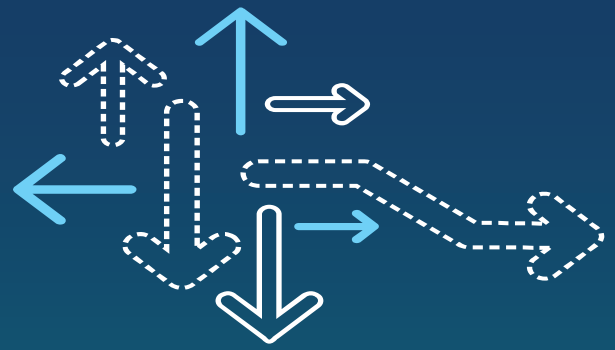


SCMS overview

ITS California Annual Meeting
18-20 Sept 2017, Burlingame CA

QUALCOMM®

ITS: Security requirements and challenges

ITS – car to car communications: Wireless Access in Vehicular Environments (WAVE)

- Communications security required as *traditional*: integrity, authenticity, authorization, confidentiality.
  - Specific to the ITS application.

- Additional challenges *for ITS* communications:
  - Privacy (untrackability) of user/device,
  - Limited channel resources
  - Device constraints (heavy processing, integrity a must)

- Additional *network* architecture challenges:
  - Complex due to privacy requirements and intermittent connectivity of vehicles.

Vehicle to everything (V2X) communications security details

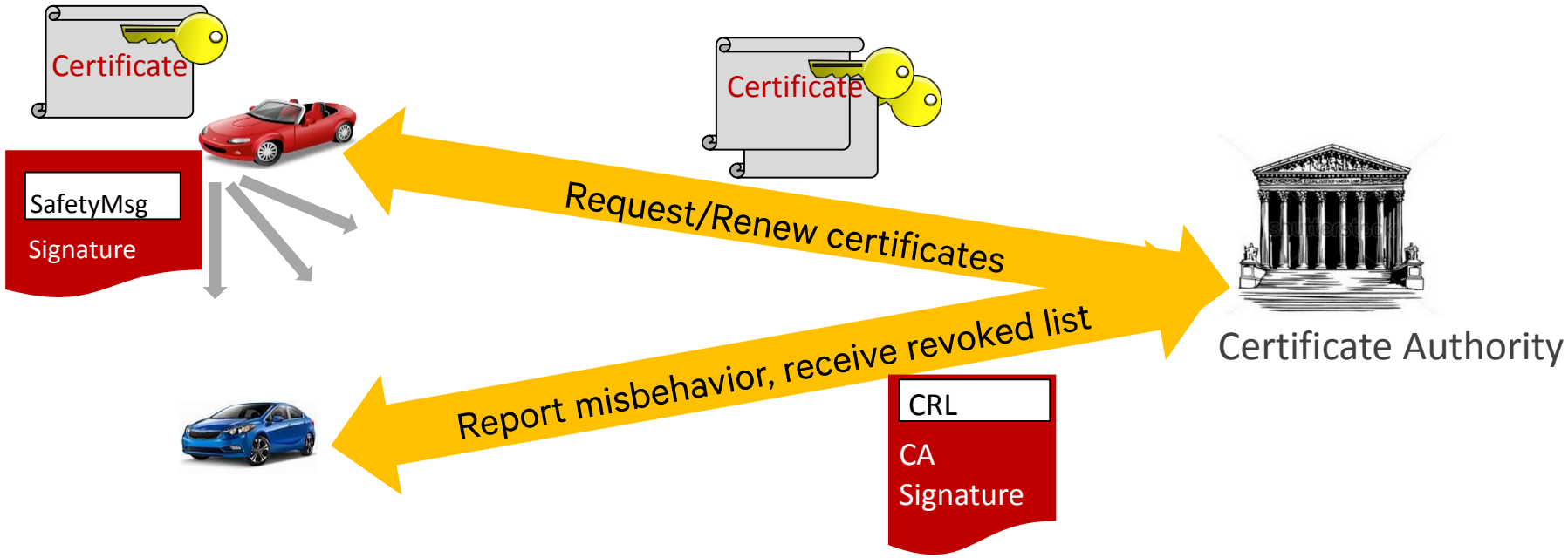
- **Integrity in V2X systems means ability of receiver devices to verify that**
  - V2X message sender is a trustworthy/authorized device
  - V2X message was not modified between sender and receiver
- **Privacy means**
  - No *single* device or network entity is able to track another device beyond a short time interval
- **Trust part of security means misbehaving devices are identified**
  - Other devices can know not to trust messages from misbehaving devices

