CONNECTED VEHICLE PILOT
Deployment Program

Preparing a Security Operational Concept for Connected Vehicle Deployments

Kevin W. Gay, Program Manager, NHTSA

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
  - Security Operating Concept
  - 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

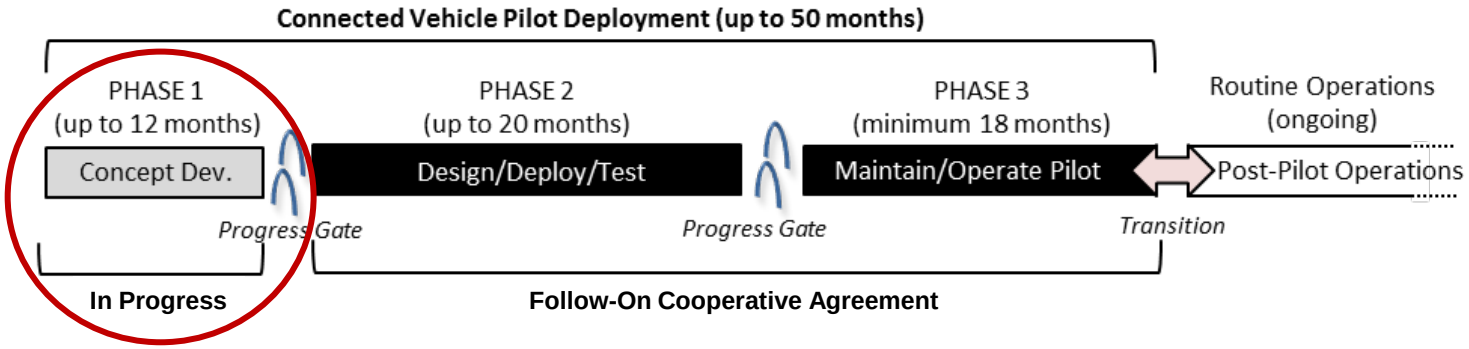
Sites Selected – 2015 Awards

- 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)

