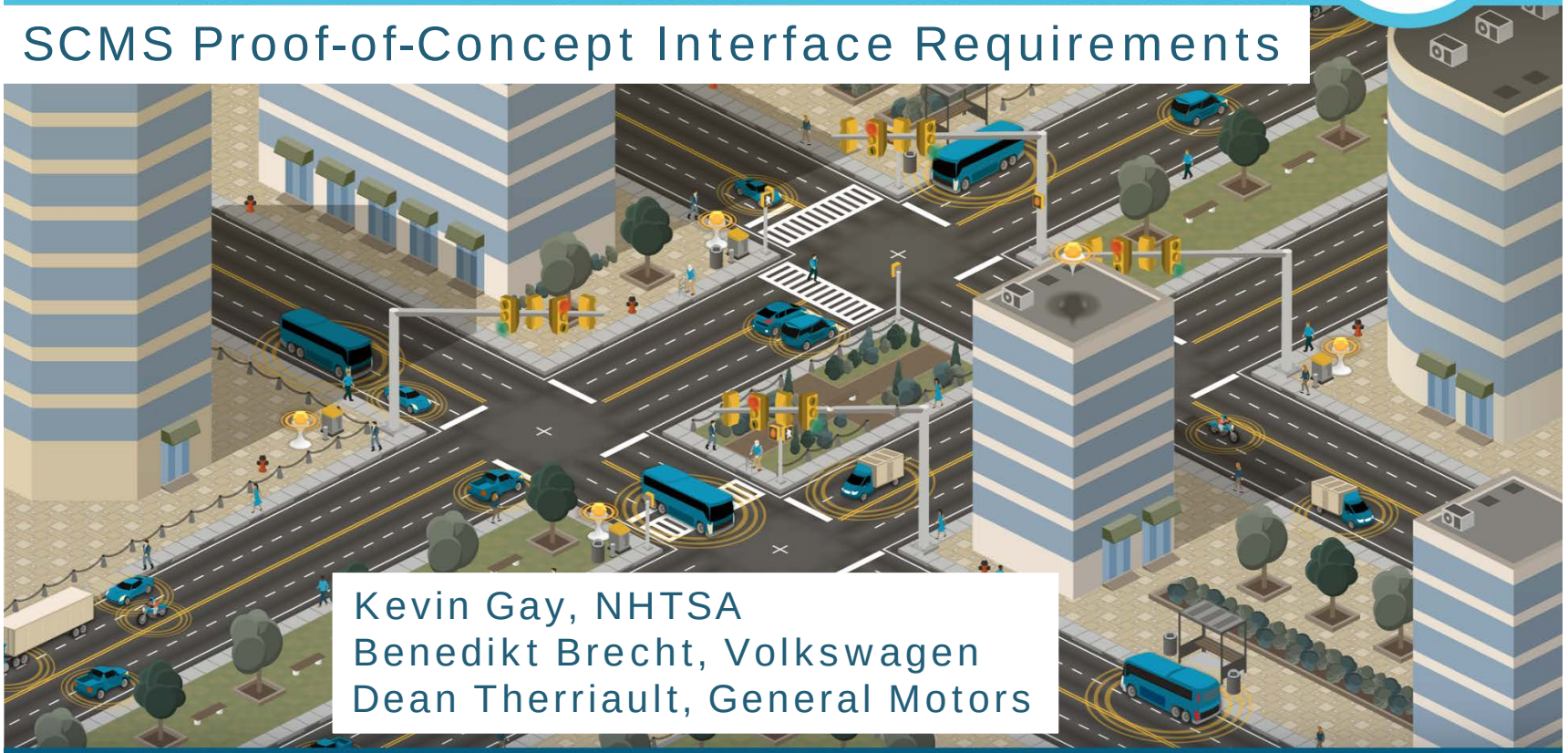
CONNECTED VEHICLE PILOT
Deployment Program

SCMS Proof-of-Concept Interface Requirements



Kevin Gay, NHTSA
Benedikt Brecht, Volkswagen
Dean Therriault, General Motors

ITS Joint Program Office

TODAY'S AGENDA

- Purpose of this Technical Assistance Webinar Series
  - To assist not only the three selected sites, but also other early deployers of connected vehicle technologies to conduct Concept Development activities.

- Webinar Content
  - Connected Vehicle Pilot Deployment Program Overview
  - SCMS Proof-of-Concept Interface Requirements
  - Stakeholder Q&A
  - How to Stay Connected

- Webinar Protocol
  - Please mute your phone during the entire webinar
  - You are welcome to ask questions via chatbox at the Q&A Section
  - The webinar will be recorded except the Q&A Section
  - The webinar recording and the presentation material will be posted on the CV Pilots website within a week