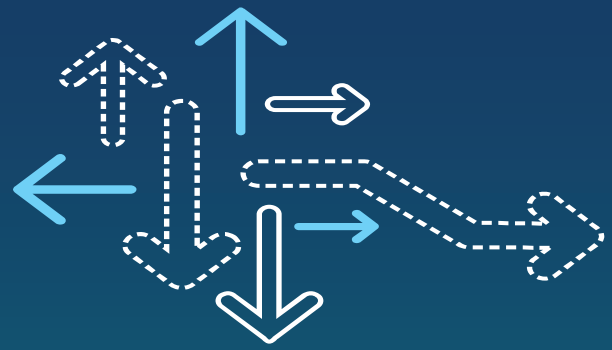
Solution

- Use digital signatures to guarantee integrity of V2 messages
- Change credentials on a regular and frequent basis to prevent tracking
- Use a central authority employing Public Key Infra as trust anchor–(privacy)
- Disseminate Cert Revocation Lists (CRL)
- Use secure links vehicle to network, encrypt confidential information

ITS communication security for WAVE

Simplified



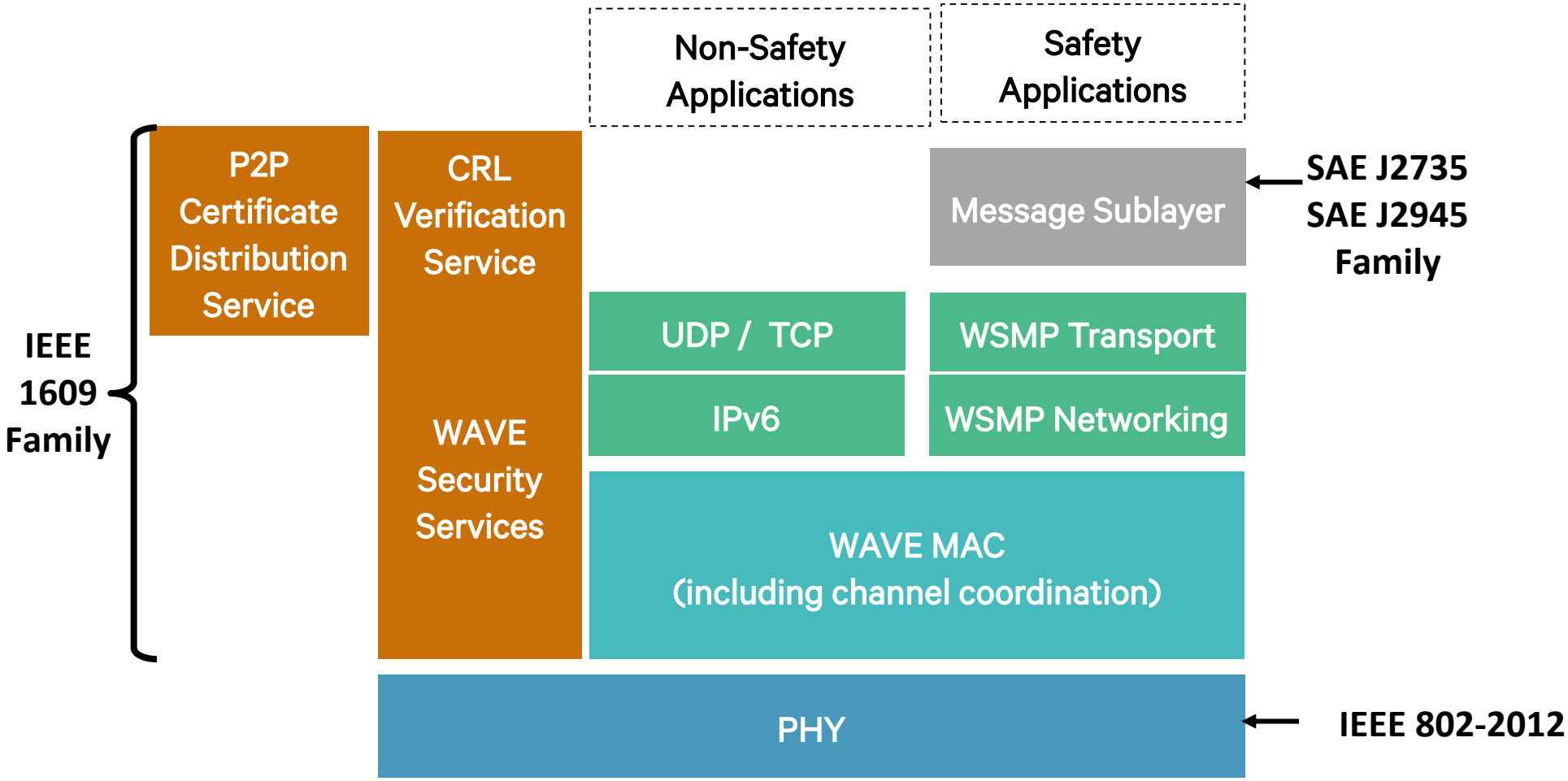


WAVE security standards aspects

The *Security Credential Management System* (SCMS) was developed over many years under a cooperative agreement by CAMP with the United States Department of Transportation (USDOT). According to the NPRM, SCMS is currently the leading candidate for vehicle-to-vehicle (V2V) security backend design in the United States

Device OSI layers and Relevant Standards (US)

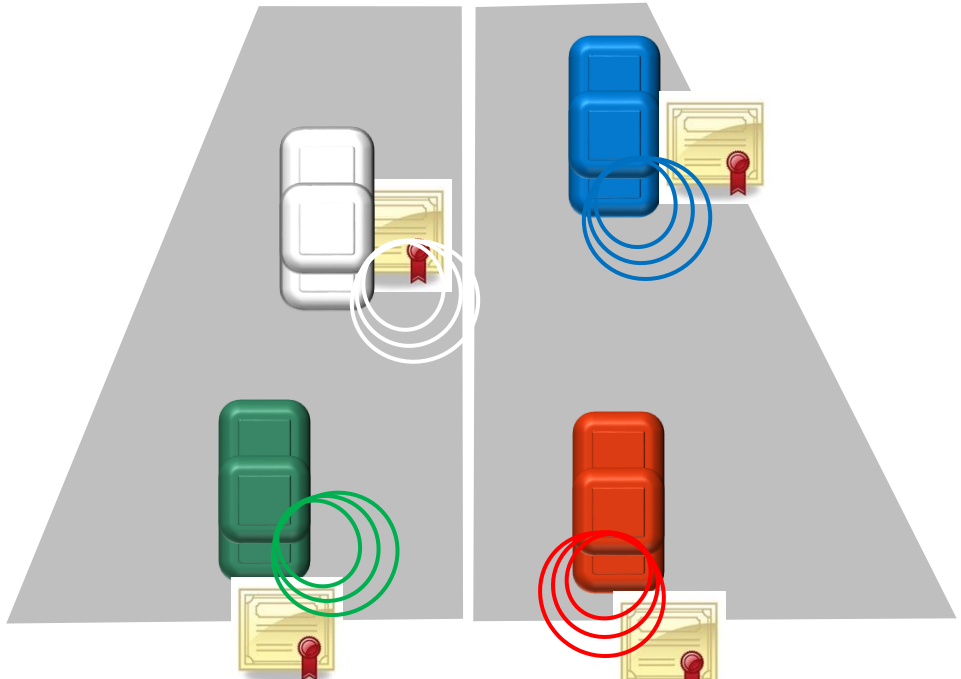
WAVE IEEE 1609 Wireless Access in Vehicular Environments stack



