Fundamental Principles and Research of the Security Credential Management System (SCMS) Proof of Concept (POC)

SECURITY CREDENTIAL MANAGEMENT SYSTEM (SCMS) PROOF OF CONCEPT (POC)

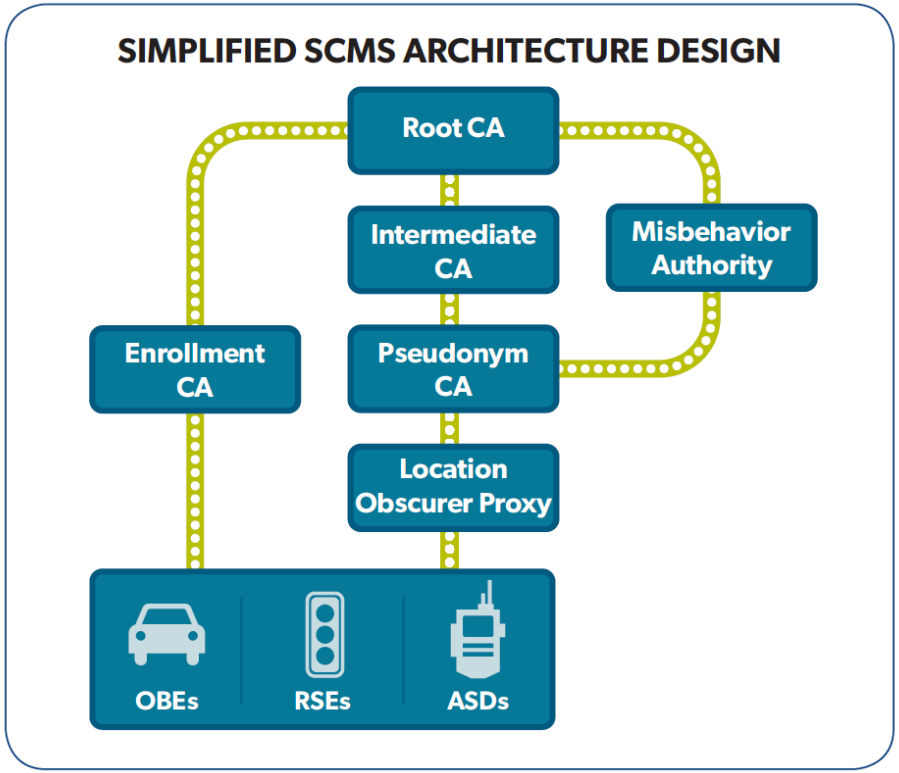
Jonathan Walker, P.E.
U.S.DOT - ITS Joint Program Office

Agenda

- What is the Security Credential Management System (SCMS) Proof-of-Concept (POC)?
- Background on the SCMS POC
  - *V2V Security Credential Management System Request for Information (RFI)*
  - *SCMS POC Research under the Connected Vehicle Pilots Program*
- The Road Map Ahead for the SCMS POC
  - *Access to the SCMS POC and the Eligibility Criteria*
  - *SCMS POC services ending in December 2020*
  - *Extracting Policies, Procedures, and Lessons Learned*
- SCMS POC Quality Assurance (QA) Enrollment Certification Process
  - *Access to the SCMS POC documentation*
  - *End-Entity Software Development*
  - *End-Entity Manual Bootstrapping Process*
- End-Entity Device Certification to Standards
  - *Certification Operating Council*
  - *October 2017 PlugFest*

What is the SCMS POC?

- The SCMS POC provides the security infrastructure to issue and manage the security certificates that form the basis of trust for Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication.
- Connected vehicle devices enroll into the SCMS, obtain security certificates from certificate authorities (CAs), and attach those certificates to their messages as part of a digital signature.
- The SCMS system and processes provide a high level of confidence that the device is a trusted actor in the system, while also maintaining privacy.



Source: https://www.its.dot.gov/factsheets/pdf/CV_SCMS.pdf

Background on the SCMS POC -*V2V SCMS RFI*

- On October 15, 2014, the National Highway Traffic Safety Administration (NHTSA) issued a Request for Information (RFI) to seek information related to the security system that will support V2V operations.
- The RFI was focused on the following:
  - **Become aware of private entities that may have an interest in exploring the possibility of developing and/or operating components of a V2V Security Credential Management System (SCMS);**
  - Receive responses to the questions posed about the establishment of an SCMS;
  - Obtain feedback, expressions of interest, and comments from all interested public, private, and academic entities on any aspect of the SCMS.

