Security Credential Management System – Operations and Management

Kevin Gay, ITS Joint Program Office
Chief – ITS Policy, Architecture and Knowledge Transfer

Vehicle-to-Vehicle Communications

SAE J2735/J2945.1 Basic Safety Message:

Information Transmitted
Random Vehicle ID, Sequence #, Time Stamp, Position (latitude, longitude, elevation, accuracy),
Motion (speed, transmission state, heading angle, brake, accel /decel),
Control (yaw rate), &
Vehicle Size (length, width)

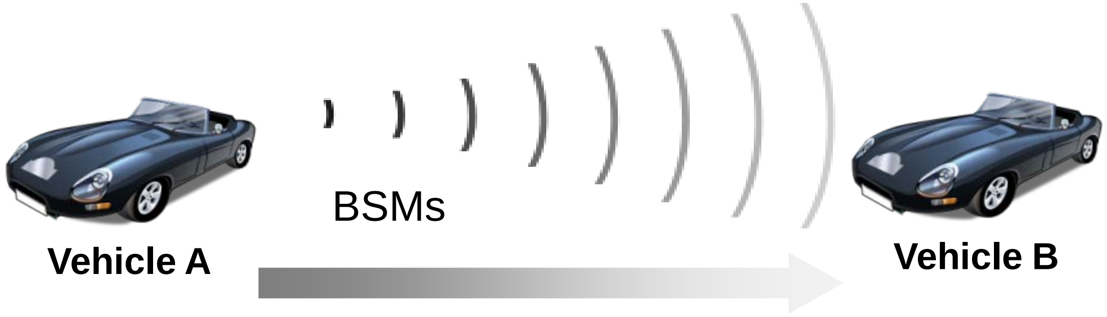
+

Security Credentials

DSRC = Dedicated Short Range Communication

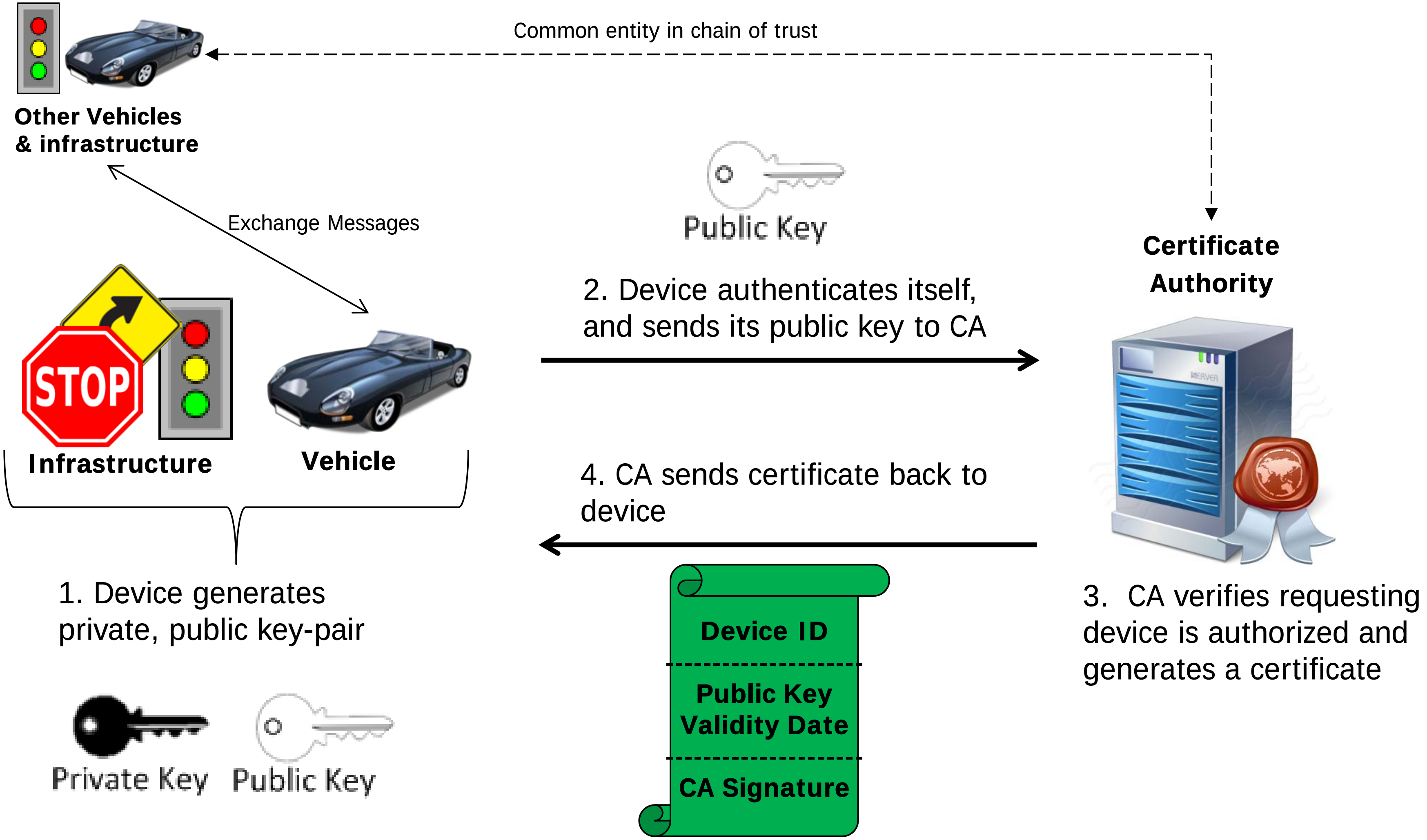
V2V: vehicles exchange BSMs with security credentials