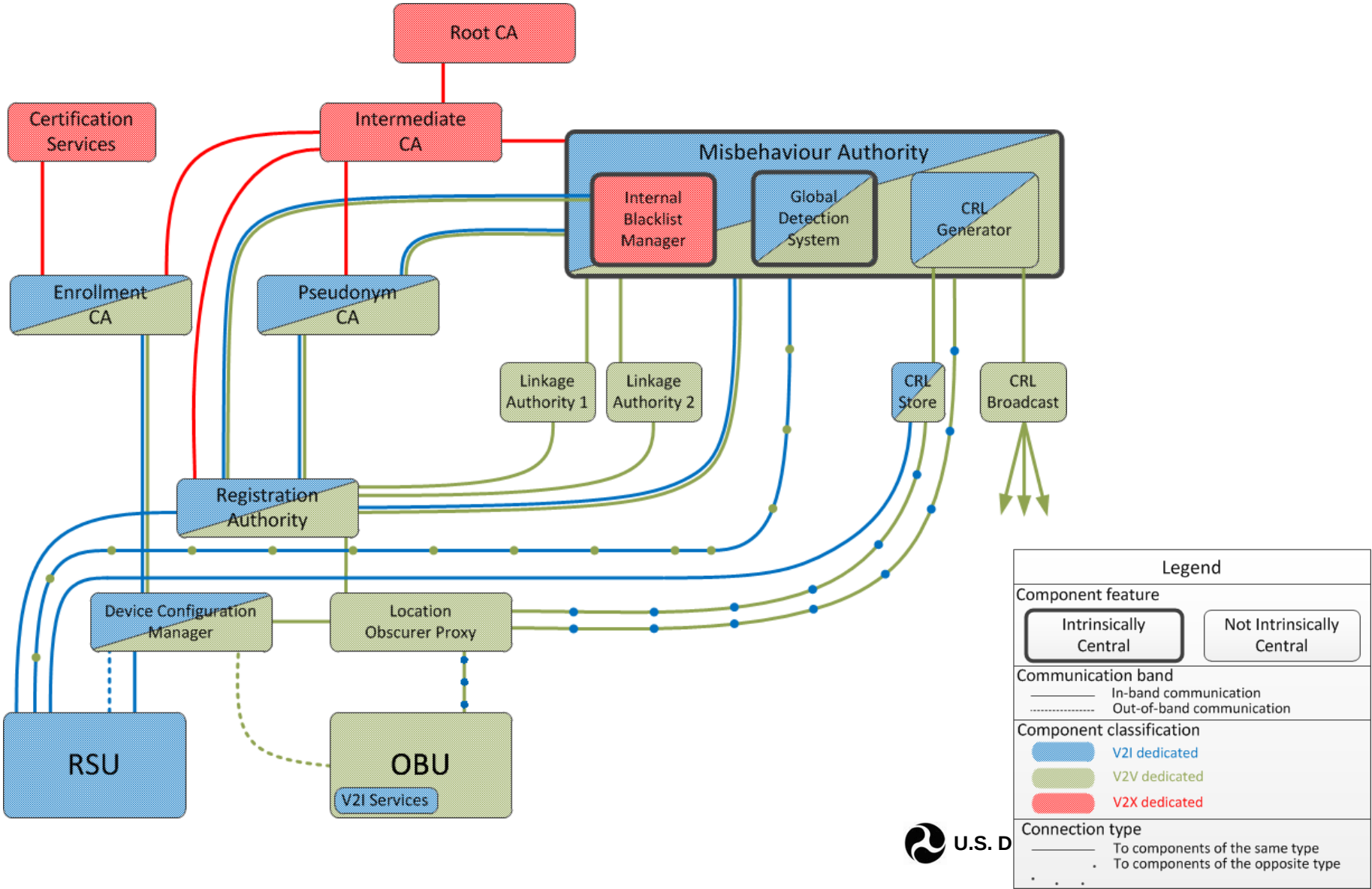
Security Concept Overview

- Communications Security
  - SCMS Overview
  - System Use Cases
  - Development, Operations, and Management
- Access Security
- Physical Security

Need for Communications Security

- Vehicle and infrastructures messages must be trusted for the system to work. That is, vehicles receiving the messages must have confidence that messages are:
  - Real (genuine); from a vehicle or infrastructure device in proximity
  - Convey accurate data about the vehicle or infrastructure
- Overall confidence in the system could erode if “fake”, altered, and/or misleading messages are broadcast – leading to false (+ / –) warnings
- Therefore…CV Systems need:
  - Method to validate the original sender of the message is trusted (authenticity)
  - Method to prevent the messages from being spoofed or altered (integrity)
- …AND, this security must be delivered without compromising privacy of end users.