Source: https://www.federalregister.gov/documents/2014/10/15/2014-24482/vehicle-to-vehicle-security-credential-management-system-request-for-information

Background on the SCMS POC -*V2V SCMS RFI*

SCMS RFI Table of Contents

- RFI Guidelines
- Background on V2V and the Agency's Actions Thus Far
- Security Overview and Operational Characteristics
- SCMS Organizational Options
- Comment Period Closed on December 15, 2014
- Document Citation: 79 FR 61927
- Document Number: 2014-24482

Source: https://www.federalregister.gov/documents/2014/10/15/2014-24482/vehicle-to-vehicle-security-credential-management-system-request-for-information

Background on the SCMS POC
-SCMS POC Research CVP Program

NYCDOT

Tampa (THEA)

WYDOT

- The USDOT issued an advance notice to release a Broad Agency Announcement (BAA) for Connected Vehicle Pilots Phase I on December 19, 2014.
- The BAA was issued on January 30, 2015
- The CV Pilot Phase I were awarded on September 13, 2015
  - New York City Department of Transportation (https://www.its.dot.gov/pilots/pilots_nycdot.htm)
  - Tampa-Hillsborough Expressway Authority (https://www.its.dot.gov/pilots/pilots_thea.htm)
  - Wyoming Department of Transportation (https://www.its.dot.gov/pilots/pilots_wydot.htm)

Sources:
https://www.fbo.gov/index?s=opportunity&mode=form&id=4bb6693ac3021c178595d83fab3b5d73&tab=core&tabmode=list&=
http://www.federalgrants.com/Connected-Vehicle-CV-Pilot-Deployment-Program-Phases-2-and-3-60170.html

Background on the SCMS POC
-SCMS POC Research CVP Program

In BAA and award contract, the three (3) CV Pilot sites were required to utilize the SCMS POC so the USDOT could obtain a full understanding of the following areas as it relates to a national SCMS:

Policy Framework	**Scalability**
Security Algorithms	**Standards Requirements**
Support Mechanisms	**Technical Challenges**

"The proposed pilot shall utilize the SCMS as a tool to support general deployment communication security. Physical security of the elements that make up the installation should be addressed as well. In addition, the proposed pilot shall utilize the SCMS for at least one of the proposed applications, and all applications where utilizing the SCMS is deemed appropriate (e.g., applications where trust and security are essential)."

Source: https://www.fbo.gov/index?s=opportunity&mode=form&id=4bb6693ac3021c178595d83fab3b5d73&tab=core&tabmode=list&=

Road Map Ahead for the SCMS POC - *Access to the SCMS POC and the Eligibility Criteria*

- The SCMS POC is comprised of a Quality Assurance (QA) system and a Production (Pr) system.
- The SCMS POC QA system is a way of avoiding problems when delivering a service based on a system requirements.
- The SCMS POC Production system is a fully function system that supports an operation (or “live”) environment.
- Research deployment sites that derive funding from the USDOT are eligible to request enrollment into the SCMS POC.
- Any agency that plans to initiate a project to deploy connected vehicle technology may consider procuring turnkey connected vehicle devices that meet the following requirements:
  - Devices are provisioned with security credentials upon delivery;
  - Security certificate services, including downloads of new certificates, are provided for the life of the device;
  - Security credentials provided by the supplier are interoperable with credentials provided by the USDOT SCMS.