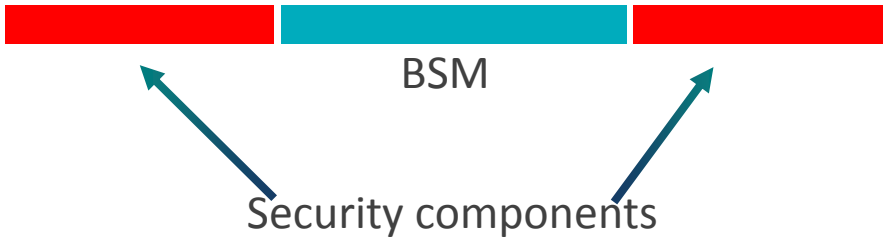
V2V WAVE security aspects

Vehicles have no prior relationship at an instance in time and space

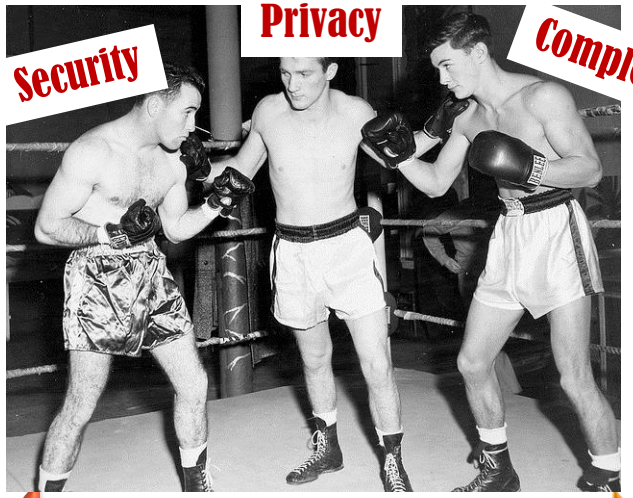
- Each vehicle is securely provisioned with many short-lived pseudonym certificates
- Each sender uses one of its certs to sign BSMs, sends them broadcast
- Each vehicle who can hear it can verify BSM legitimacy on its own
- Authentication, authorization, privacy, un-trackability enforced