Security Credential Management System (SCMS)



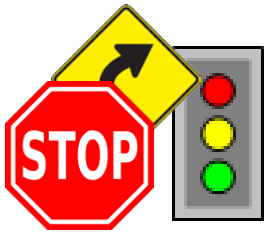
U.S. D

V2X Public Key Infrastructure Overview

Common entity in chain of trust

Other Vehicles & infrastructure

Exchange Messages



Infrastructure **Vehicle**

1. Device generates private, public key-pair

Private Key

Public Key

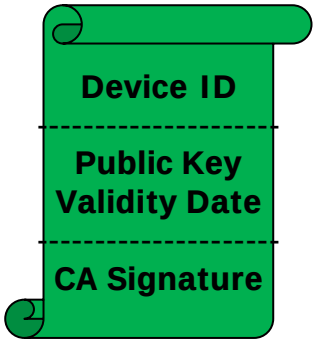
Public Key

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

Certificate Authority

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

4. CA sends certificate back to device



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.)

SCMS Use Cases

1. Bootstrapping
2. Provisioning of Certificates
3. Misbehavior Detection
4. Certificate Revocation List Distribution

Bootstrapping

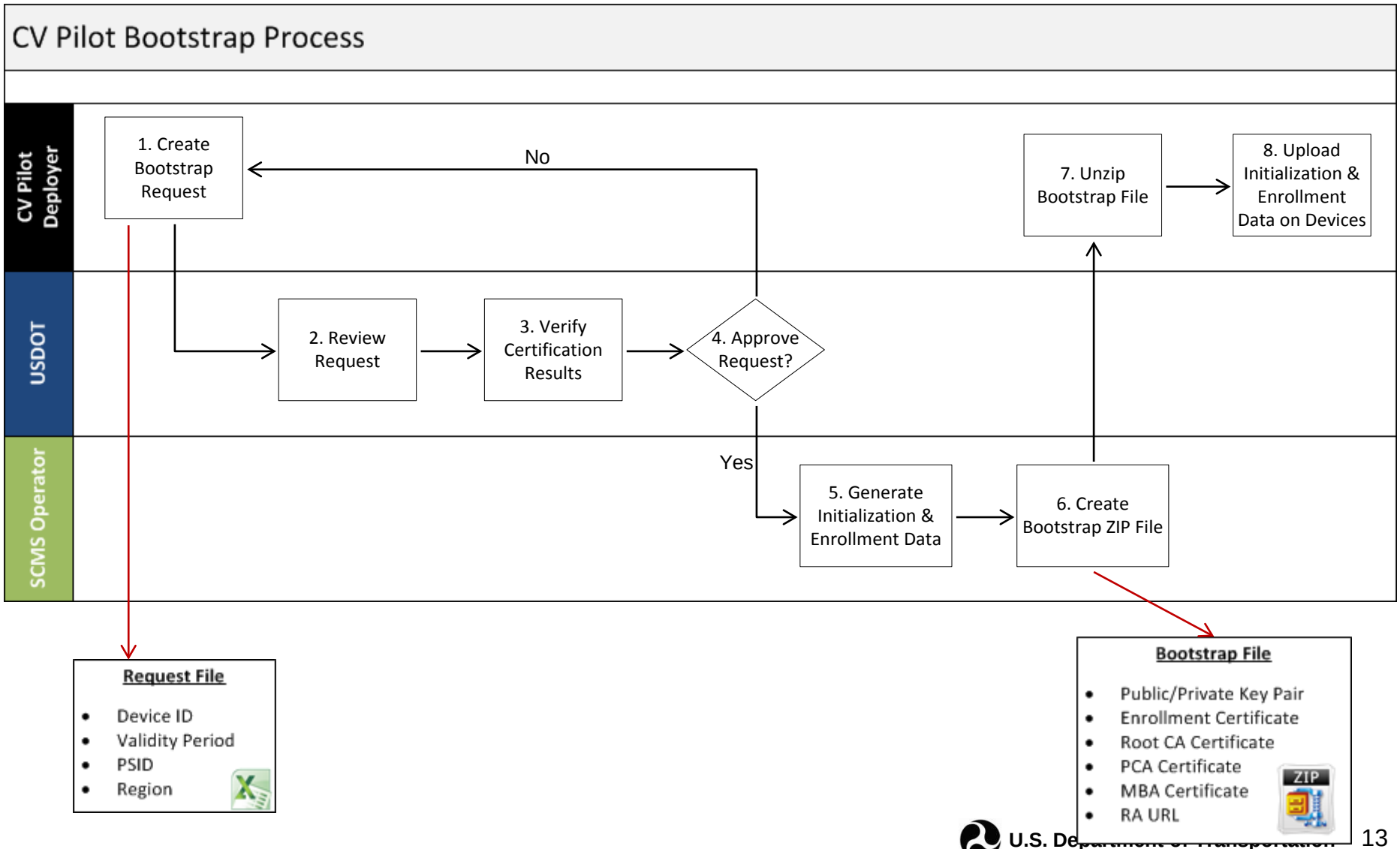
- Initially a device has no certificates and no knowledge of how to contact SCMS