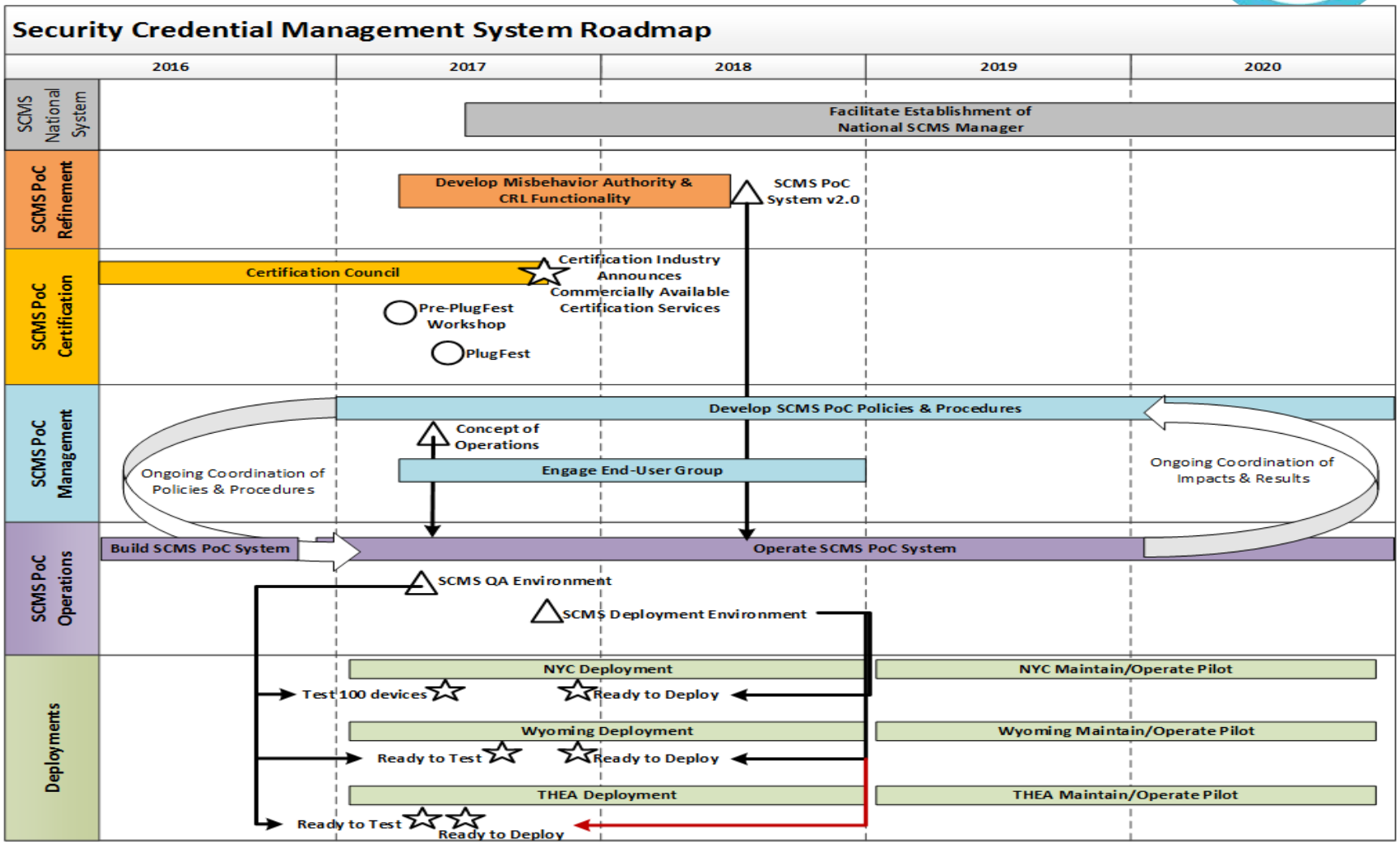
Source: https://www.its.dot.gov/factsheets/pdf/CV_SCMS.pdf

Road Map Ahead for the SCMS POC - *Extracting Policies, Procedures, and Lessons Learned*

- The SCMS POC will end services in December 2020.
- The SCMS is a proof-of-concept system with a limited funding budget.
- One goal of the SCMS POC is to extract the policies, procedures, and lessons learned from the design, deployment, and operations with a focus on generating public documents for stakeholders who are interested in establishing a National SCMS.