Basic Safety Message Structure



Basic Safety Message			
Message Content	**Digital Signature**	**Pseudonym Certificate**	**Timestamp**
• Speed • Position • Heading • Acceleration	• 64 byte number created with the private key of an associated pseudonym certificate issued by CA	• Public key that corresponds to the private key used for signature • Validity interval • CA signature	• Date / Time in UTC

V2X Public Key Infrastructure Overview



Common entity in chain of trust

Other Vehicles
& infrastructure

Exchange Messages

Public Key

Certificate Authority

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

Infrastructure

Vehicle

4. CA sends certificate back to device

1. Device generates private, public key-pair

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

Private Key

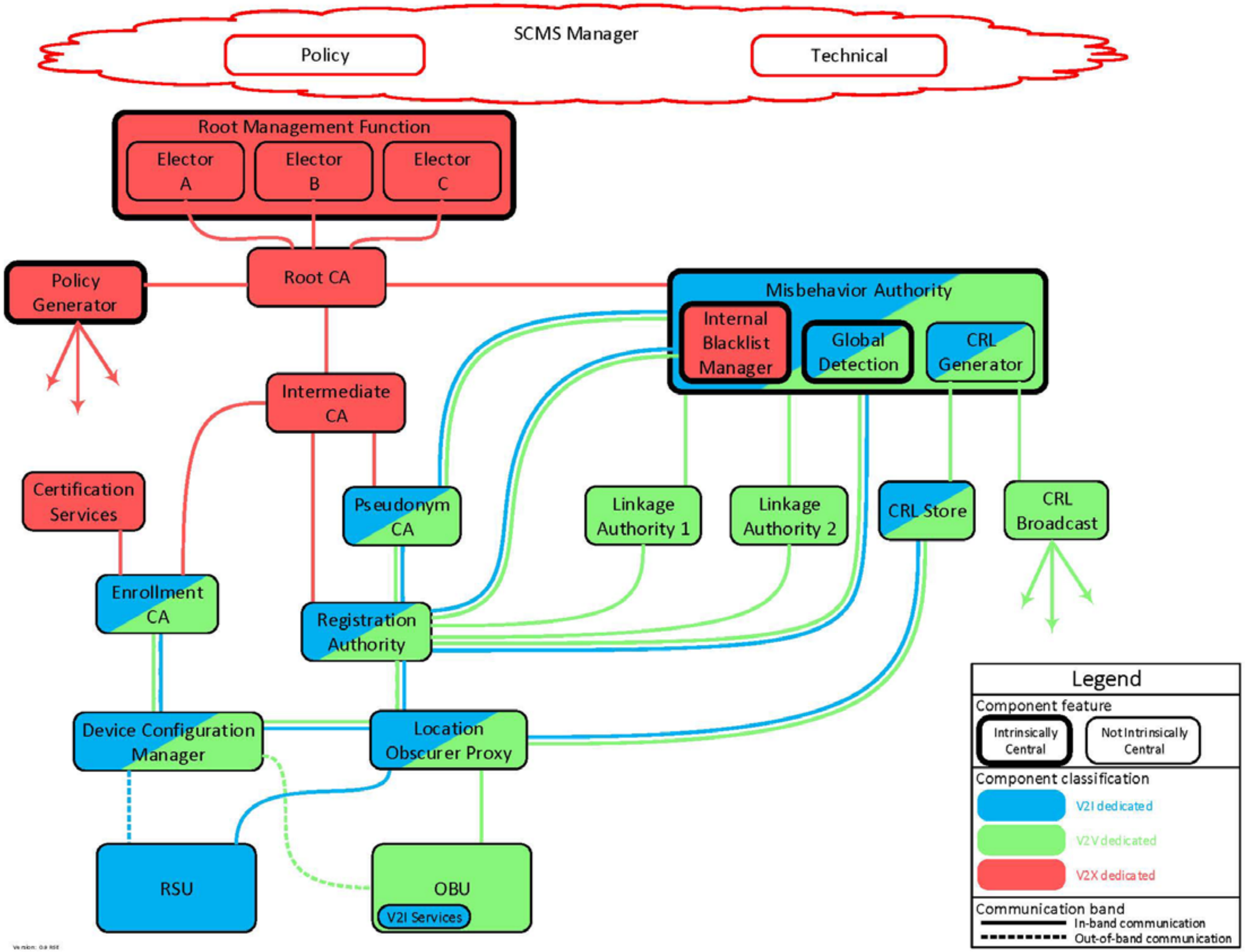
Public Key

Device ID

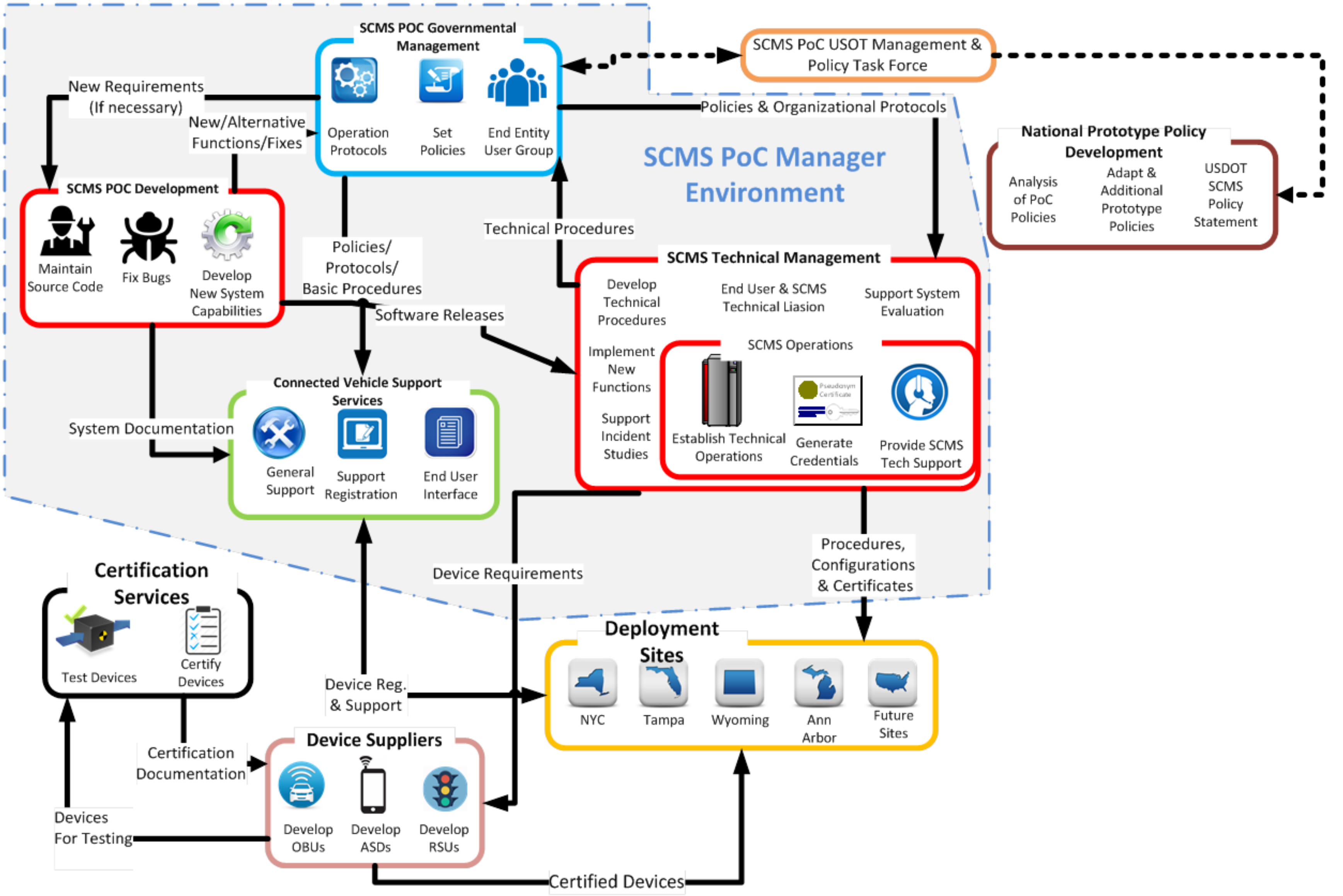
Public Key
Validity Date

CA Signature

V2X SCMS Architecture

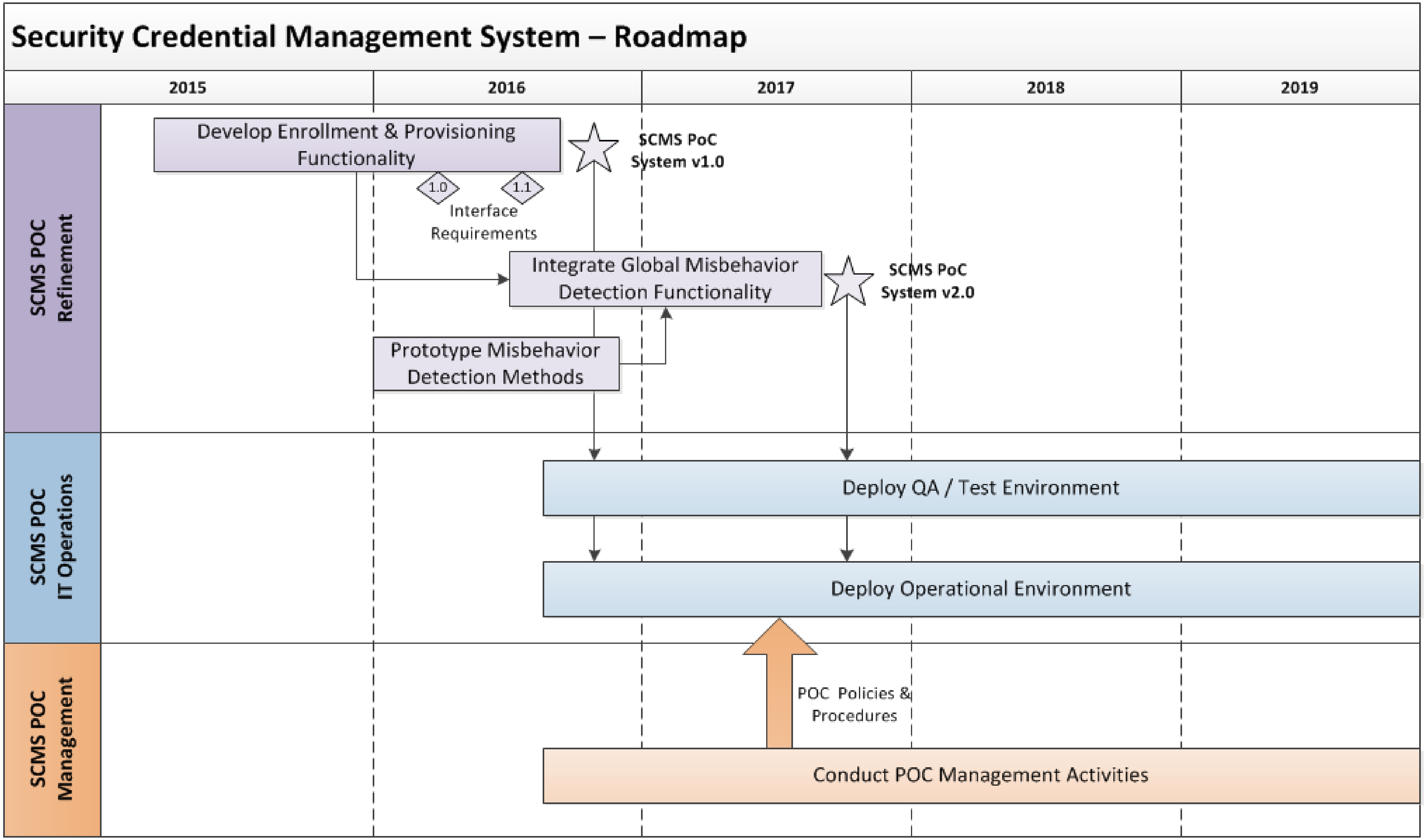


SCMS Management and Operations

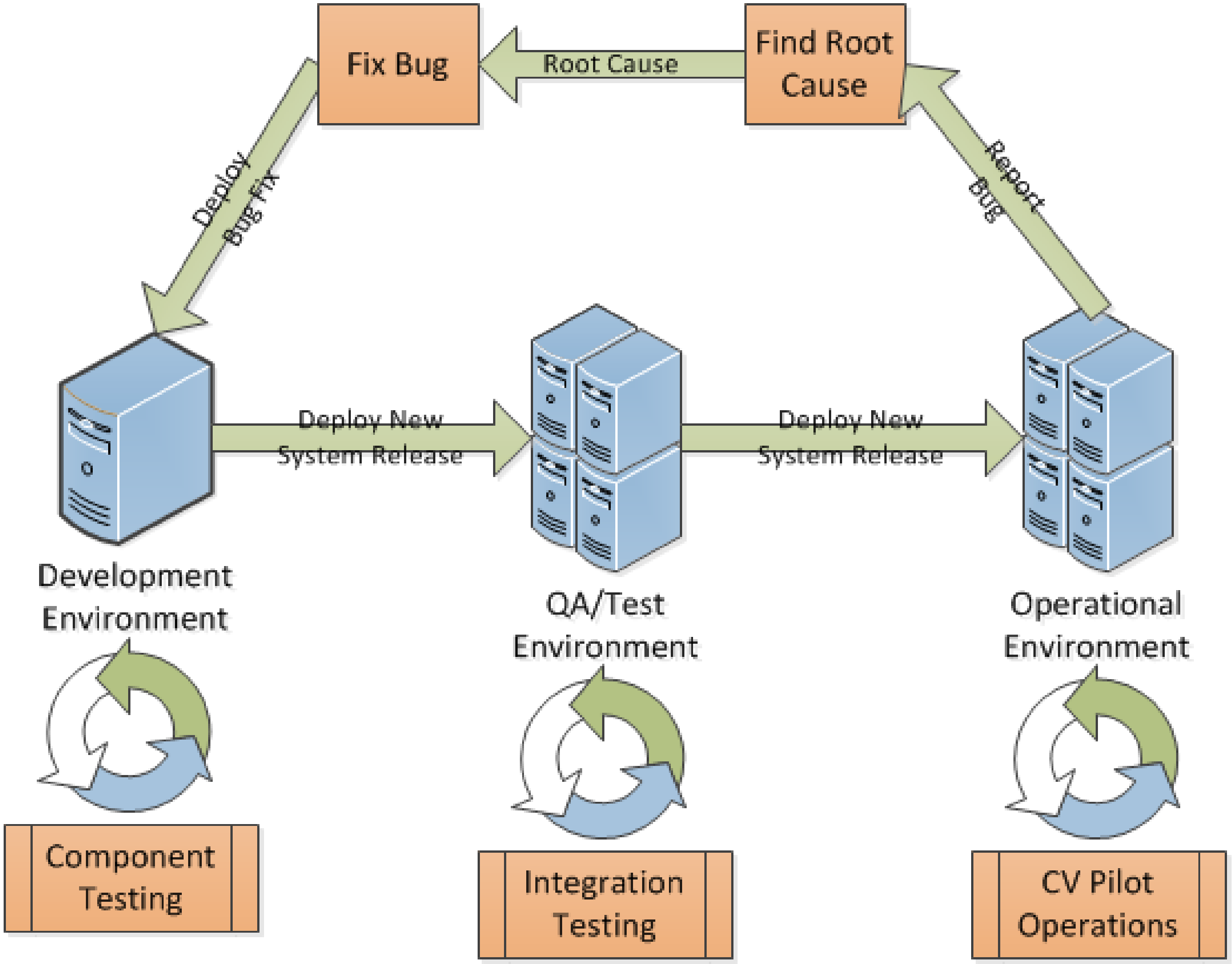

SCMS POC Governmental Management
Operation Protocols
Set Policies
End Entity User Group
SCMS PoC USOT Management & Policy Task Force
New Requirements (If necessary)
New/Alternative Functions/Fixes
Policies & Organizational Protocols
SCMS PoC Manager Environment
National Prototype Policy Development
Analysis of PoC Policies
