escrypt
SECURITY. TRUST. SUCCESS.

Secure V2X Proof-of-Concept Deployment in the City of Stratford

Kevin Henry
ESCRYPT Canada

Overview

escrypt
SECURITY. TRUST. SUCCESS.

- City of Stratford - Project Overview
- Rationale for a Complex PKI for V2X Applications
- High-Level Requirements
  - Tradeoff of authenticity and anonymity
  - Connectivity assumptions
  - Distributed Control
- North-American SCMS Architecture
- SCMS Operating Model

City of Stratford Project

escrypt
SECURITY. TRUST. SUCCESS.

APMA
LEAD. REACH. CONNECT.

Stratford
ONTARIO CANADA

escrypt
SECURITY. TRUST. SUCCESS.

TRUSTPOINT
INNOVATION

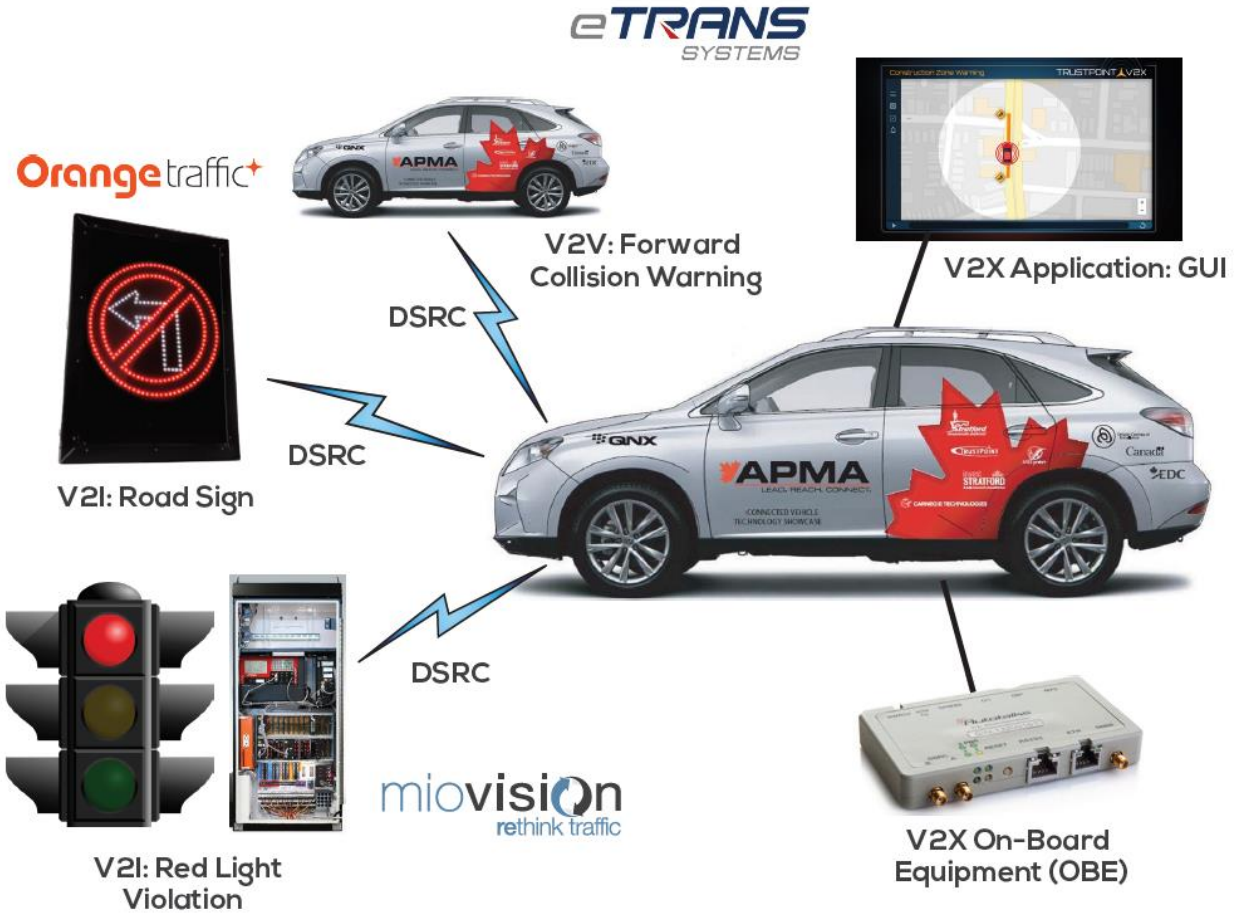
Demonstration site to test and showcase developed AV/CV technologies

Serves as a platform for collaboration amongst Ontario and Canadian based AV/CV companies

Promotes and supports a “super-cluster” of AV/CV and automotive companies in Southwestern Ontario

City of Stratford Project

escrypt
SECURITY. TRUST. SUCCESS.