Source: https://www.its.dot.gov/factsheets/pdf/CV_SCMS.pdf

Road Map Ahead for the SCMS POC - *Extracting Policies, Procedures, and Lessons Learned*



SCMS POC QA Enrollment Certification Process – *Access to the SCMS POC documentation*

- The U.S. Department of Transportation (USDOT) is committed to ensuring that connected vehicle technologies operate in a safe, secure, and privacy-protective manner.
- For this reason, the USDOT has partnered with the automotive industry and industry security experts through the Crash Avoidance Metrics Partnership (CAMP) to implement a temporary proof-of-concept security system.
- The temporary proof-of-concept security system will enable the USDOT's connected vehicle (CV) projects to address unanswered questions regarding the exchange of information among vehicles, roadway infrastructures, traffic management centers, and wireless mobile devices.
- The CAMP wiki is the central location for documentation related the SCMS POC https://wiki.campllc.org/#all-updates.

SCMS POC QA Enrollment Certification Process - *End-Entity Software Development*

- A device (or “End-Entity device”) seeking to communicate with the SCMS POC will require some level of software development.
- If the End-Entity device software achieves 9 of 13 steps detailed in the “Introduction for EE Developers” guide, the device should be successful in communication with the current version of the SCMS POC.
- The “Introduction for EE Developers” guide is located at https://wiki.campllc.org/display/SCP

SCMS POC QA Enrollment Certification Process - *End-Entity Software Development*

wiki.campllc.org

TinkercadCrea...gitalDesigns | Save to Mendeley | Scholar : My ... Library Help | Johnny Walker LA - YouTube | Apple | Google | Wikipedia