Adapt & Additional Prototype Policies
USDOT SCMS Policy Statement
SCMS POC Development
Maintain Source Code
Fix Bugs
Develop New System Capabilities
Policies/ Protocols/ Basic Procedures
Technical Procedures
Software Releases
SCMS Technical Management
Develop Technical Procedures
End User & SCMS Technical Liasion
Support System Evaluation
Implement New Functions
Support Incident Studies
SCMS Operations
Establish Technical Operations
Generate Credentials
Pseudonym Certificate
Provide SCMS Tech Support
Connected Vehicle Support Services
General Support
Support Registration
End User Interface
System Documentation
Device Requirements
Procedures, Configurations & Certificates
Certification Services
Test Devices
Certify Devices
Deployment Sites
NYC
Tampa
Wyoming
Ann Arbor
Future Sites
Device Reg. & Support
Certification Documentation
Device Suppliers
Develop OBUs
Develop ASDs
Develop RSUs
Devices For Testing
Certified Devices

]

SCMS POC Roadmap


Security Credential Management System – Roadmap
2015
2016
2017
2018
2019
SCMS POC Refinement
SCMS POC IT Operations
SCMS POC Management
Develop Enrollment & Provisioning Functionality
SCMS PoC System v1.0
1.0
1.1
Interface Requirements
Integrate Global Misbehavior Detection Functionality
SCMS PoC System v2.0
Prototype Misbehavior Detection Methods
Deploy QA / Test Environment
Deploy Operational Environment
POC Policies & Procedures
Conduct POC Management Activities