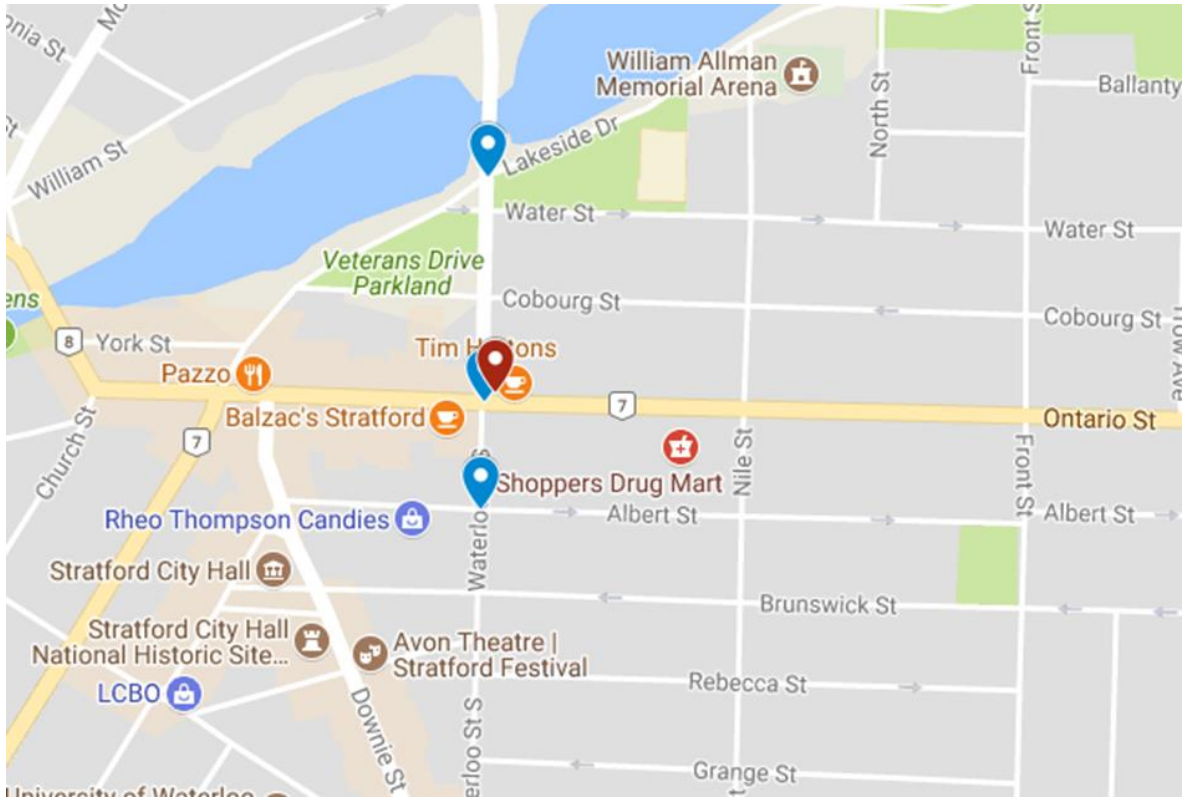


- Establish V2I "nodes" to demonstrate V2X applications:
  - **V2X Security Infrastructure**
  - **Secure communications adhereing to V2X SCMS specifications**
- V2X Applications:
  - RLV: Red Light Violation (V2I)
  - RS: Road Sign (V2I)
  - FCW: Forward Collision Warning (V2V)
  - V2X security uses cases
  - GUI Interface
- Finishing Up Initial Project (Field Trials)

