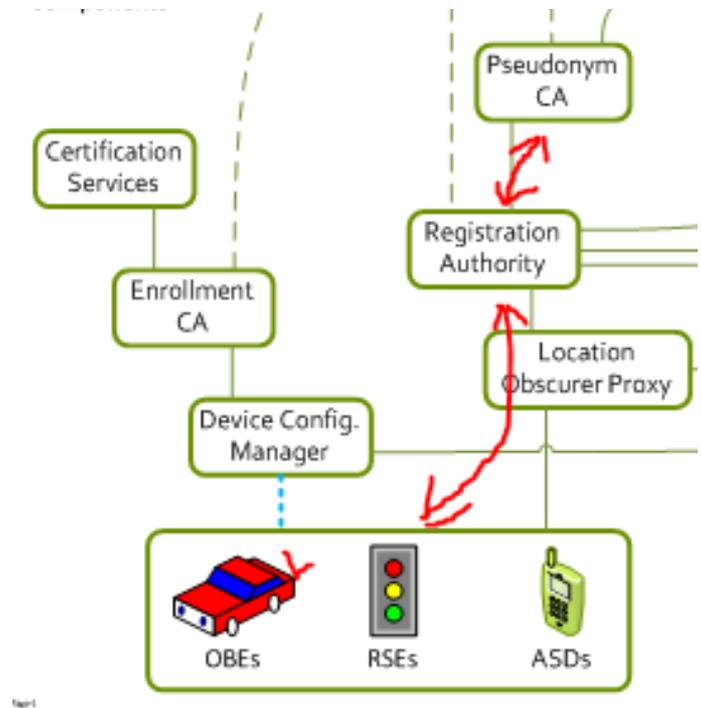
Download doc: wiki.campllc.org/display/SCP/RA+--+Download+Pseudonym+Certificate+Batch

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

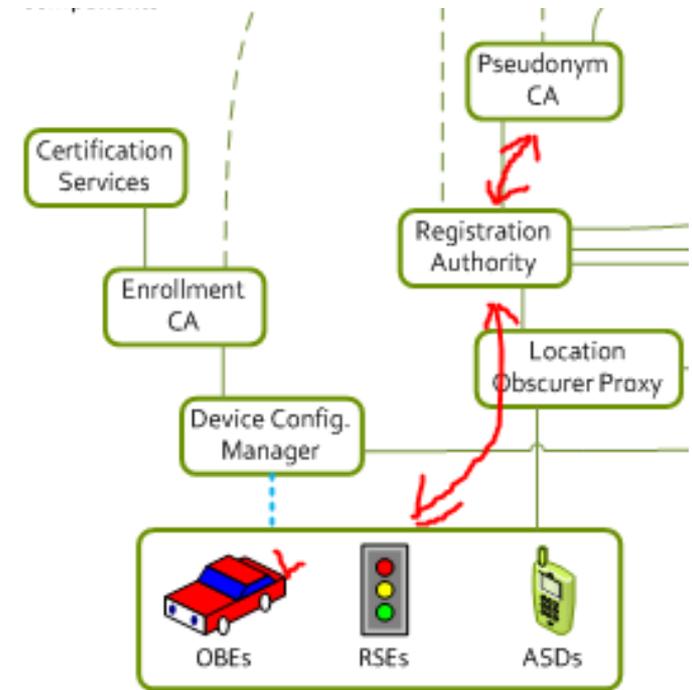
Download doc: wiki.campllc.org/display/SCP/RA+--+Download+Application+Certificate

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/Use+Case+19%3A+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?