Confluence CAMP Wiki Spaces Log in

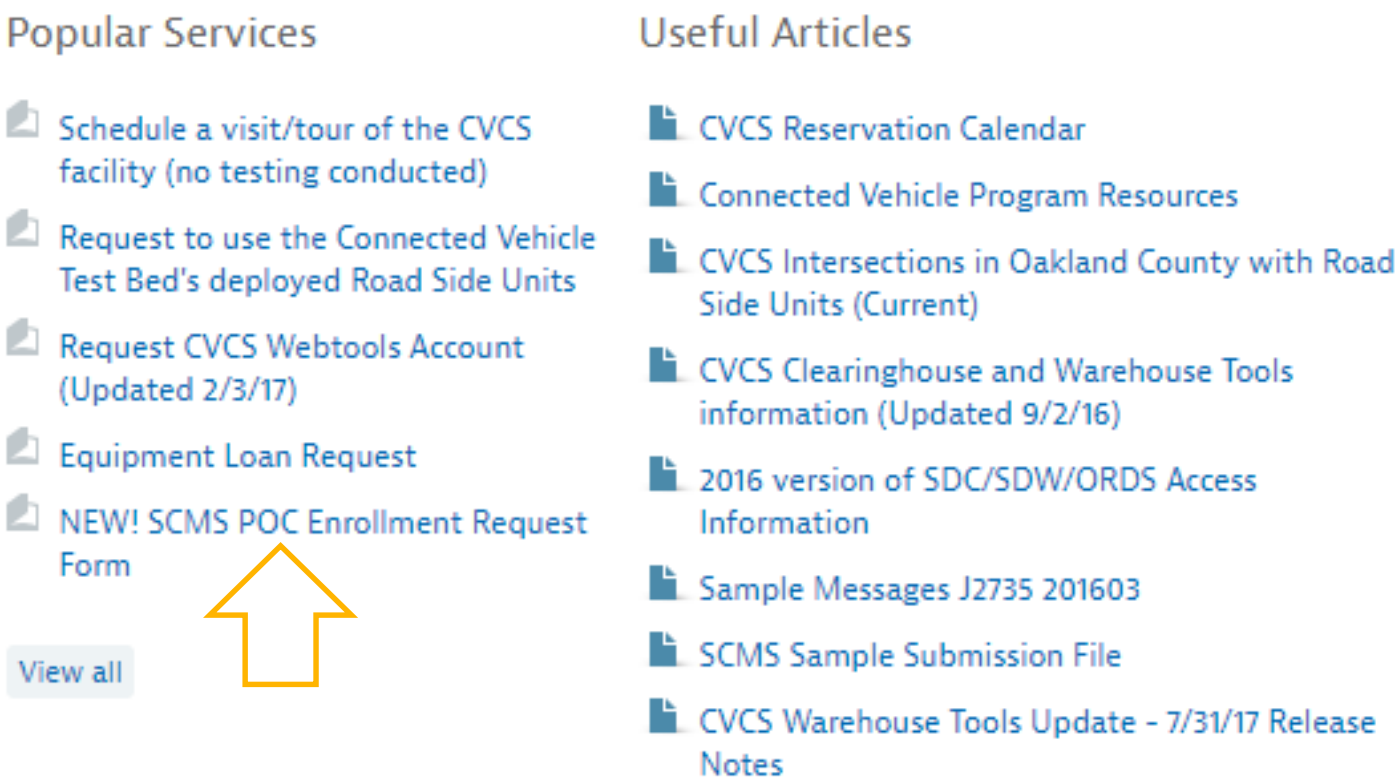
Introduction for EE Developers

The following paragraph will guide you as an EE developer through this documentation highlighting requirements and API documentation in the order of an EE's lifecycle. If you implement your EE software following this guide, you should have a device at the end that is able to communicate with the SCMS throughout the whole lifecycle.

1. First of all you need a Secure Environment for Device Enrollment where initialization and bootstrapping of your device will be executed
2. You need to have a device that applies to the requirements and descriptions laid out in Hardware, Software and OS Security Requirements
3. You need to have a True Random Number Generator
4. Your device needs to support in either hardware or software Approved Cryptographic Algorithms
5. You need to have an HTTP client that is able to communicate securely (HTTPS) to the SCMS as described in EE-RA Communications - General Guidance and EE-SCMS Core Communication Requirements
6. You need to know which Certificate Types you need to have on your device, which depends on the SCMS PoC Supported V2X Applications that you want to run on your device
7. The EE lifecycle starts with Use Case 2: OBE Bootstrapping (Manual), respectively Use Case 12: RSE Bootstrapping (Manual) depending on your EE type (OBE vs. RSE). Currently both processes are exactly the same.
8. Based on the EE type you are developing, you then create and send one of the following requests. All devices should always check for a new local certificate chain file (API: RA - Download Local Certificate Chain File) and a new local policy file (API: RA - Download Local Policy File) before sending subsequent request. All requests in this step #8 should be sent within the same HTTPS session.
    a. Pseudonym Certificates:
        i. Following the process in Use Case 3: OBE Pseudonym Certificates Provisioning, your OBE should create a pseudonym certificate batch request as described in Step 3.1: Request for Pseudonym Certificates and send it to the RA API as documented in RA - Request Pseudonym Certificate Batch Provisioning. Your OBE needs to create the butterfly seed pairs as described in SCP1: Butterfly Keys. Your OBE will get a response from RA with an *URL* and a *download time*.
        ii. Once your OBE's clock reaches *download time*, your OBE can download the initial pseudonym certificate batch at *URL* following the process in Step 3.3: Initial Download of Pseudonym Certificates using the RA API as documented in RA - Download Pseudonym Certificate Batch and the .info file using RA's API documented in RA - Download .info File.
    b. Application Certificate:
        i. Following the process in Use Case 13: RSE Application Certificate Provisioning, your RSE should create an application certificate request as described in Step 13.1: Request RSE Application Certificate and send it to the RA API as documented in RA - Request Application Certificate Provisioning. Your RSE will get a response from the RA with an *URL* and a *download time*.
        ii. Once your RSE's clock reaches *download time*, your RSE can download the application certificate at *URL* following the process in Step 13.3: Download RSE Application Certificate using the RA API as documented in RA - Download Application Certificate.
    c. OBE Identification Certificate:
        i. Following the process in Use Case 19: OBE Identification Certificate Provisioning, your OBE should create an identification certificate request as described in Use Case 19: OBE Identification Certificate Provisioning and send it to the RA API as documented in RA - Request Identification Certificate Provisioning. Your OBE will get a response from RA with an *URL* and a *download time*.
        ii. Once your OBE's clock reaches *download time*, your OBE can download the identification certificate at *URL* following the process in Step 19.3: Initial Download of OBE Identification Certificates using the RA API as documented in RA - Download Identification Certificate and the .info file using RA's API documented in RA - Download .info File.
9. Depending on the certificate type, the SCMS constantly pre-generates them and your EE can download top-offs like this:
    a. Pseudonym Certificates: Whenever it suits your pseudonym certificate download strategy at a point of time that is after the time given in the .info file, follow the process described in Step 3.5: Top-off Pseudonym Certificates using RA's API documented in RA - Download Pseudonym Certificate Batch to download additional pseudonym certificates.
    b. Identification Certificate: Whenever it suits your identification certificate download strategy at a point of time that is after the time given in the .info file, follow the process described in Step 19.5: Top-off OBE Identification Certificates using RA's API documented in RA - Download Identification Certificate to download the next identification certificate.
10. Your EE should download the latest CRL as often as possible but no later than once a week using the process described in Use Case 6: CRL Download using the API documented in MA - Download CRL.
11. Your EE must verify incoming messages. Part of the verification is to check if the senders certificate was revoked following the process described in Step 8.4: OBE CRL Check, respectively Step 16.4: RSE CRL Check, as well as if a CA certificate in their certificate chain was revoked.
12. Report misbehavior: This is still TBD and will be supported with SCMS Release 2
13. Re-enroll: This is still TBD and will be supported with SCMS Release 2