- Composed of two operations:
  - **Initialization** – SCMS component certificates and contact info (URLs) transmitted to device

  - **Enrollment** – Device receives a long-term certificate (40 years) that authorizes communication with SCMS

- Process must protect device from receiving incorrect information
- Process must prevent SCMS from issuing certificates to unauthorized devices

Proposed CV Pilot Process



Pseudonym Certificates

- Issued by in-vehicle devices transmitting Basic Safety Messages (BSMs)
  - ASDs, VADs, and OBUs
- Each certificate is valid for 1 week
- 20 certificates are valid simultaneously
- Rotate the pseudonym certificate used to sign BSMs every 5 minutes
- Initial provisioning process will provide certificates for 3 years of operations
  - 3,120 total
- Devices replenish certificates periodically

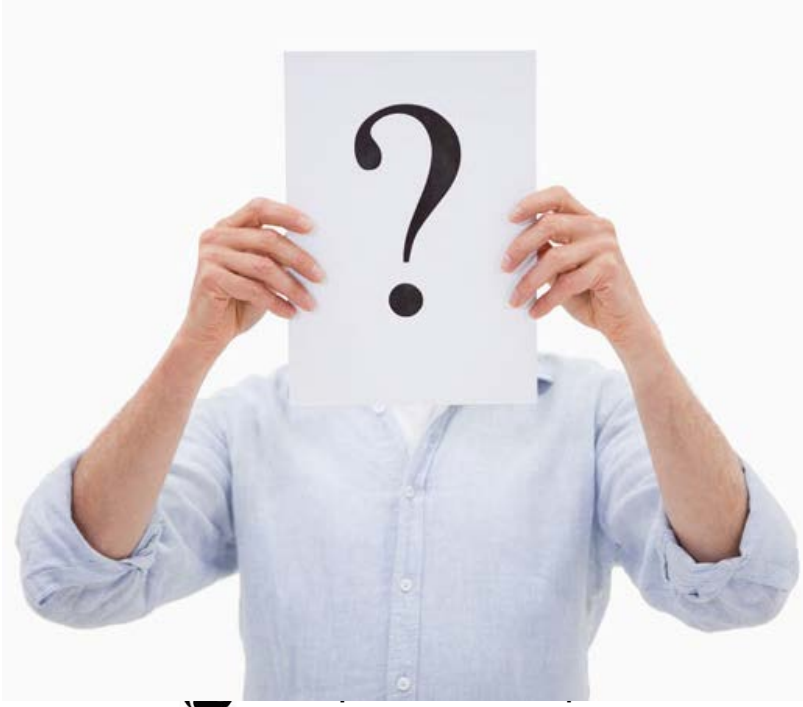
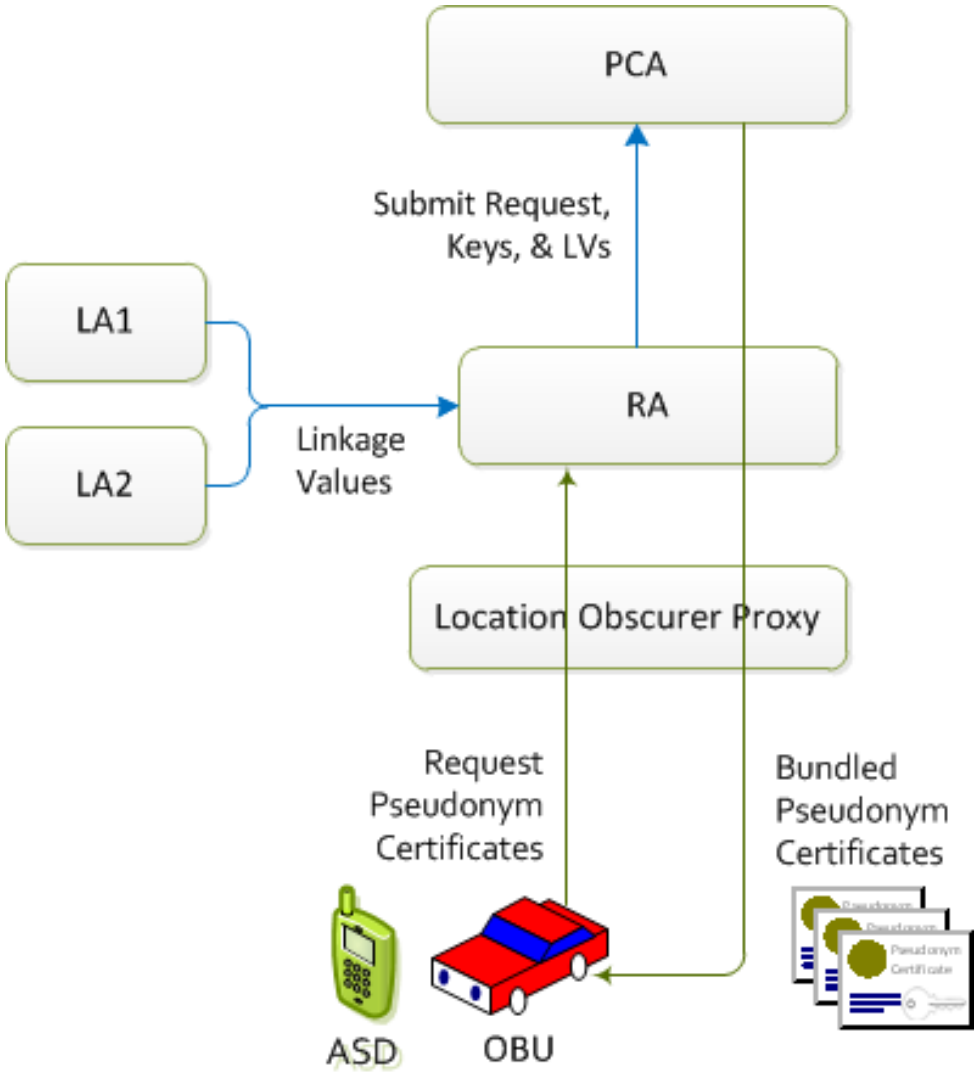


Photo Source: Barnes and Nobles / Joel Cunningham

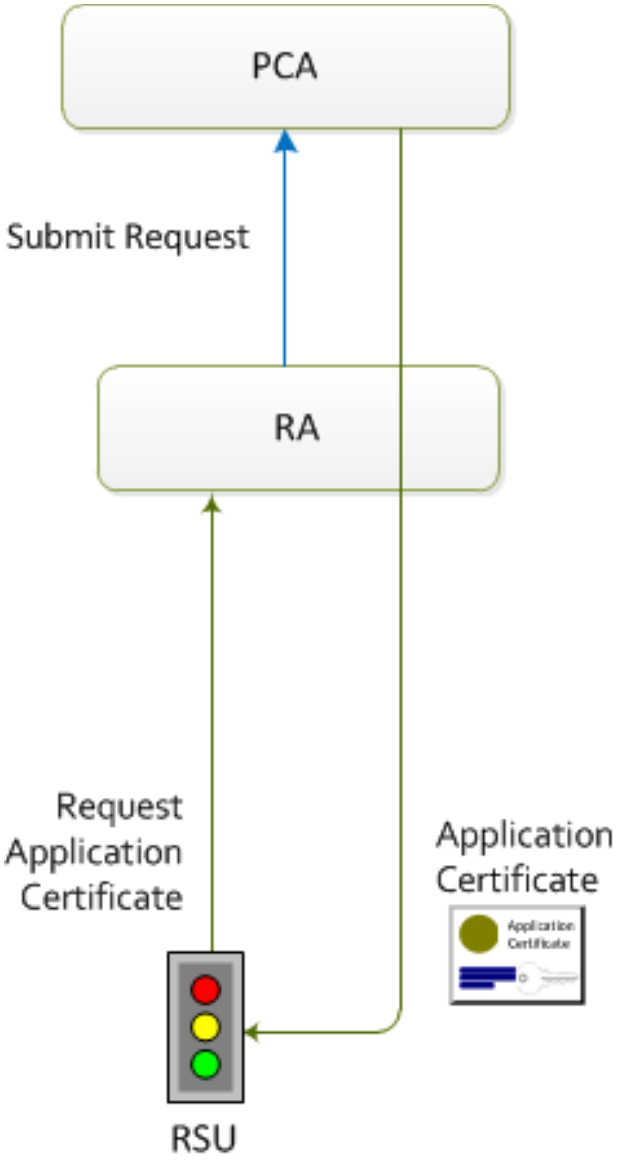
Pseudonym Certificate Request

1. Device generates request, includes
   - ECC Butterfly Seed Pair
   - Current Time
   - Start & End Time for Certs
2. Device signs the request with Enrollment Certificate
3. Device encrypts the signed message with the RA certificate
4. SCMS generates pseudonym certificates
5. RA transmits the bundled certificates back to the device.