CV Pilot Deployment Program Goals

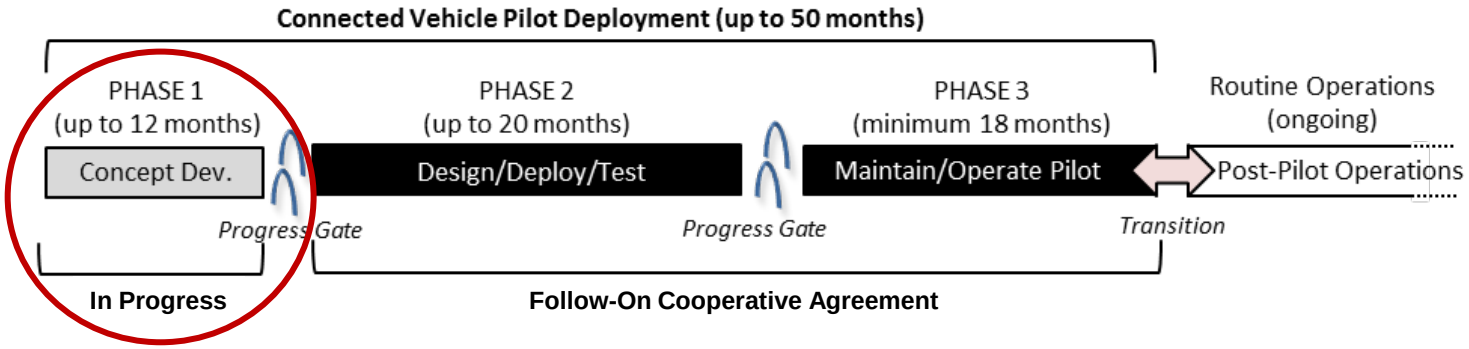
Sites Selected – 2015 Awards

- Reduce the number and severity of adverse weather-related incidents in the I-80 Corridor in order to improve safety and reduce incident-related delays.
- Focused on the needs of commercial vehicle operators in the State of Wyoming.

- Improve safety and mobility of travelers in New York City through connected vehicle technologies.
- Vehicle to vehicle (V2V) technology installed in up to 10,000 vehicles in Midtown Manhattan, and vehicle to infrastructure (V2I) technology installed along high-accident rate arterials in Manhattan and Central Brooklyn.

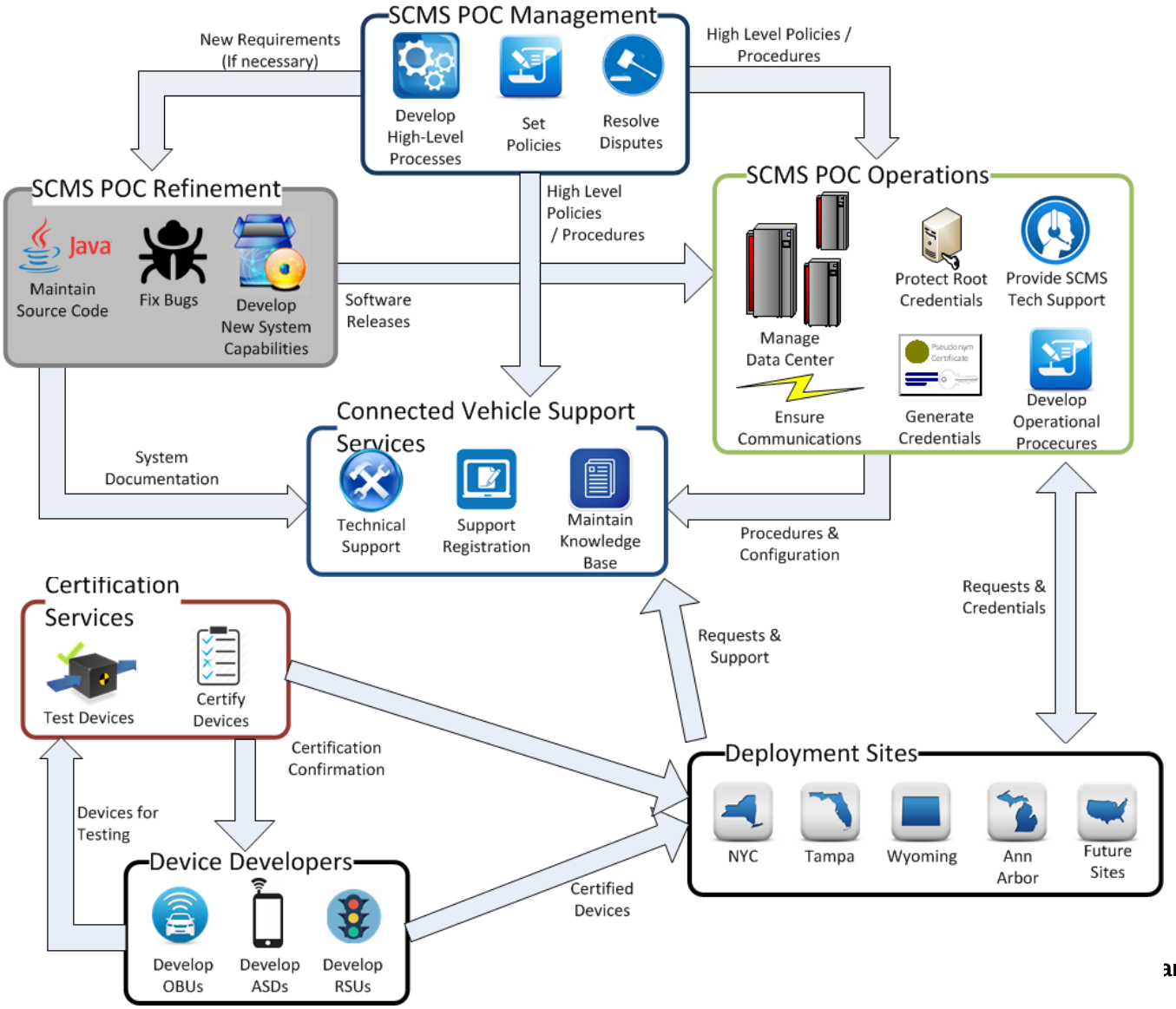
- Alleviate congestion and improve safety during morning commuting hours.
- Deploy a variety of connected vehicle technologies on and in the vicinity of reversible express lanes and three major arterials in downtown Tampa to solve the transportation challenges.