BSM: basic safety message*
Processed at the app layer



The challenges of WAVE security design



Integrity of messages

Anonymity of sender

Simplicity of network architecture

Unlinkability /trackability by network

Complete CRL distribution

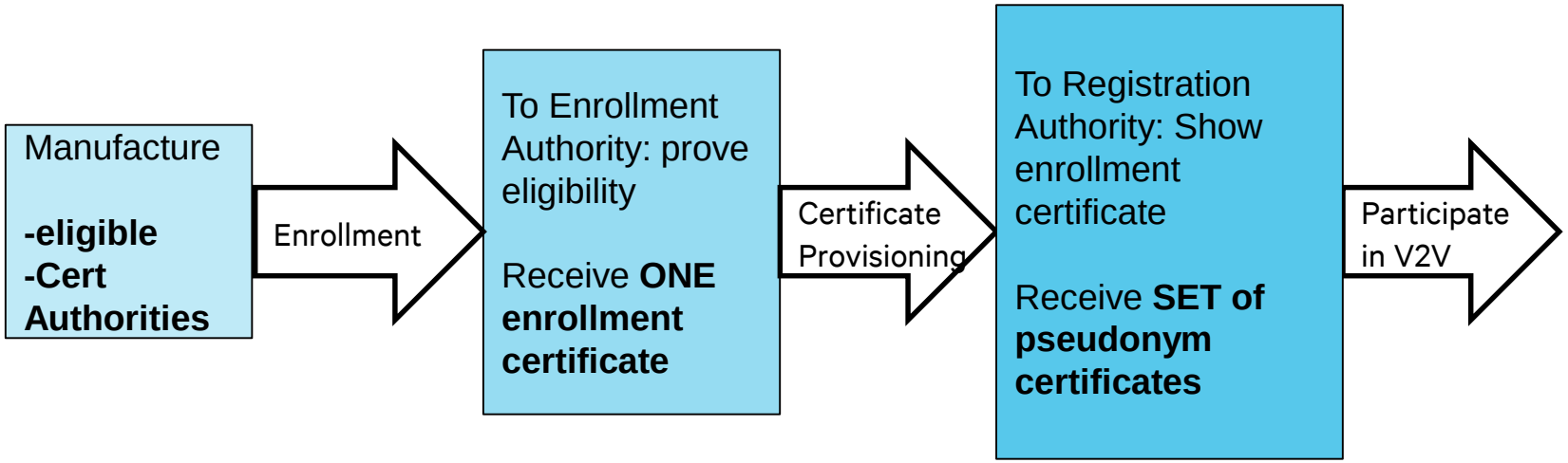
Data download reduction

Security of certificate generation

Ease device computation

Phases of configuration for vehicle security module