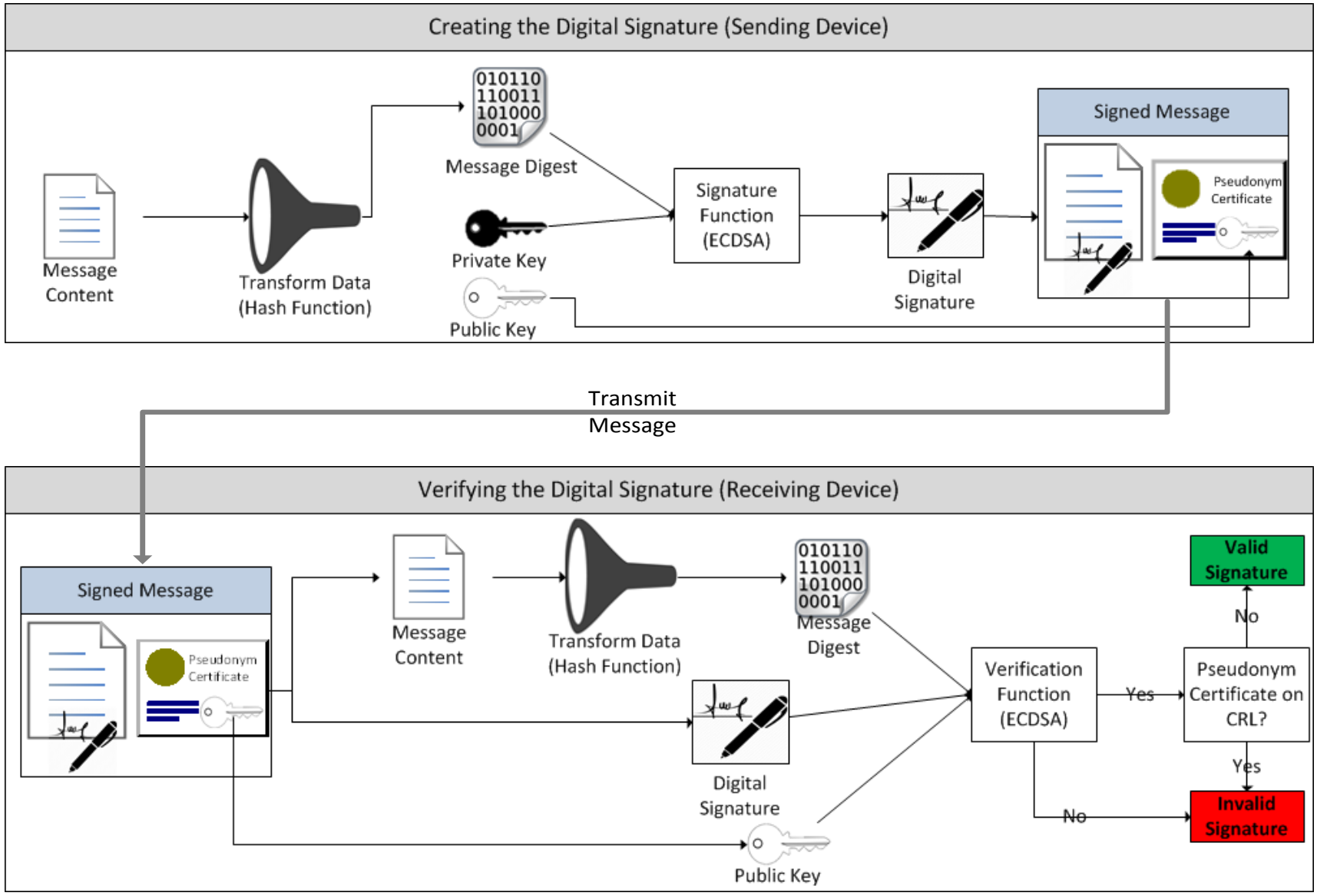


Application Certificates

- Issued by devices transmitting infrastructure messages (TIM, SpaT, MAP, etc.)
- Each certificate is valid for a short period of time (i.e. weeks)
- RSU will request new application certificates periodically
- No need for the privacy offered by pseudonym certificates