Deployment Schedule

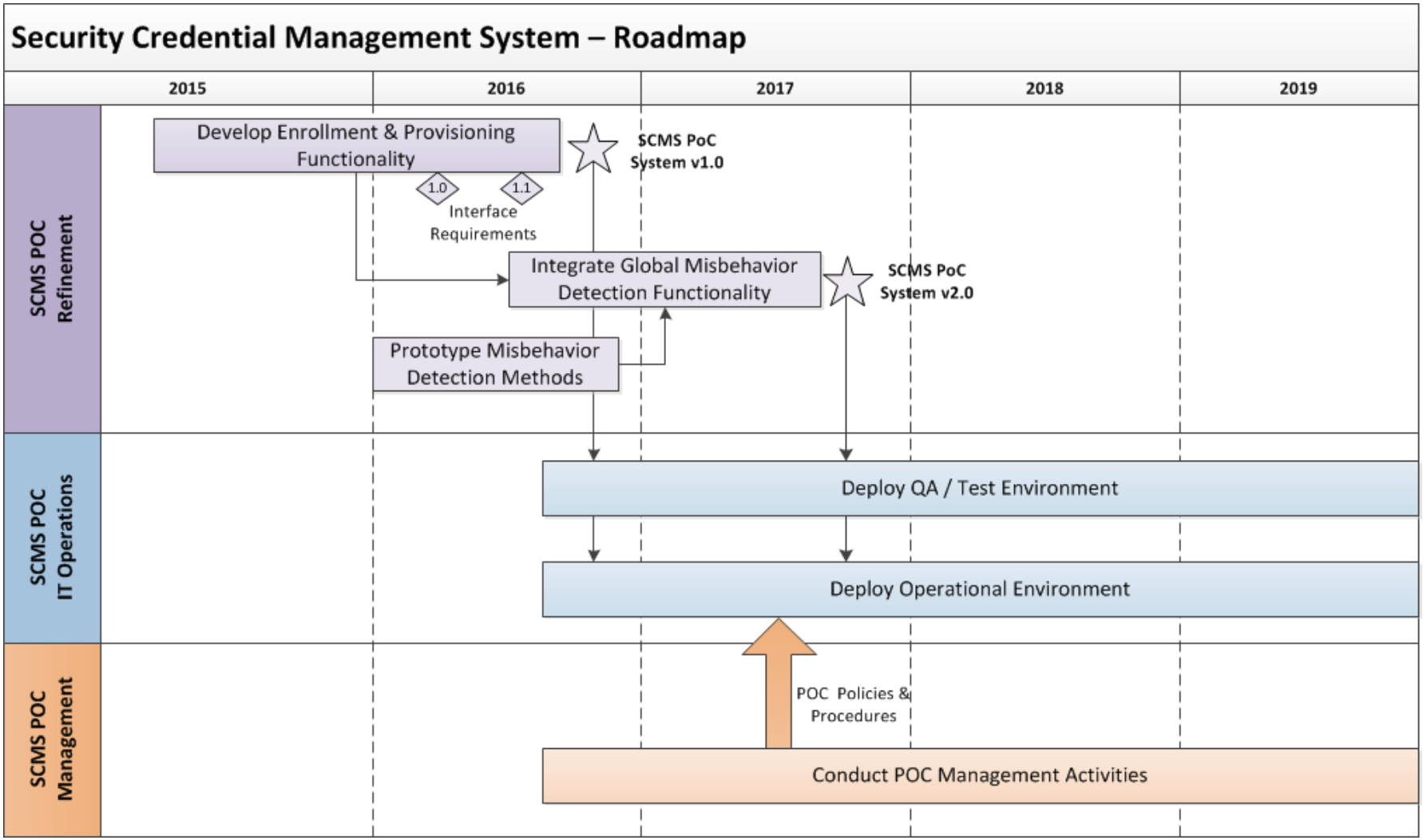


- Overall Deployment Schedule
  - Phase 1: Concept Development
    - Creates the foundational plan to enable further design and deployment
  - Phase 2: Design/Deploy/Test
    - Detailed design and deployment followed by testing to ensure deployment functions as intended (both technically and institutionally)
  - Phase 3: Maintain/Operate
    - Focus is on assessing the performance of the deployed system
  - Post Pilot Operations (CV tech integrated into operational practice)
- Public webinars to share the concept development activities from the three sites
  - Concept of Operations Webinar (February – March 2016)
  - Performance Measurement Webinar (May – June 2016)
  - Deployment Plan Webinar (August 2016)