Supported by SCMS

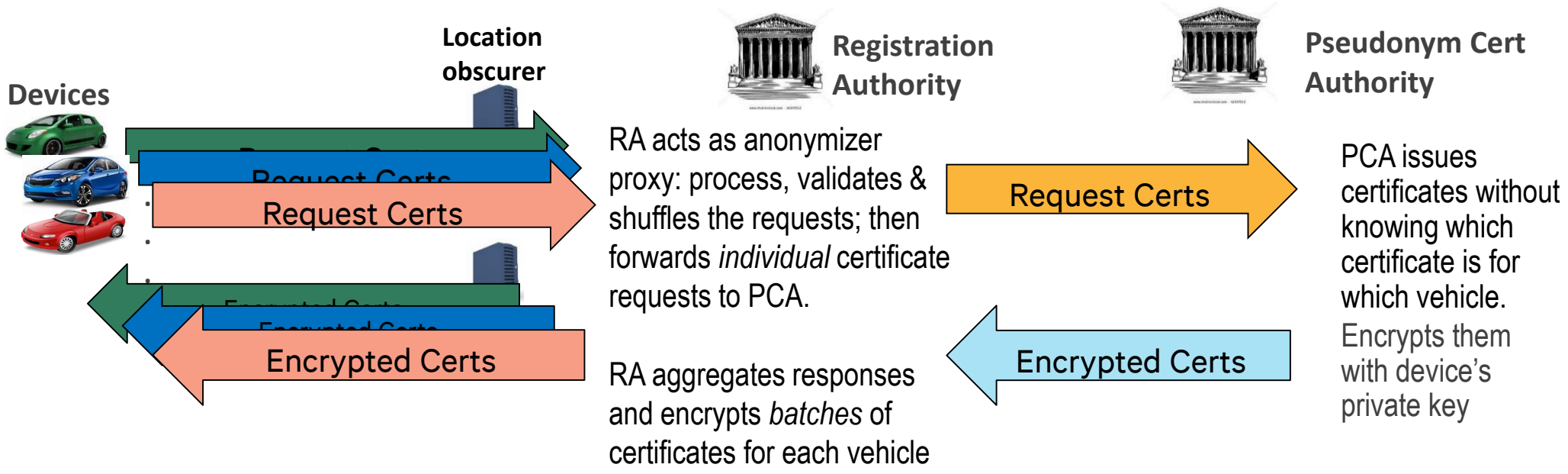


Enrollment Authority validates that Device can be trusted to function correctly; issues long-term enrollment cert, temporary ID for the Device.

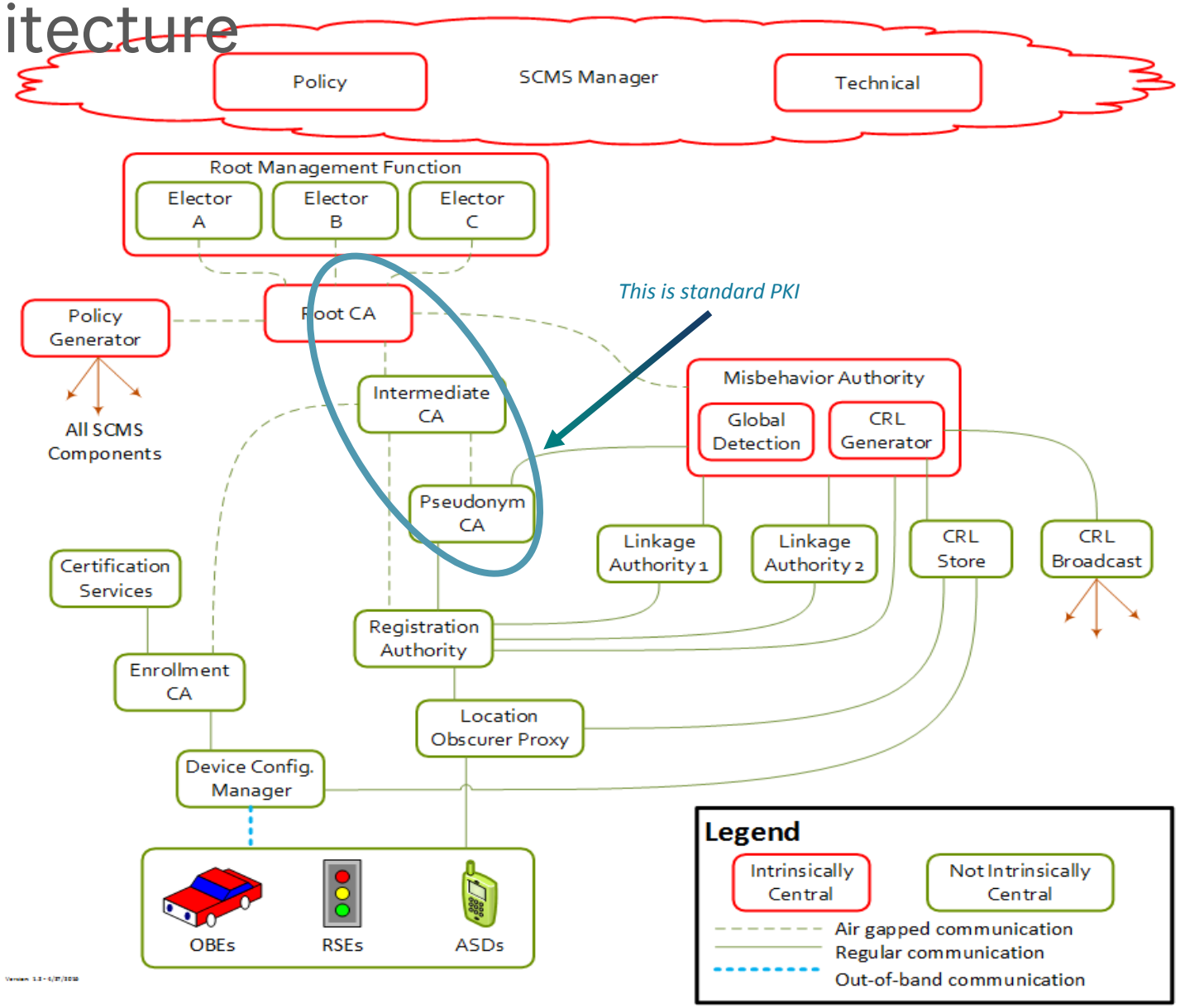
Registration Authority is the one interface of the Device to the SCMS network from here on (provision, CRL); makes available short-term pseudonym certs (via location obscurer function)