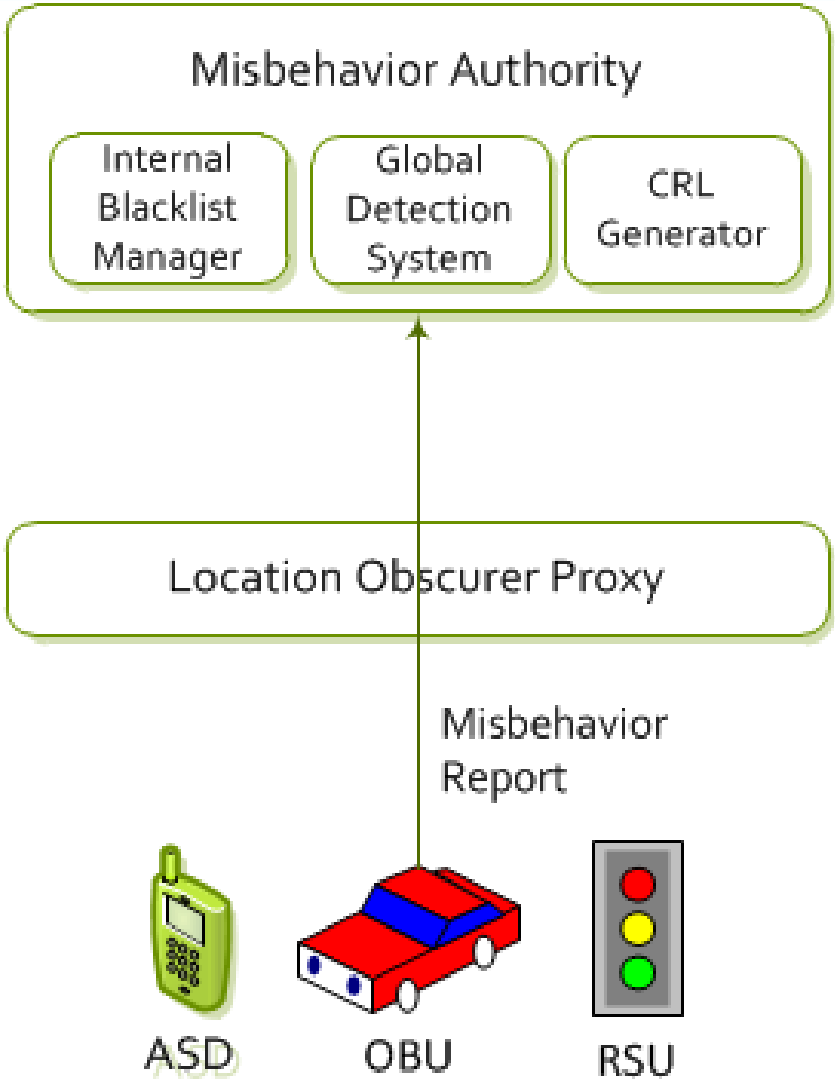


Message Signing



Misbehavior Reporting

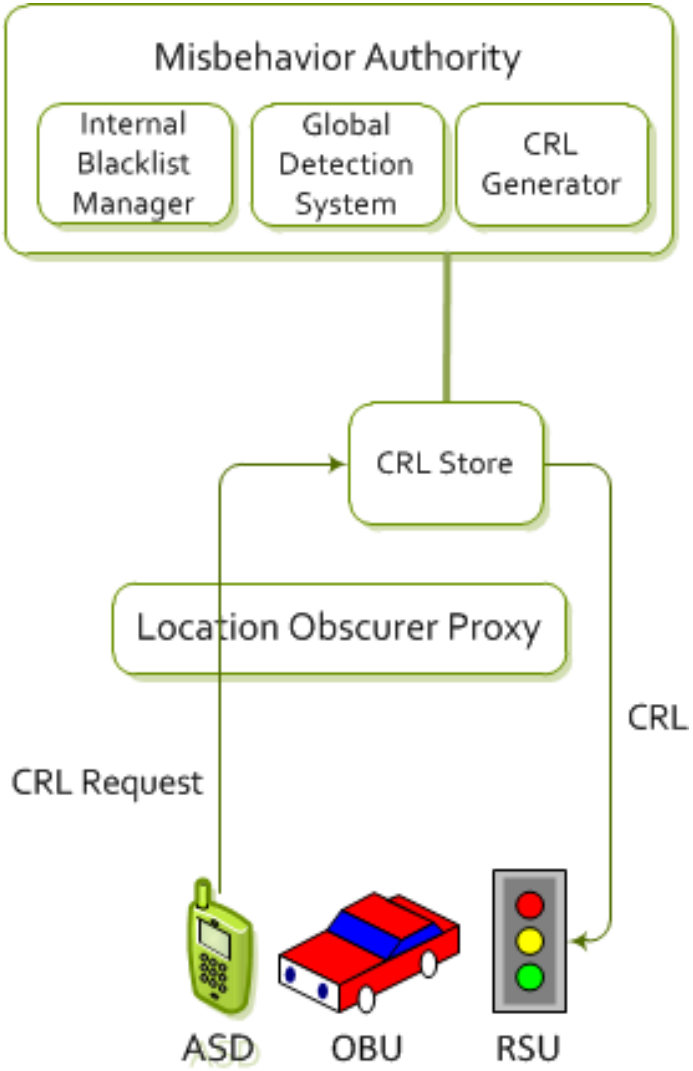
1. Device identifies potential misbehavior based on local misbehavior detection algorithms
2. Device creates misbehavior report, encrypts it, and sends to LOP
3. LOP removes any identifies from the encrypted misbehavior report and forwards to the MA
4. Global Detection System processes the misbehavior report and determines what action to take (if any) against the reported device