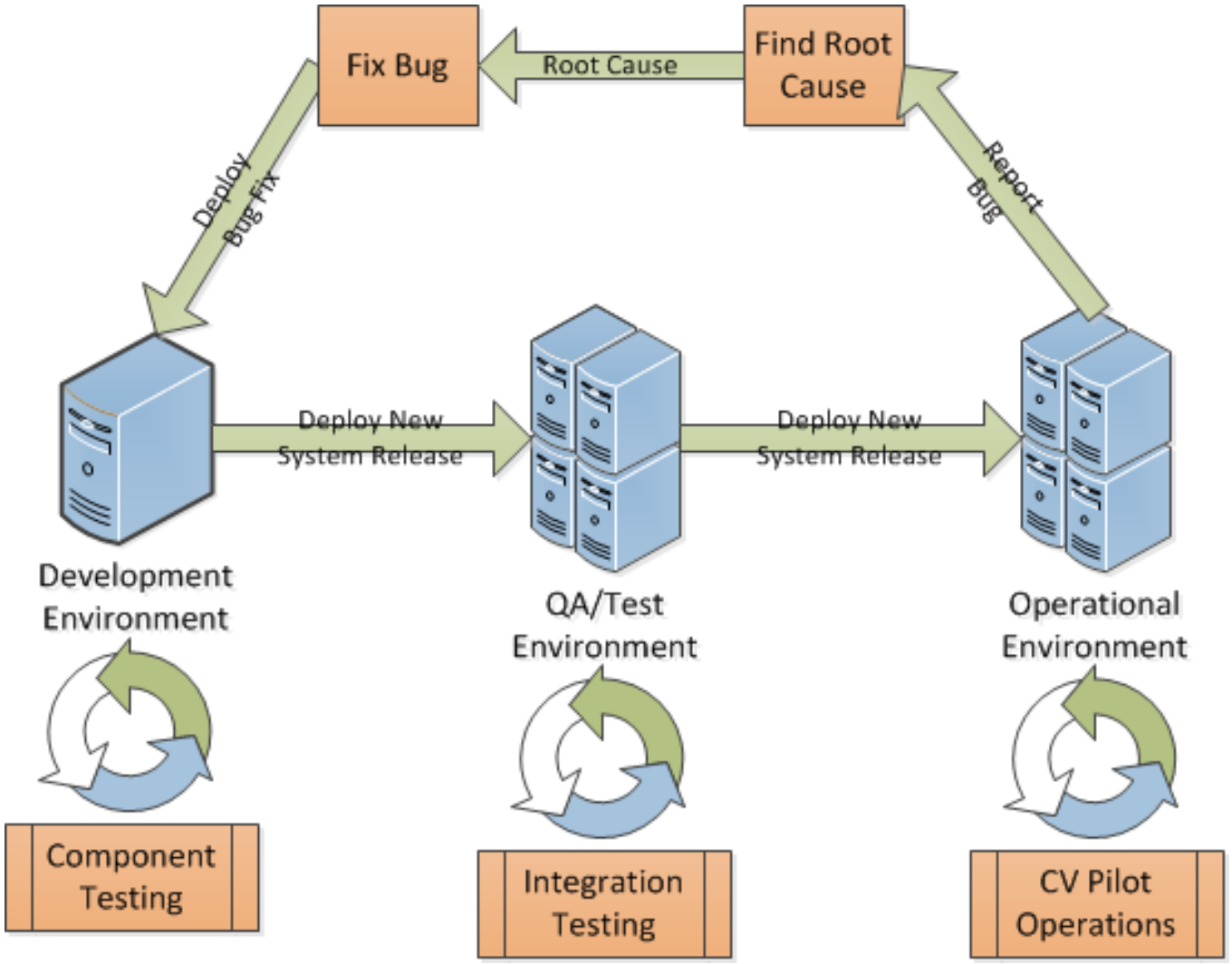
SCMS Management and Operations



SCMS POC Roadmap



SCMS Software Environments

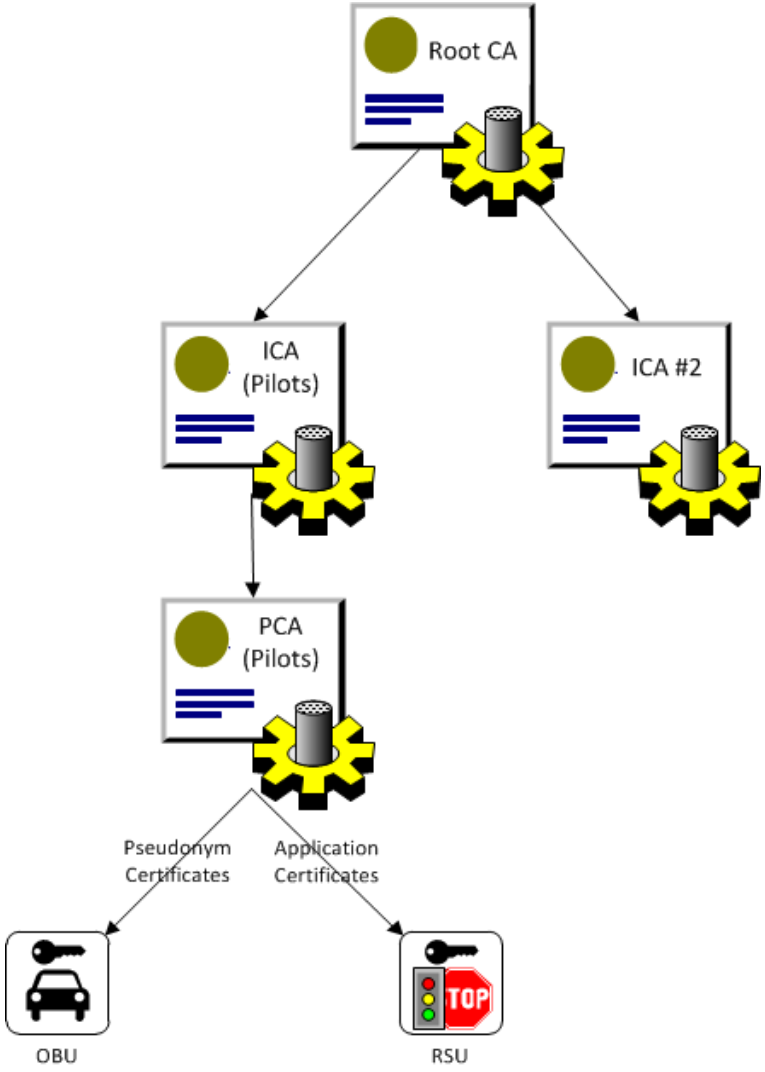


Certificate Authority Hierarchy

- 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

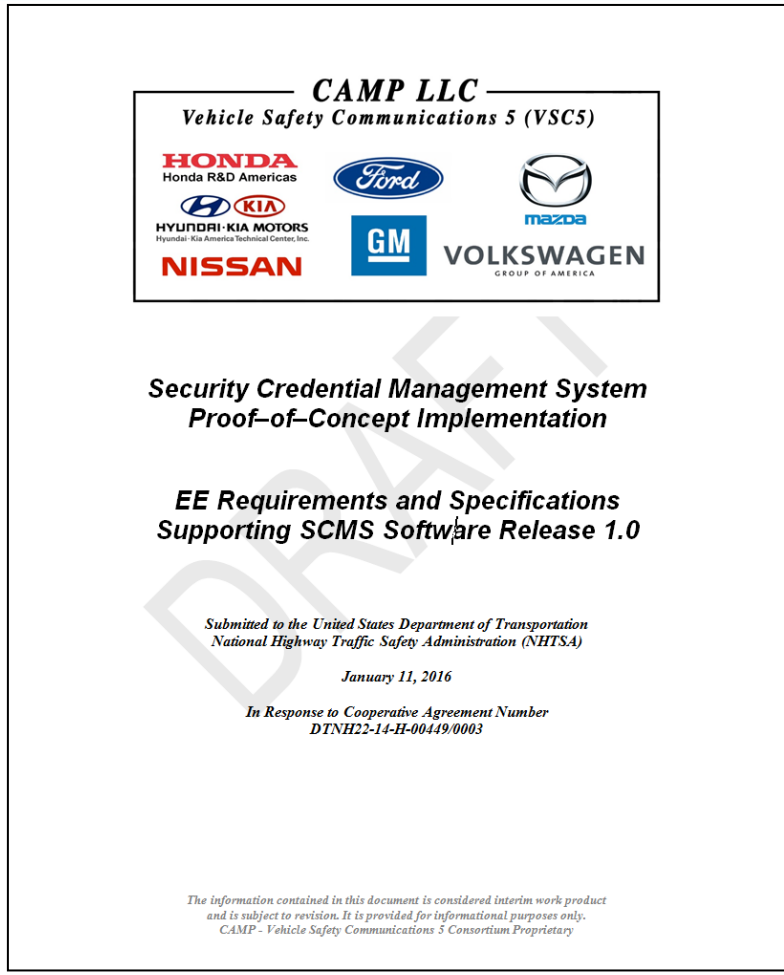


SCMS POC Certificate Types

Issued To	Name	Purpose
OBU / ASD	Enrollment	Initialize the OBU to allow communication with the SCMS
OBU / ASD	Pseudonym	Used to sign all BSMs generated by an OBU
OBU	Authorization	Used to identify public sector vehicles for specific apps
RSU	Enrollment	Initialize the RSU to allow communication with SCMS
RSU	Application	Used to sign application messages generated by RSU (TIM, SPaT, etc.)

EE Requirements and Specification

- Documentation is publicly available
  - Version 1.0 – Released in January 2016
  - Version 1.1 – Scheduled for April 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:
  - https://stash.campllc.org/projects/SCMS/repos/scms-asn/browse/cert-profile.asn?at=refs/heads/master



CAMP LLC

Vehicle Safety Communications 5 (VSC5)

HONDA Honda R&D Americas · Ford · mazda · HYUNDAI·KIA MOTORS Hyundai-Kia America Technical Center, Inc. · GM · VOLKSWAGEN GROUP OF AMERICA · NISSAN

Security Credential Management System
Proof–of–Concept Implementation

EE Requirements and Specifications
Supporting SCMS Software Release 1.0

Submitted to the United States Department of Transportation
National Highway Traffic Safety Administration (NHTSA)