SCMS Software Environments

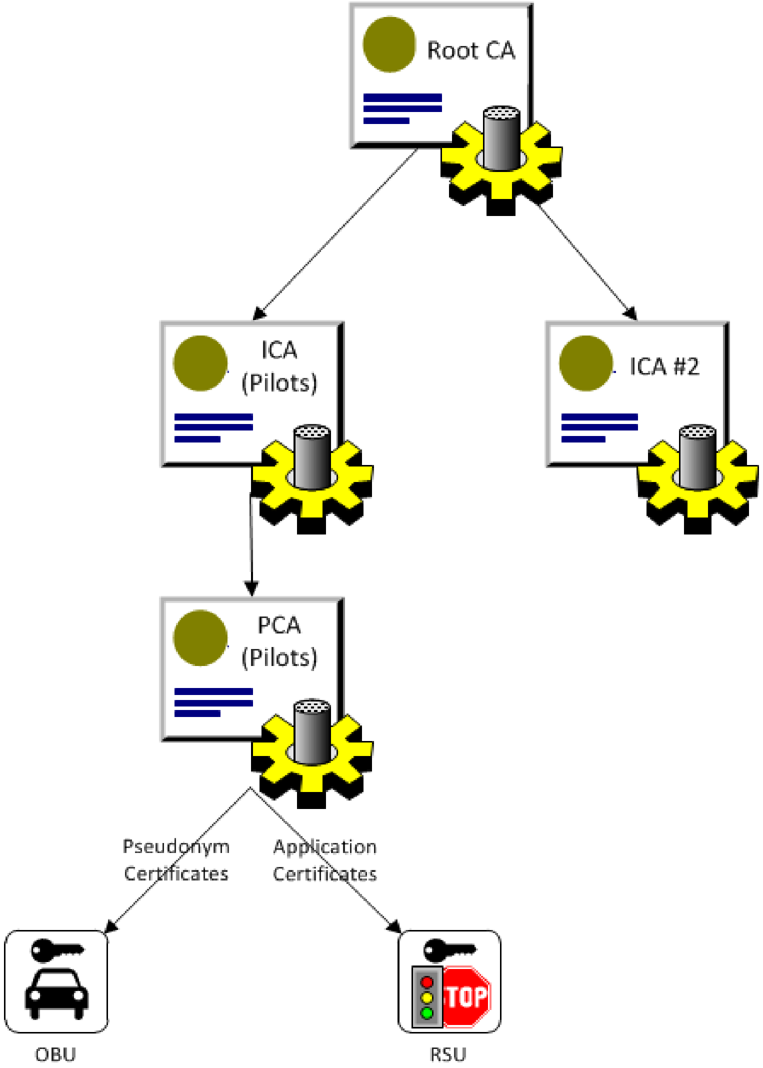


Certificate Authority Hierarchy

- 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

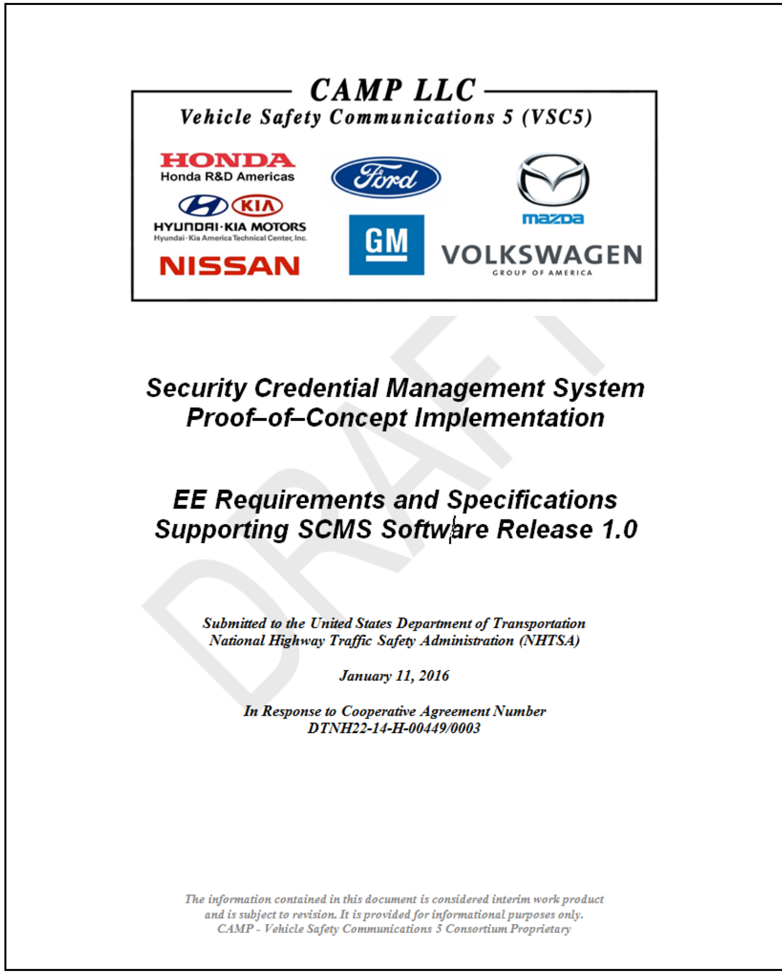
Issued To	Name	Purpose
OBU / ASD	Enrollment	Initialize the OBU to allow communication with the SCMS
OBU / ASD	Pseudonym	Used to sign all BSMs generated by an OBU
OBU	Authorization	Used to identify public sector vehicles for specific apps
RSU	Enrollment	Initialize the RSU to allow communication with SCMS
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 – Released in May 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
HYUNDAI·KIA MOTORS
Hyundai·Kia America Technical Center, Inc.
NISSAN
Ford
GM
mazda
VOLKSWAGEN
GROUP OF AMERICA

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)