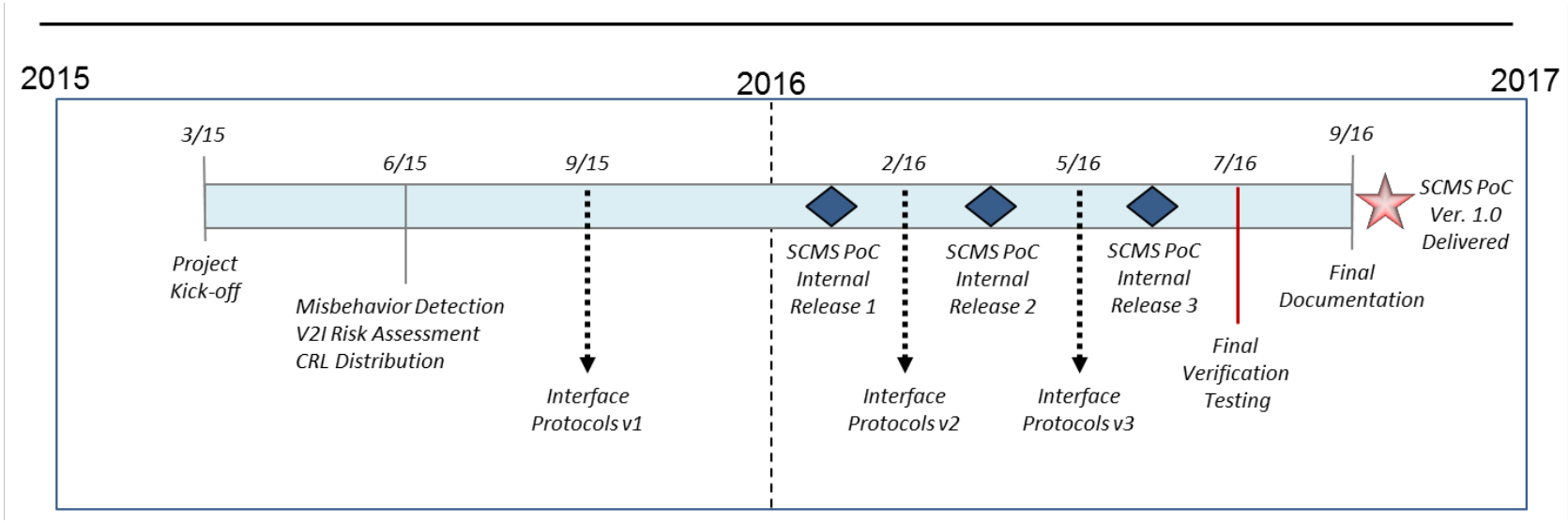
Certificate Revocation List Distribution