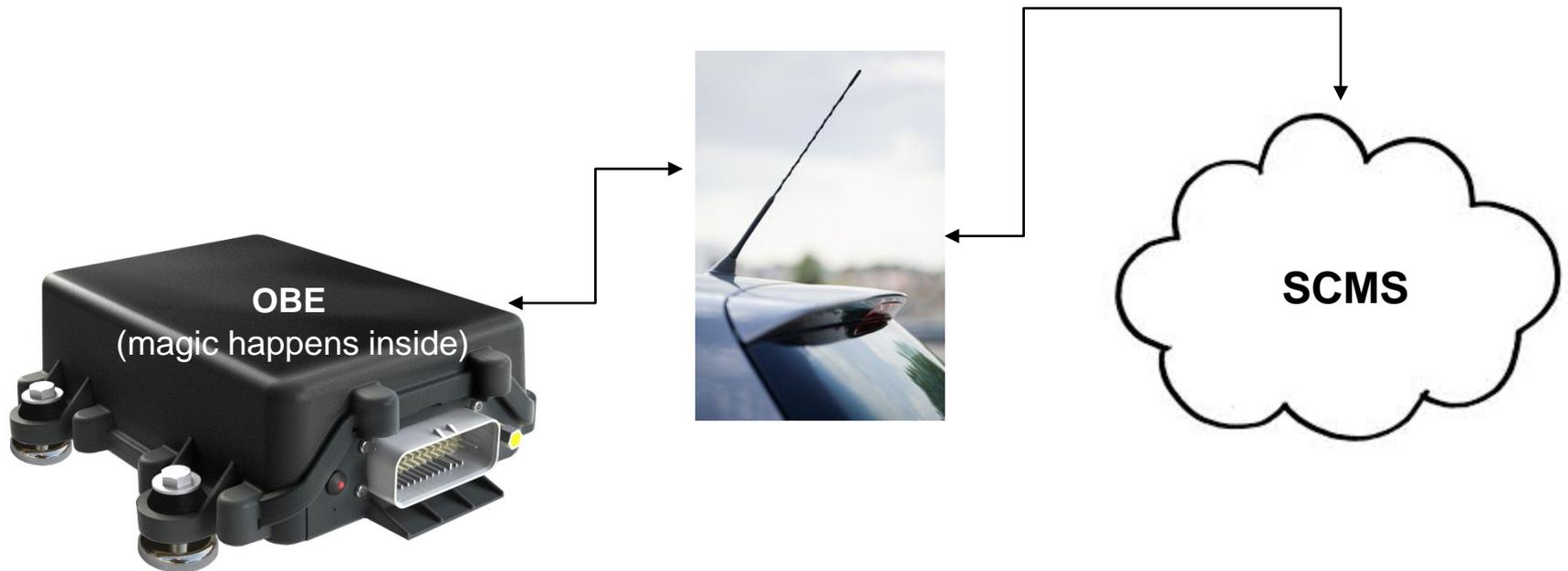
The foundation of V2V safety is based on BSM