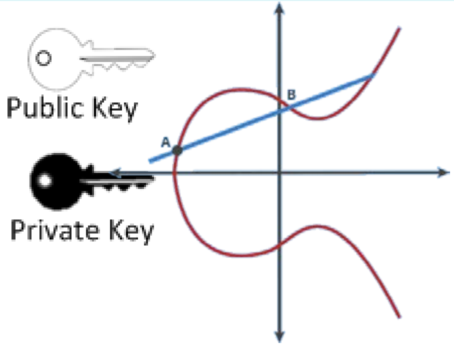
January 11, 2016

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

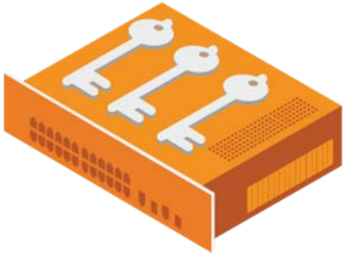
The information contained in this document is considered interim work product and is subject to revision. It is provided for informational purposes only.
CAMP - Vehicle Safety Communications 5 Consortium Proprietary

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

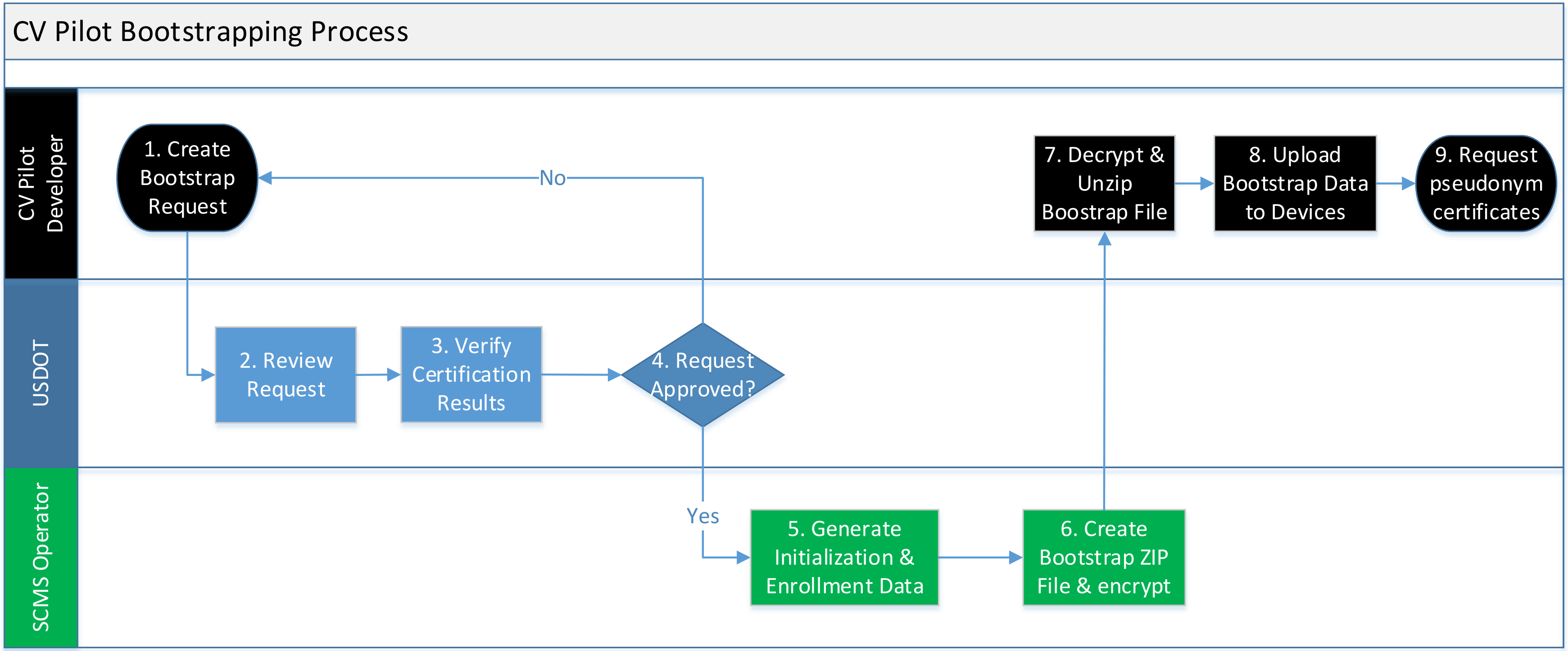


3. Definition of Time
   - SCMS POC will utilize TAI as the time basis according to IEEE 1609.2

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

UC 2: Bootstrapping

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

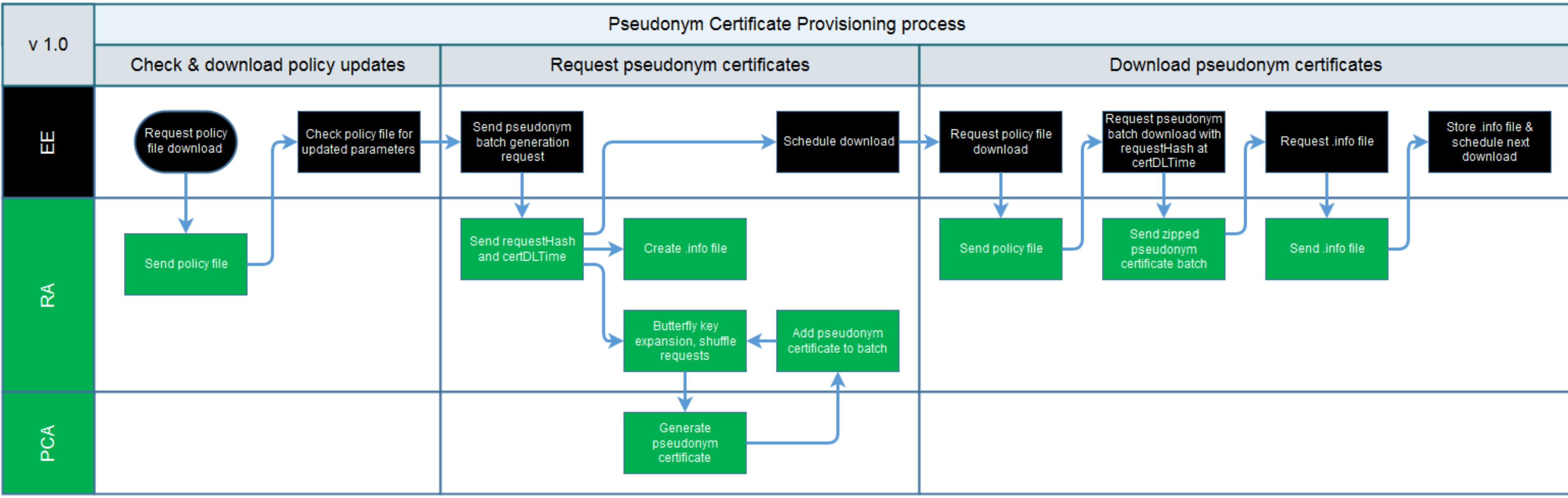


CV Pilot Bootstrapping Process

CV Pilot Developer
USDOT
SCMS Operator
1. Create Bootstrap Request
2. Review Request
3. Verify Certification Results
4. Request Approved?
No
Yes
5. Generate Initialization & Enrollment Data
6. Create Bootstrap ZIP File & encrypt
7. Decrypt & Unzip Boostrap File
8. Upload Bootstrap Data to Devices
9. Request pseudonym certificates

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



v 1.0

Pseudonym Certificate Provisioning process