January 11, 2016

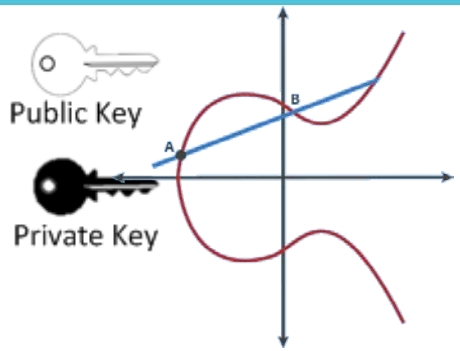
In Response to Cooperative Agreement Number
DTNH22-14-H-00449/0003

DRAFT

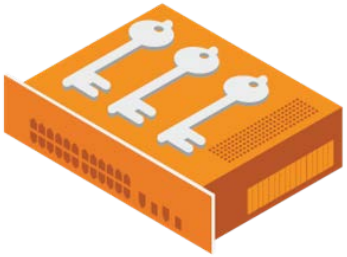
The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

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



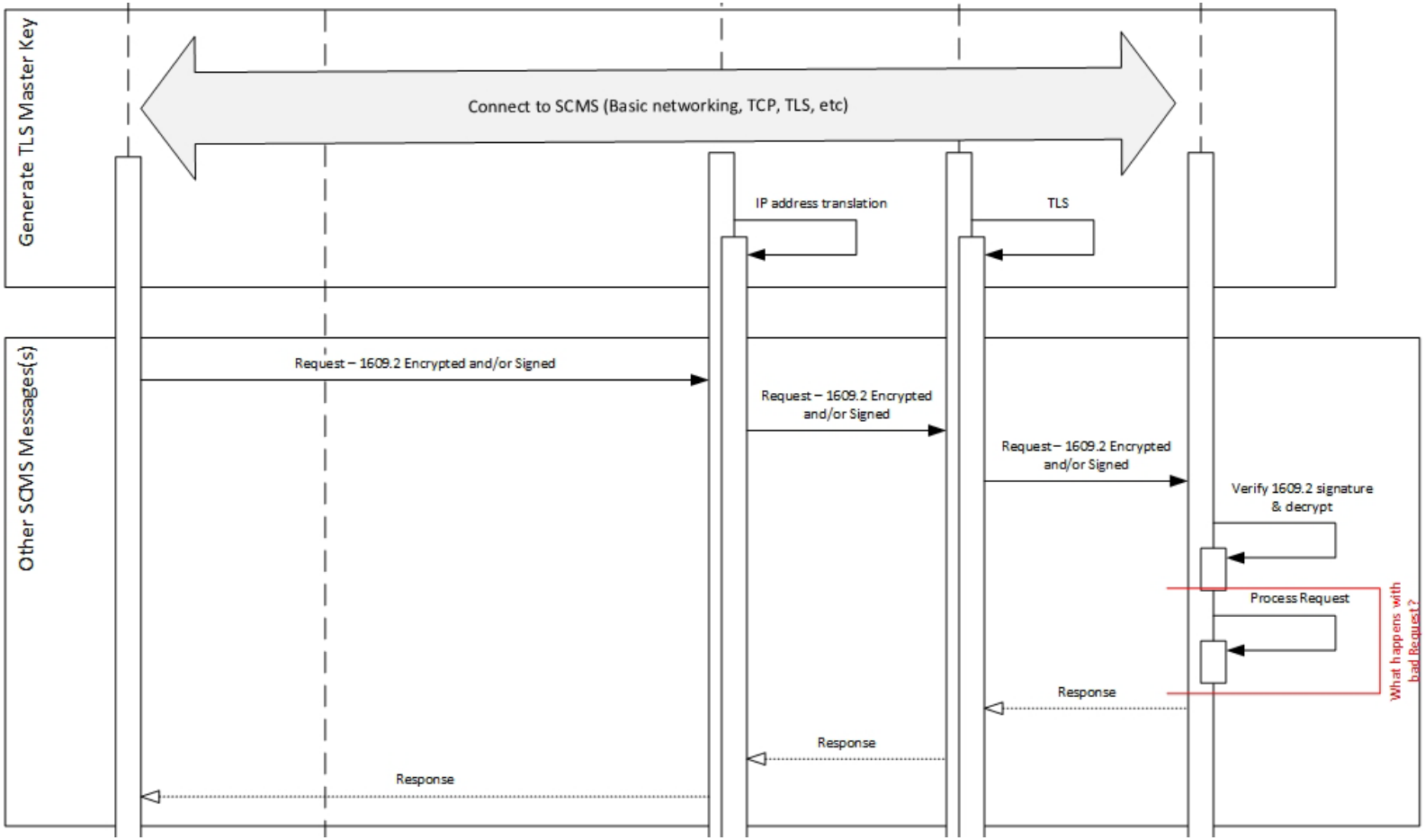
2. Secure Storage of Cryptographic Materials
   - Certificates and private keys need to be stored in secure, tamper evident module in the system
   - Minimum requirements are equivalent to FIPS 140 Level 2
   - Requirements available in 1.1 Release of Interface Documentation



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

HSM image created by SafeNet (http://www.safenet-inc.com/uploadedImages/images/Icons/Hardware-Security-Module-Icon.png)

SCMS Communication Methods



- Common Process for File Download Operations
- Common Process for Sending SCMS Messages

SCMS Communication Methods cont.