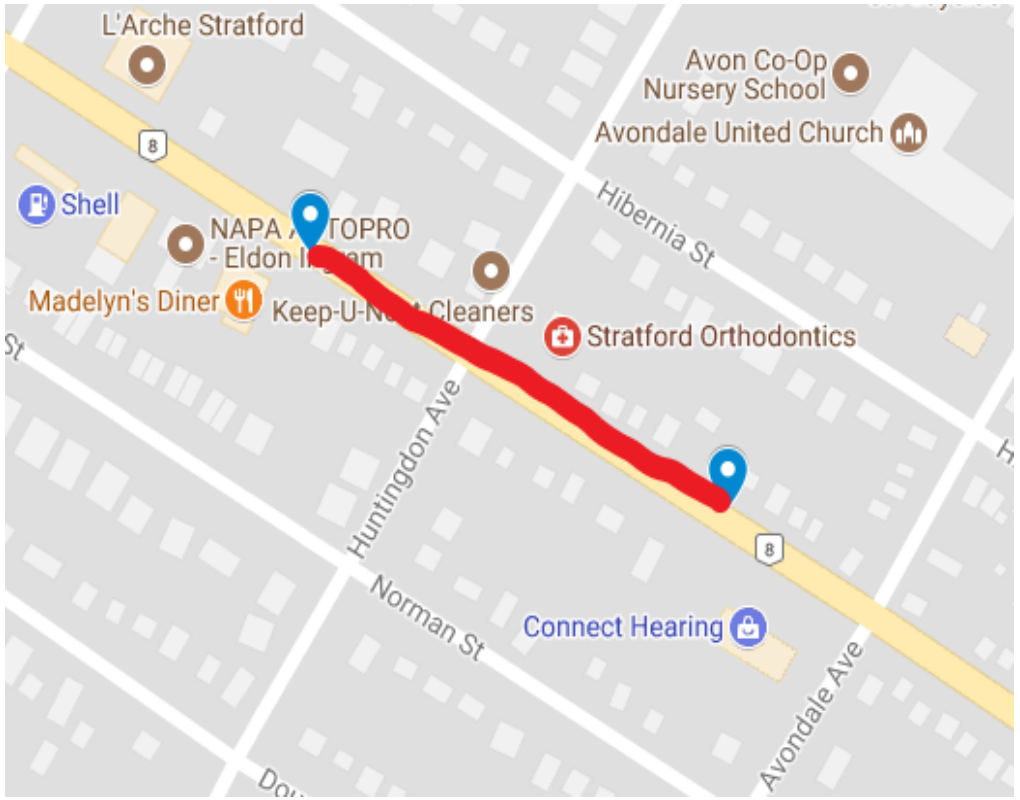
info@escrypt.com

City of Stratford Project

escrypt
SECURITY. TRUST. SUCCESS.