Check & download policy updates

Request pseudonym certificates

Download pseudonym certificates

EE

RA

PCA

Request policy file download

Send policy file

Check policy file for updated parameters

Send pseudonym batch generation request

Send requestHash and certDLTime

Schedule download

Create .info file

Butterfly key expansion, shuffle requests

Add pseudonym certificate to batch

Generate pseudonym certificate

Request policy file download

Send policy file

Request pseudonym batch download with requestHash at certDLTime

Send zipped pseudonym certificate batch

Request .info file

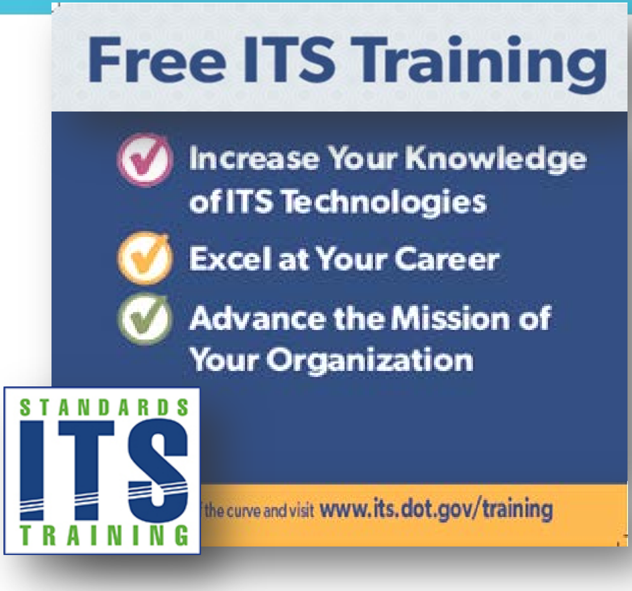
Send .info file

Store .info file & schedule next download

Stay Connected

Visit our website for information on:

- Webinars
- Events
- Publications
- News



Free ITS Training

- ✓ Increase Your Knowledge of ITS Technologies
- ✓ Excel at Your Career
- ✓ Advance the Mission of Your Organization

STANDARDS ITS TRAINING

the curve and visit www.its.dot.gov/training

Twitter: @ITSJPODirector

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

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

Kevin Gay, PMP
Chief – ITS Policy, Architecture and Knowledge Transfer
Kevin.Gay@dot.gov