1. Device sends a request for a CRL to the CRL Store
2. CRL Store responds with the most current CRL

NOTE: Maximum of 10,000 entries (40 bytes each) in the CRL

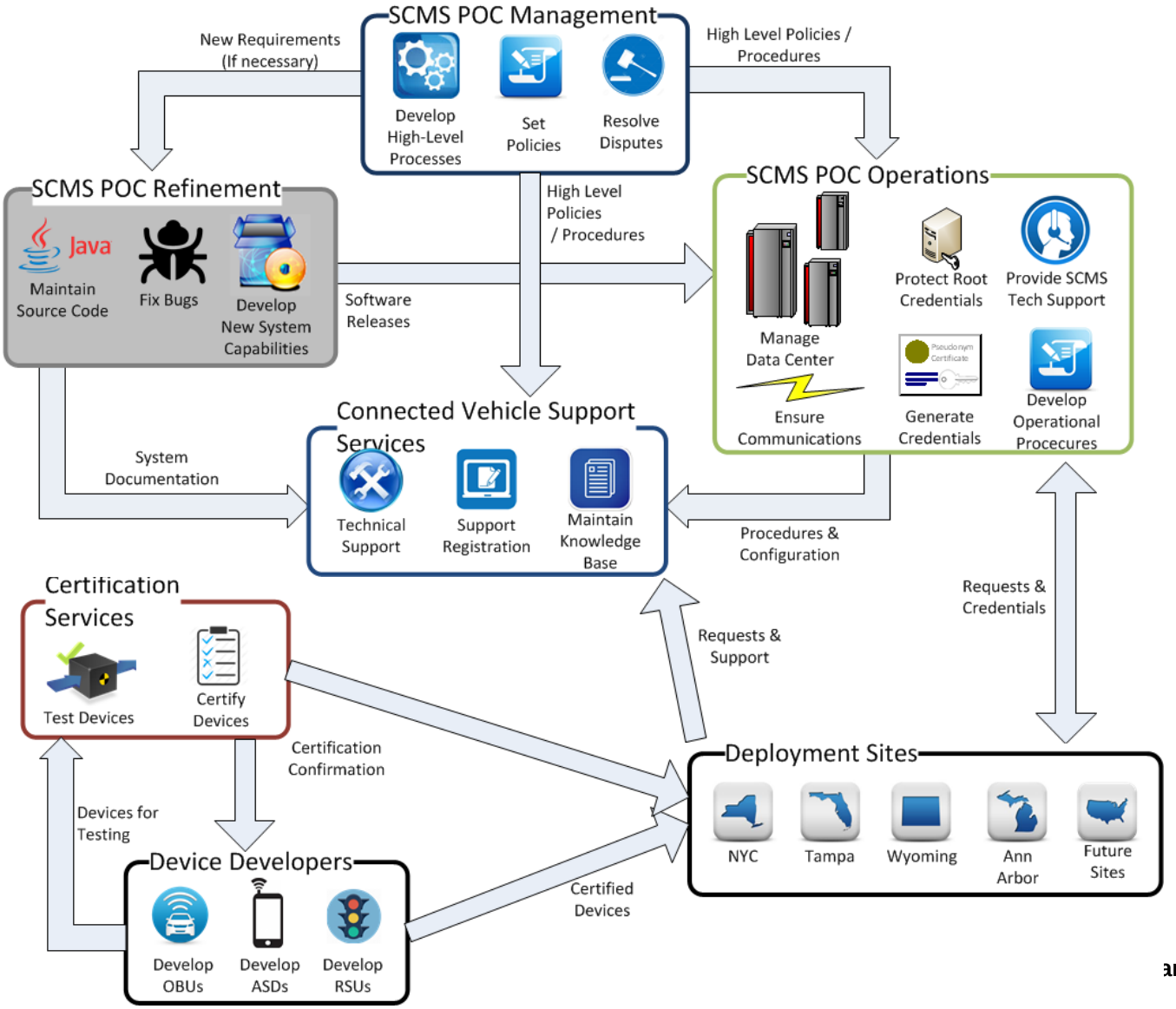


SCMS POC – Development Schedule



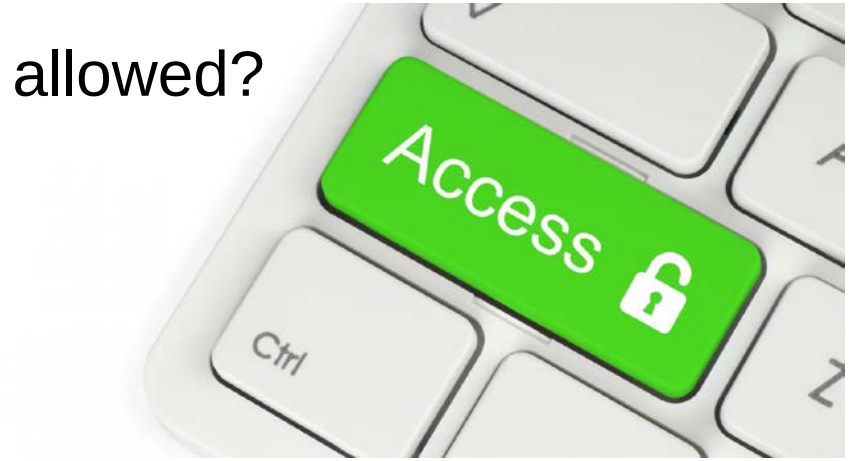
- 3 Internal SCMS Releases for Testing/Auditing Purposes
  - Feb 2016, March, 2016, and June 2016
- SCMS PoC Version 1.0 Delivered by September 2016
  - Does not include Misbehavior Authority
- Final Documentation Delivered at Project End
  - Includes requirements, design, test, and code

SCMS Management and Operations



Access Security

- How are the security materials stored internally?
- Which users are allowed to access to the device?
- What are the user name and password policies for authorized users?
- Is remote access to the device allowed?



Physical Security

- What protections are being utilized to prevent tampering with device?

- Tamper evident protections?
  - Seals?
  - Tape?

- Tamper resistant protections?
  - Specialized screws/keys
  - Software protections

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

Join us for the *Getting Ready for Deployment* Series

- Discover more about the Wave 1 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

Contact for CV Pilots Program:

Kate Hartman, Program Manager

Kate.hartman@dot.gov

December 2015 Technical Assistance Webinars:

- 12/7/2015, 2:00 – 3:30 pm EST
  Preparing a Safety Management Plan for Connected Vehicle Deployments
- 12/9/2015, 1:30 – 3:00 pm EST
  Preparing a Security Concept for Connected Vehicle Deployments
- 12/10/2015, 12:30 – 2:00 pm EST
  Preparing Institutional/Business Models and Financial Sustainability for Connected Vehicle Deployments

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