- 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

- <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

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



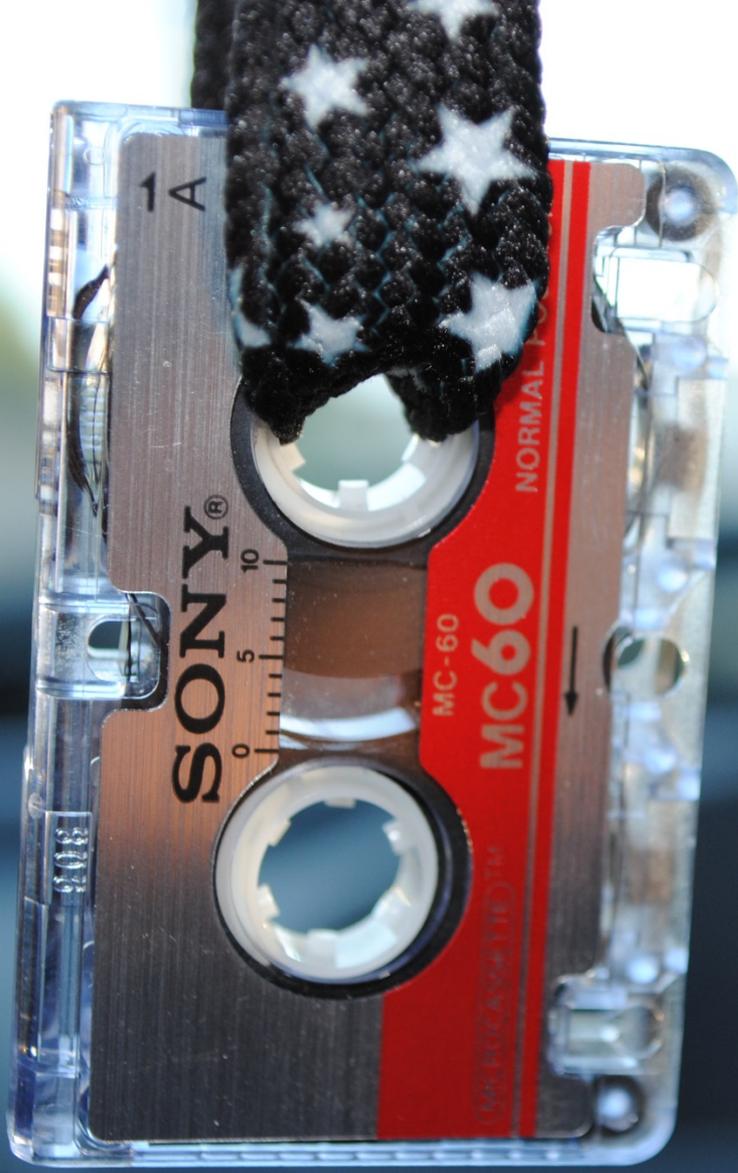
Photo Source: slideshare.net



Sources:

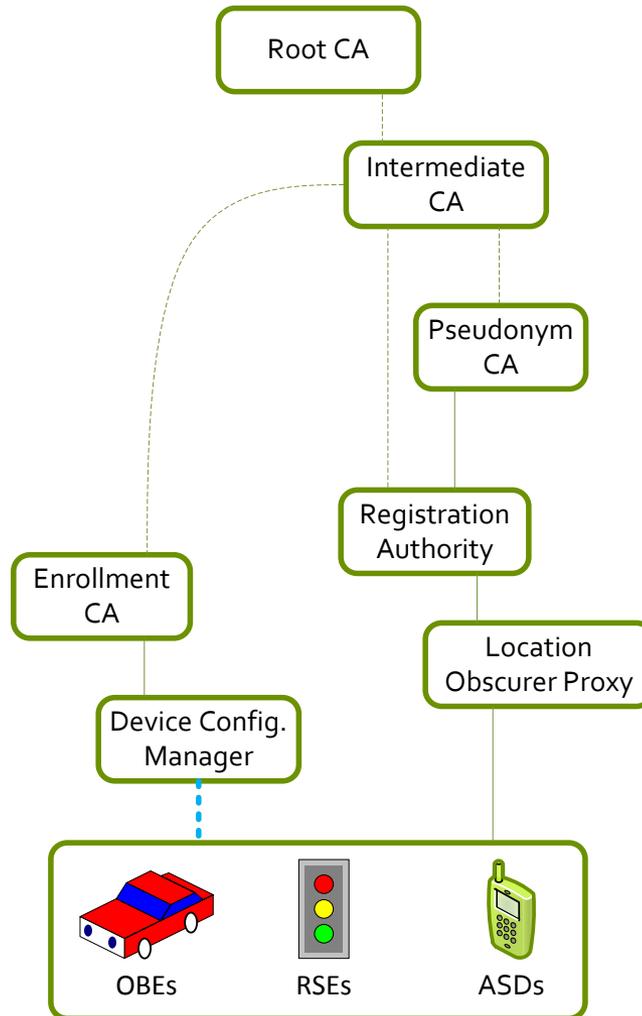
- Elector-based Root Management System to Manage a Public Key Infrastructure:
<http://priorart.ip.com/IPCOM/000245336>
- A security credential management system for V2V communications, Dec 2013
<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6737583>
- Vehicle Safety Communications Security Studies: Technical Design of the Security Credential Management System, July 2013
- Security Credential Management System Design, April 2012
http://www.its.dot.gov/meetings/pdf/Security_Design20120413.pdf
- USDOT CV pilots awarded 2015: <http://www.its.dot.gov/pilots/>
- USDOT Smart City Challenge: <https://www.transportation.gov/smartcity>
- IEEE 1609.2: <https://standards.ieee.org/findstds/standard/1609.2-2016.html>
- IEEE 802.11p: <http://standards.ieee.org/getieee802/download/802.11-2012.pdf>
- SAE J2945/1: http://standards.sae.org/j2945/1_201603/

Photo Source: Wikimedia Commons/Jean-Pol GRANDMONT



Backup

SCMS Trust Relationship





pseudonym certificate