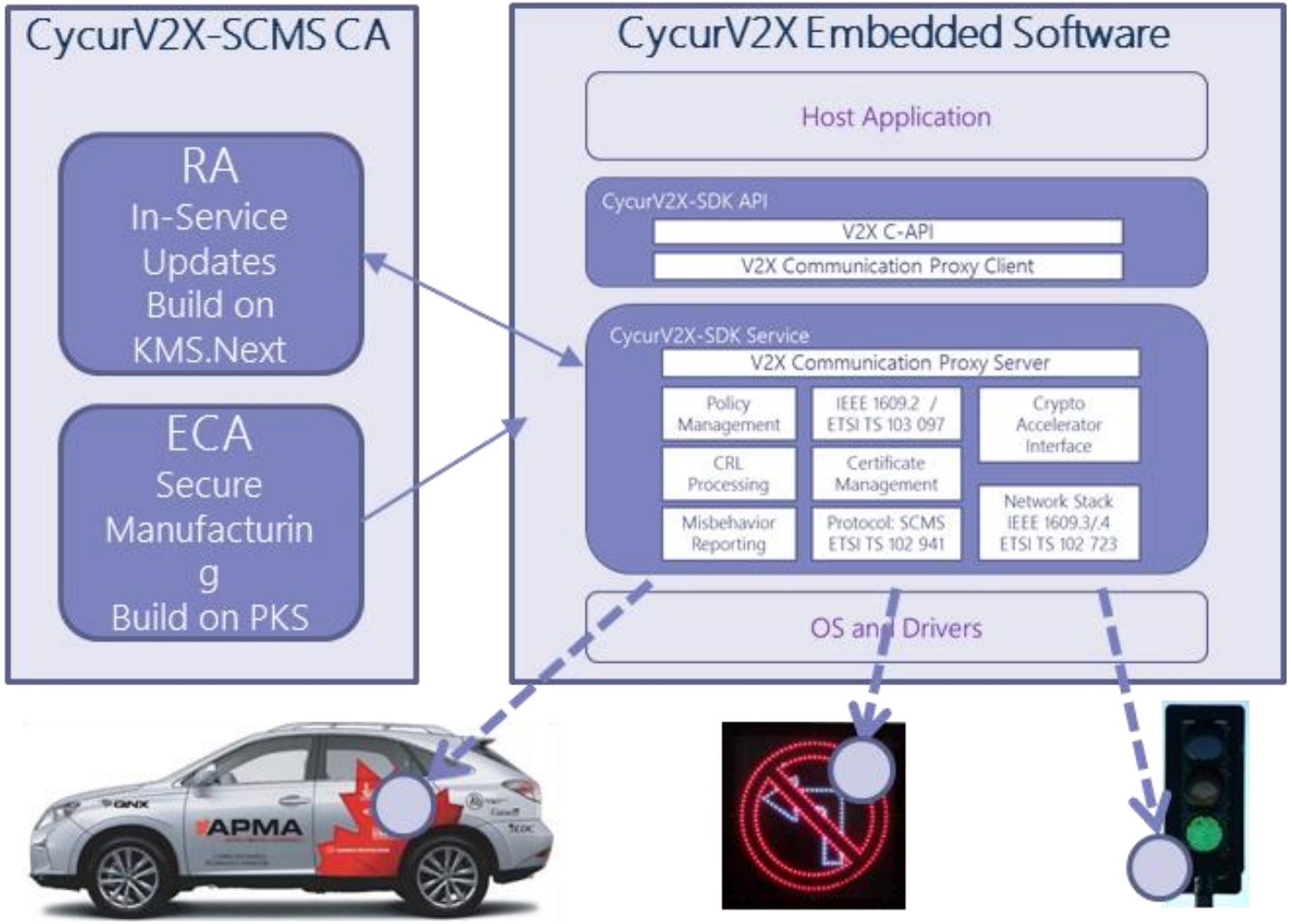
V2X Enabled Intersections on Waterloo Street



School Zone Signs deployed on Huron Street

ESCRYPT's Role in Stratford

escrypt
SECURITY. TRUST. SUCCESS.



- Embedded software security solution and CA services for connected-vehicle and connected-infrastructure communications
- The same security technology can be used in cars, roadside equipment, and smart-city infrastructure

info@escrypt.com

Inherent Tension

It is difficult to prove authenticity while also supporting privacy

escrypt
SECURITY. TRUST. SUCCESS.

Authenticity

Need to validate that messages are from trusted devices

- Prevent attackers from creating fake messages to change traffic patterns or create a road hazard

VS.

Privacy

Can't make it easy to track personal cars

- Each BSM contains exact position information
- Data is sent unencrypted to enable fast response time

- Digital Signatures can prove that a message is "authentic" and unmodified, but only if you know you can trust the sender
- How do you trust the sender if you can't know who the sender is?

Simple Solution: Pseudonyms

Pseudonyms protect privacy, but with a cost of complexity

escrypt
SECURITY. TRUST. SUCCESS.

- Give each car a fake name or pseudonym
- If you trust the entity that issued the pseudonym, then you can trust the message