SCMS POC QA Enrollment Certification Process – *Register To Start The Certification Process*

- Step 1: Register at the Samanage website: https://cvcs.samanage.com
- Step 1: Under the "Popular Services" column, there is a selection for **"New! SCMS POC Enrollment Request Form."**



SCMS POC QA Enrollment Certification Process - *End-Entity Manual Bootstrapping Process*

The manual bootstrap process will enable the End-Entity device to interact with the SCMS POC. Bootstrapping is executed at the start of the End-Entity device's lifecycle. At the start of bootstrapping, the End-Entity device has no SCMS POC certificates and no knowledge of how to contact the SCMS.

- Step 1: Go to CAMP Wiki page (https://wiki.campllc.org/#all-updates) and review the section titled, "Use Case 2: OBE Bootstrapping (Manual).
- Step 2: Read each section and following the step-by-step instructions under "Process Steps – Manual Bootstrapping Process – QA Environment".
- Step 3: Also, there are instructions for "Process Steps – Manual Bootstrapping Process – PROD Environment" once the End-Entity device is ready for field operations under the production environment.

SCMS POC QA Enrollment Certification Process - *End-Entity Manual Bootstrapping Process*

Confluence CAMP Wiki Spaces

Pages / ... / Requirements by Use Case

Use Case 2: OBE Bootstrapping (Manual)