- 2.2.3 EE-SCMS Core Communication Requirements (pp16 – 19)
  - Universal SCMS Handshake Processes
  - Common Process for File Download Operations
  - Common Process for Sending SCMS Messages

- 2.3 RA – Services View
  - Provision Pseudonym Certificate Batch
  - Download .info file
  - Download global policy file
  - Download Pseudonym Certificate Batch
  - Retrieve Registration Authority Certificate

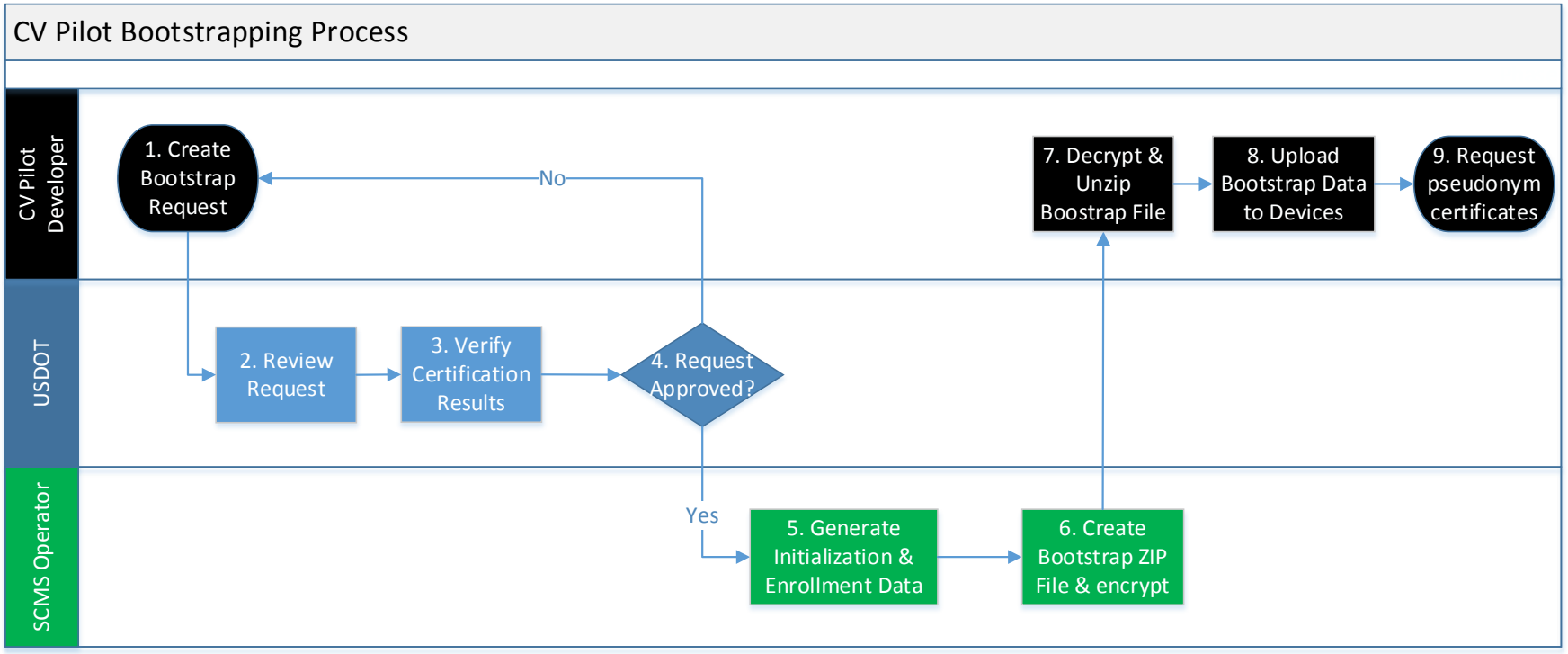
To be extended with release 1.1

On-board Equipment Use Cases

- The following are the main use cases for OBE's
  - Use Case 2: Bootstrapping
  - Use Case 3: Initial Provisioning of Pseudonym Certificates
  - Use Case 5: Misbehavior Reporting
  - Use Case 6: CRL Download
  - Use Case 8: OBE Revocation
  - Use Case 9: Refresh Pseudonym Certificates
  - Use Case 10: Update Pseudonym Certificate Request Parameters