Simplified cert provisioning flow

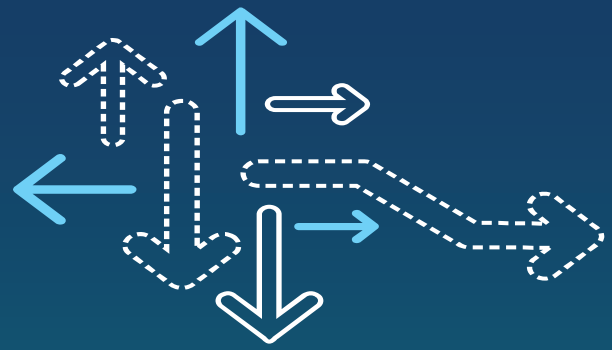
How the vehicles get certs for signing safety messages



SCMS architecture



Courtesy IEEE 1609.2 2016



Trials/POCs of SCMS

Jim Misener

SCMS on the Road

- Base Document (now in version 2): *Security Credential Management System Proof–of–Concept Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.1:*
  - https://www.its.dot.gov/pilots/pdf/SCMS_POC_EE_Requirements.pdf
- Developed by CAMP (OEMs/NHTSA).
- Under testing:
  - US DSRC Connected Vehicle Pilots: NYC, Tampa, and Montana. NYC is the prime test site.
  - Next: Columbus Smart City (USDOT-funded initiative with DSRC as a requirement)
  - Promoted as a model for rest of world by US-EU-Japan-Australia governments “Harmonization Task Group”

SCMS next steps

- New for SCMS since its stable version:
  - Modified IEEE 1609.2 (security services) to accommodate SCMS
    - Specified interfaces of vehicle to network
    - Standardized Peer to peer certificate distribution
    - Completed specification of policies
- Next:
  - Make technical changes based on trials. This may be 1 – 2 years downstream
  - Have SCMS ready for 1st US deployment (2020 – 2021)
    - Need to address objections/comments and variants stated in the NPRM.
    - Need to develop sustainable business model.

Thank you

References in this presentation to "Qualcomm" may mean Qualcomm Incorporated, Qualcomm Technologies, Inc., and/or other subsidiaries or business units within the Qualcomm corporate structure, as applicable.

Qualcomm Incorporated includes Qualcomm's licensing business, QTL, and the vast majority of its patent portfolio. Qualcomm Technologies, Inc., a wholly-owned subsidiary of Qualcomm Incorporated, operates, along with its subsidiaries, substantially all of Qualcomm's engineering, research and development functions, and substantially all of its product and services businesses,
including its semiconductor business.

QUALCOMM®