Created by Benedikt Brecht, last modified on Sep 05, 2017

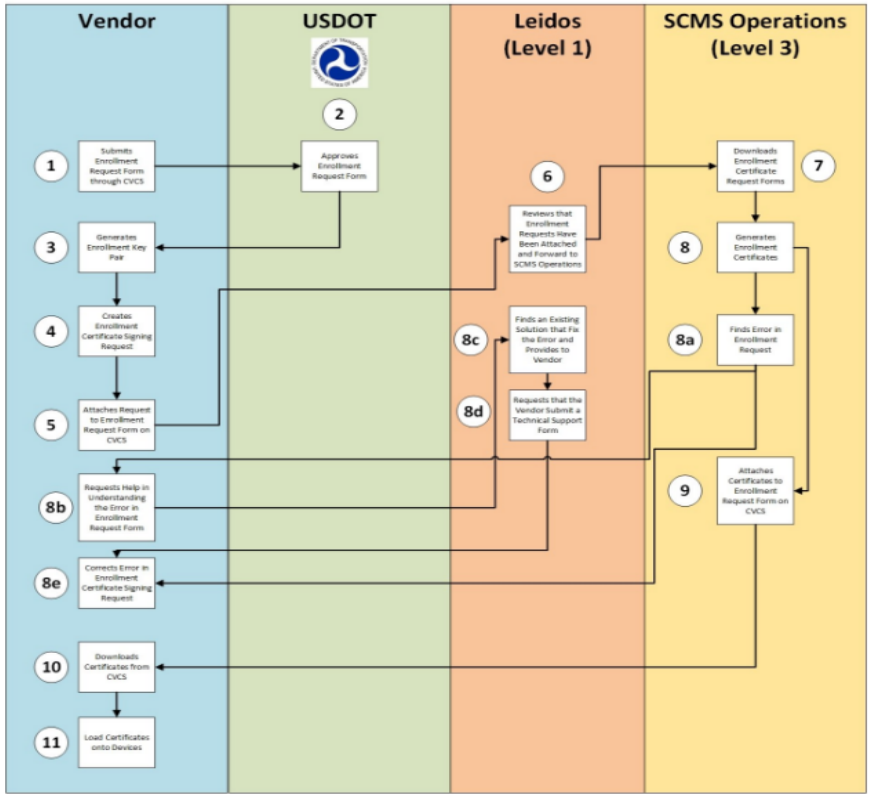
Table of Contents

- Background and Goals
- Assumptions and Preconditions
- Process Steps
  - Manual Bootstrapping Process - QA Environment
  - Manual Bootstrapping Process - PROD Environment
    - OBE Bootstrap Process Logging Requirement
- Enrollment Certificate Request Example
- Requirements
- Additional Reference Information
- ASN.1 Specification

SCMS POC QA Enrollment Certification Process - *End-Entity Manual Bootstrapping Process*

Manual Bootstrapping Process - QA Environment

The CV Pilot will initially use a manual bootstrapping process that combines device initialization and enrollment. The following process applies to the SCMS QA stage. The vendor will initiate this process by requesting device initialization information and enrollment certificate from a **DOT Workflow Approval** tool, as depicted in this process:



SCMS POC QA Enrollment Certification Process - *End-Entity Manual Bootstrapping Process*

Step	Actor	Description	Status	Assignee
1	Vendor	Logs into CVCS Samanage, initiates an enrollment certificate request. There is a dedicated form for that.	**New**	USDOT
2	USDOT	Logs into CVCS Samanage and reviews the enrollment certificate request form. They ensure that: • The vendor is on the list of known vendors for CV device manufacture. • If the request is not correct, USDOT will deny the request, and the vendor will need to correct the request and resubmit through Step 3. USDOT Personnel approve the request, if it meets the above criteria, and USDOT sends the request back to the Vendor for them add the enrollment certificate signing request.	**Awaiting Customer Input**	Leidos
3	Vendor	The vendor **in his secure environment** generates **in each OBE** a verification key pair (see Public Key Algorithms in CB2: Types of Cryptographic Algorithms). The private key is used to sign the enrollment certificate request (CSR) in step 2. The public key is added to the request and used by the ECA subsequently as input to calculating the public value within the implicit certificate, issued at end of this process. **NOTE:** The verification key pair must be generated using an algorithm approved for use (see Approved Cryptographic Algorithms, Approved Random Number Generators). Best practice is to generate the verification key pair inside the EE's HSM and the private key never leaves the EE.	**Awaiting Customer Input**	Leidos
4	Vendor	The vendor **in his secure environment** creates an enrollment certificate signing request **for each device**, signs it with the **each device's private key**, and writes the CSR to a file with filename format <enrollment pub hex>.oer. He then collects multiple CSRs, places them in a flat directory and zips the directory. The directory structure within the zip file should look similar to the following example: **Enrollment Request Zip File Example** › Expand source	**Awaiting Customer Input**	Leidos
5	Vendor	Vendor logs into CVCS Samanage and attaches the enrollment request zip file to the previous enrollment request form.	**Awaiting Customer Input**	Leidos
6	Leidos	Reviews Enrollment Request Form and ensures files have been attached and manually verifies the following fields: • PSID • Region	**Assigned**	SCMS Operations
7	SCMS Operations	Logs into CVCS Samanage and downloads the enrollment certificate request zip file.	**Work in Progress**	SCMS Operations

SCMS POC QA Enrollment Certification Process - *End-Entity Manual Bootstrapping Process*