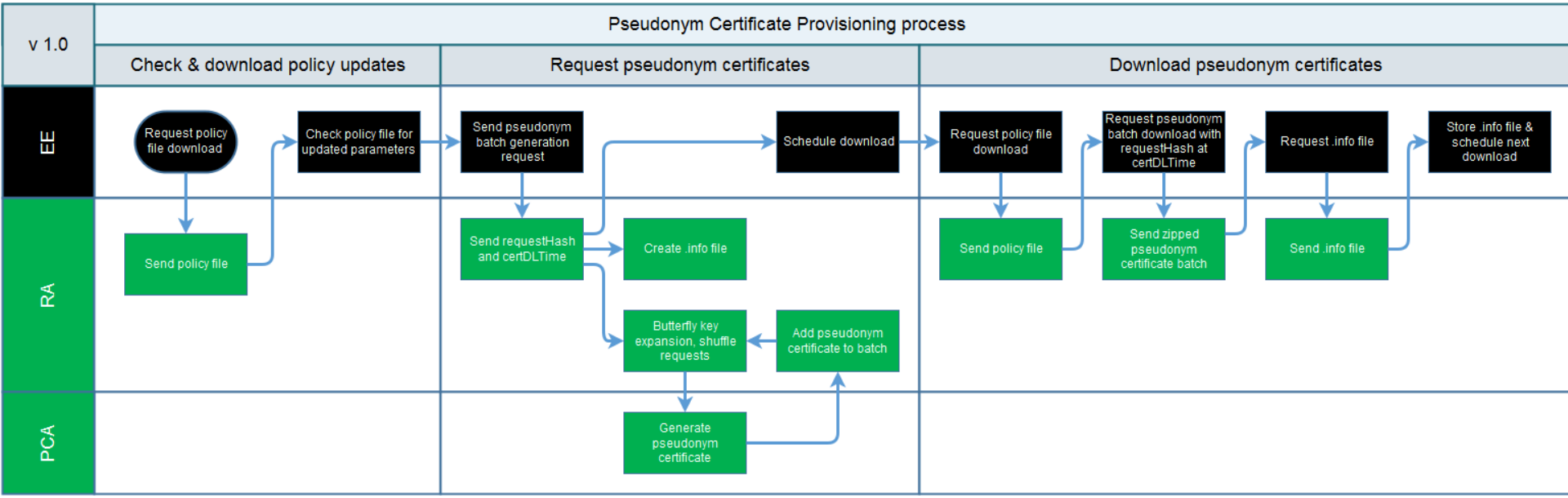
UC 2: Bootstrapping

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



UC 3: Initial Provisioning of 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



UC 3: Initial Provisioning of Pseudonym Certificates

PATH	/provision-pseudonym-certificate-batch
HTTP Method	POST
HTTP Request Body	ASN1 serialized SecuredPseudonymCertProvisioningRequest
HTTP Response Body	SecuredPseudonymCertProvisioningAck with a *requestHash* property containing the lower 8 bytes of the request hash. This value will identify this device from this point on, and it is to be used in subsequent download calls. The *reply* property contains a *PseudonymCertProvisioningAck* with a *certDLTime* property containing the expected time of the requested batch, and a *certDLURL* property containing the URL where the batch can be downloaded from.

Roadside Equipment Use Cases

- The following chapters are about RSE requirements:
  - Use Case 12: RSE Bootstrapping
  - Use Case 13: RSE Application Certificate Provisioning
  - Use Case 14: RSE Misbehavior Reporting
  - Use Case 15: RSE CRL Check
  - Use Case 16: RSE Application and OBE Identification Certificate Revocation
  - Use Case 17: Refresh RSE Application Certificates

Provider Service Identifiers

- Provider Service Identifiers (PSIDs) & SCMS
  - PSID values are included in the security certificates generated by the SCMS
  - PSID values indicate which applications a message is authorized to support
  - PSIDs are described in IEEE1609 standards

- Existing PSIDs to support CV Pilot applications
  - Basic Safety Message – 0x20
  - SPaT & MAP – 0x8002

- Additional PSIDs are needed for V2I CV Pilot applications
  - Speed Harmonization
  - Basic Information Message
  - Traffic Signal Pre-emption / Priority

Applications Supported by PSID

SPaT & MAP
Red Light Violation Warning
Pedestrian in Signalized Crosswalk Warning
Mobile Accessible Pedestrian Signal System

Basic Safety Message
Probe Enabled Traffic Monitoring
Intelligent Traffic Signal System In-Vehicle Information Potential
Vehicle Turning Right in Front of Bus Warning
Forward Collision Warning
Emergency Electronic Brake Light
Blind Spot Warning
Lane Change Warning / Assist
Intersection Movement Assist
Stationary Vehicle Ahead
Do Not Pass Warning

Traffic Signal Preemption
Transit Signal Priority / Special Vehicles

Speed Harmonization
Modified Eco-Speed Harmonization
Speed Harmonization

Basic Information Message
Curve Speed Warning
Reduced Speed / Work Zone
Spot Specific Weather Warning
Variable Speed Limits
Work Zone Alerts
Truck Restrictions

Stakeholder Q&A

- Please keep your phone muted
- Please use chatbox to ask questions
- Questions will be answered in the order in which they were received
- This Q&A section will not be recorded, nor posted to the website

STAY CONNECTED

Contact for CV Pilots Program:

Kate Hartman, Program Manager

Kate.hartman@dot.gov

Join us for the *Getting Ready for Deployment* Series

- Discover more about the 2015 CV Pilot Sites
- Learn the Essential Steps to CV Deployment
- Engage in Technical Discussion

Website: http://www.its.dot.gov/pilots

Twitter: @ITSJPODirector

Facebook: https://www.facebook.com/DOTRITA

February 2016 Webinars

Technical Assistance Webinars

- 2/1/2016, 11:00 – 12:30 pm EST
  Preparing a Privacy Concept for Connected Vehicle Deployments
- 2/9/2016, 2:00 – 3:00 pm EST
  Preparing a Performance Measurement Plan for Connected Vehicle Deployments
- 2/10/2016, 2:30 – 4:00 pm EST
  SCMS Proof-of-Concept Interface Requirements for Connected Vehicle Deployments

Public ConOps Webinars

- 2/5/2016, 1:00 – 2:00 pm EST: ICF/Wyoming
- 2/8/2016, 2:00 – 3:00 pm EST: Tampa (THEA)

Please visit the CV pilots website for the recording and the briefing material of the previous webinars.