8	SCMS Operations	Executes their enrollment requests script to create enrollment certificates. If successful move to Step 9. The ECA generates and returns an enrollment certificate for each individual request. The response is a signed structure called SignedEeEnrollmentCertResponse. The SCMS operator collects all ECA responses, creates a directory structure that includes bootstrapping information as well as one directory per CSR using the filename of the CSR as directory name. Each of those directories contains the RA certificate to be used by the OBE to communicate with the SCMS, the certificate of the ECA that signed the enrollment certificate, as well as the enrollmentCert itself and the privKeyReconstruction. The SCMS operator zips all files into a single zip file. Following the example in step 4, the directory structure within the zip file would look like this (please be aware that the Root CA certificate is explicitly given in the file root.oer): **Enrollment Resonse Zip File Example** › Expand source	**Work in Progress**	SCMS Operations
8a	SCMS Operations	If SCMS Operations finds an error within the request, SCMS Operations will send the Error Response to the Vendor through the CVCS enrollment request.	**Awaiting Customer Input**	SCMS Operator
8b	Vendor	Requests help/clarification in understanding the error found in the enrollment certificate signing request as a comment to the Enrollment Request Form.	**Work in Progress**	Leidos
8c	Vendor	Looks for an existing solution that will fix the vendors error. If they find a solution they provide it to the vendor.	**Awaiting Customer Input**	SCMS Operator
8d	Vendor	If an existing solution cannot be found, Leidos requests the vendor submit the Technical Support form and sends the Vendor the link.	**Awaiting Customer Input**	SCMS Operator
8e	Vendor	Corrects the error and reattaches the enrollment certificate signing request to the Enrollment Request Form.	**Awaiting Customer Input**	SCMS Operator
9	SCMS Operator	Logs into the CVCS Samanage and creates an enrollment certificate response for the appropriate vendor and attaches the enrollment response **zip file.**	**Resolved**	Vendor
10	Vendor	Vendor logs into CVCS Samanage and downloads their device enrollment certificates **in their secure environment**.	**Resolved**	Vendor
11	Vendor	The vendor loads the appropriate enrollment certificate onto the appropriate device, **in their secure environment.**	**Resolved**	Vendor

End-Entity Device Certification to Standards - *Connected Vehicle Standards and Certification Operating Council*

In order to maintain interoperability between devices, there are three (3) sets of standards that are commonly used in the connected vehicle environment:

- One developed under the IEEE 802.11.p standard
- Two under SAE J2735 and SAE J2945
- Several standards under IEEE 1609

The Certification Operating Council (COC) has been tasked with creating a foundation for industry to develop a self-sustainable certification program.

Going forward, the COC and OmniAir are launching a formal certification program as of October 1, 2017 and are hosting their own PlugFest on October 16th – 20th, 2017. ***[More details will be provided in the next presentation]***

Source:

https://www.eventbrite.com/e/omniair-consortiums-plugfest-by-the-bay-2017-tickets-36163330495

http://omniair.org/plugfest-bay-october-16/

End-Entity Device Certification to Standards - *October 2017 PlugFest*

- October 16-20, 2017
- Day 1
  - Connected Vehicle Policy Workshop 11:00am-5:30pm
  - Reception 5:30-7:30pm
  - Metropolitan Transportation Commission (MTC) Offices:
    - 375 Beale St., San Francisco, California 94105
- Days 2-5
  - Bench and V2V Mobile Interoperability 8am-6pm
  - UL Fremont Office:
    - 47266 Benicia Street, Fremont, CA

[More details will be provided in the next presentation]

Source:
https://www.its.dot.gov/research_archives/connected_vehicle/connected_vehicle_standards.htm

http://omniair.org/

Contacts

SCMS

- USDOT – NHTSA SCMS Lead: John Harding (John.Harding@dot.gov)
- USDOT – SCMS Operations Lead: Jonathan Walker (Jonathan.B.Walker@dot.gov)
- USDOT – National SCMS Lead: Kevin Gay (Kevin.Gay@dot.gov) & Robert Kreeb (Robert.Kreeb@dot.gov)

CV-Pilot Deployment Program

- USDOT Lead: Kate Hartman (Kate.Hartman@dot.gov)

CV Pilot Sites

- For inquiries regarding the individual pilots, please contact the respective Point of Contacts:
- NYCDOT pilot
  - Mohamad Talas: Mtalas@dot.nyc.gov
  - Wesam Daraghmeh: WDaraghmeh@dot.nyc.gov
- Tampa (THEA) pilot
  - Steve Novosad: snovosad@hntb.com
- WYDOT pilot
  - dot-cvpilot@wyo.gov

Source: https://www.its.dot.gov/pilots/index.htm