  … but then you can track the car, so

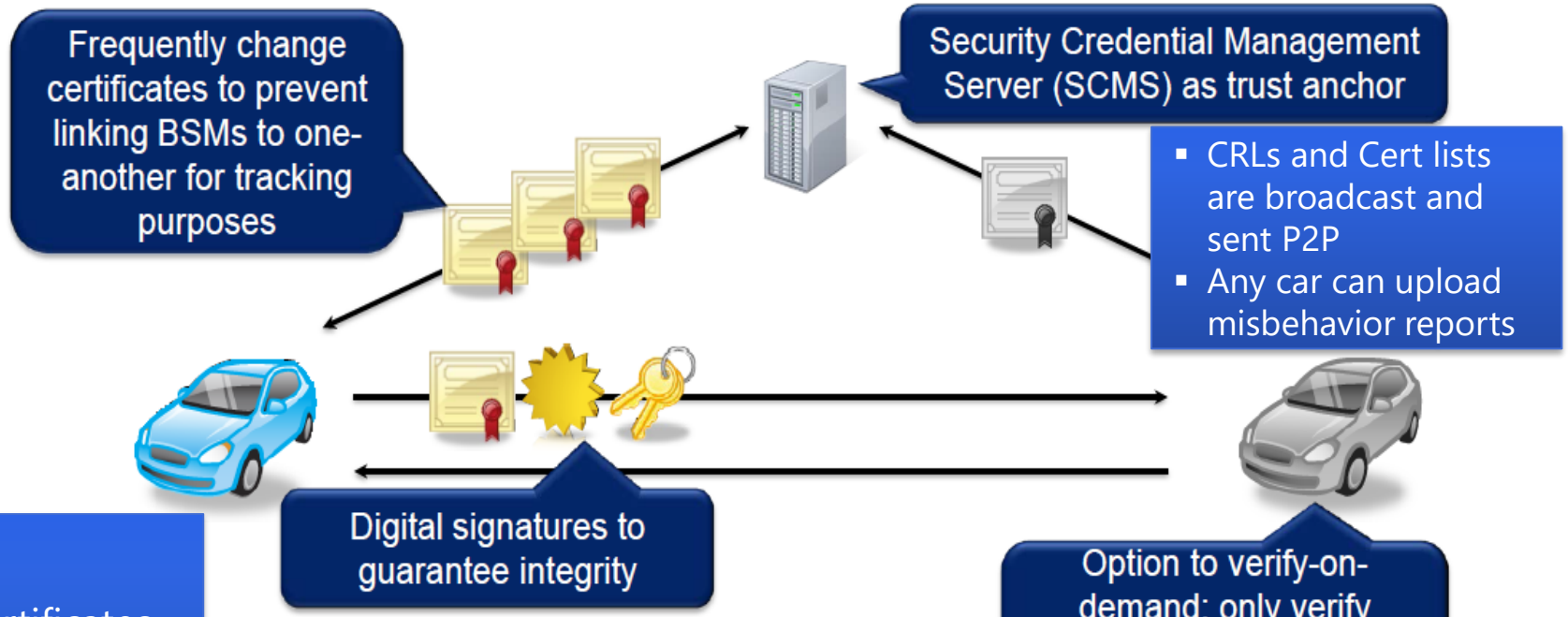
- Give each car a LOT of pseudonyms and switch identities frequently

  … but how do these IDs get issued and what happens if you run out of fake identities, can you get more?

- Assume some vehicles will have very limited access to a wide-area network

Security / Privacy Solution

escrypt
SECURITY. TRUST. SUCCESS.



Each Car:
- Stores 3 Years of certificates
- Uses batch of 20 certs / week
- Switches current cert every 5 min

Basic Safety Message (BSM)
- Vehicle position and velocity vector
- Steering angle, throttle, brake status
- Broadcast 10 times / second

info@escrypt.com

Design for Security and Privacy

The complexity in the SCMS is driven by requirements

escrypt
SECURITY. TRUST. SUCCESS.

Security

- Every message is digitally signed (but not encrypted)
- Use ECC implicit certificates to minimize storage and bandwidth
- Add linkage values to support "misbehavior detection" and revocation

Privacy

- No unique information about the car or the owner
- Certificate changes every 5 minutes
- Re-use a batch of 20 certificates for a period of 1 week

20 new certificates per week per car with ~250M cars (US)

= 260B certificates per year

info@escrypt.com

SCMS and 1609.2

The SCMS is built using IEEE 1609.2 certificates

escrypt
SECURITY. TRUST. SUCCESS.

- **IEEE 1609.2** is a standard that defines how to encode secure information
  - Includes structures for digitally signed and encrypted data
  - Defines how to encode several types of digital certificates
  - Specifies encoding, byte ordering, padding, etc.
  - Is (mostly) complete and stable (1609.2-2016, 1609.2-2017a)

- **SCMS** is a set of requirements that describe how to issue and manage security credentials
  - Introduces an architecture and roles for security management components
  - Describes how to *technically* issue 1609.2 certificates to devices
  - Introduces special messages for communicating with the security infrastructure and among back-end components
  - Includes technical procedures for managing system components
  - Does not (currently) specify policies or assign roles
  - Is (mostly) stable-enough to use, but still evolving

Crash Avoidance Metrics Partnership (CAMP)

SCMS design was developed and documented by CAMP

escrypt
SECURITY. TRUST. SUCCESS.

Public documentation on SCMS interface (release 1.2.2) is avalable online:

https://wiki.campllc.org/display/SCP/SCMS+CV+Pilots+Documentation

CAMP is under contract to the US DOT (technically NHTSA)

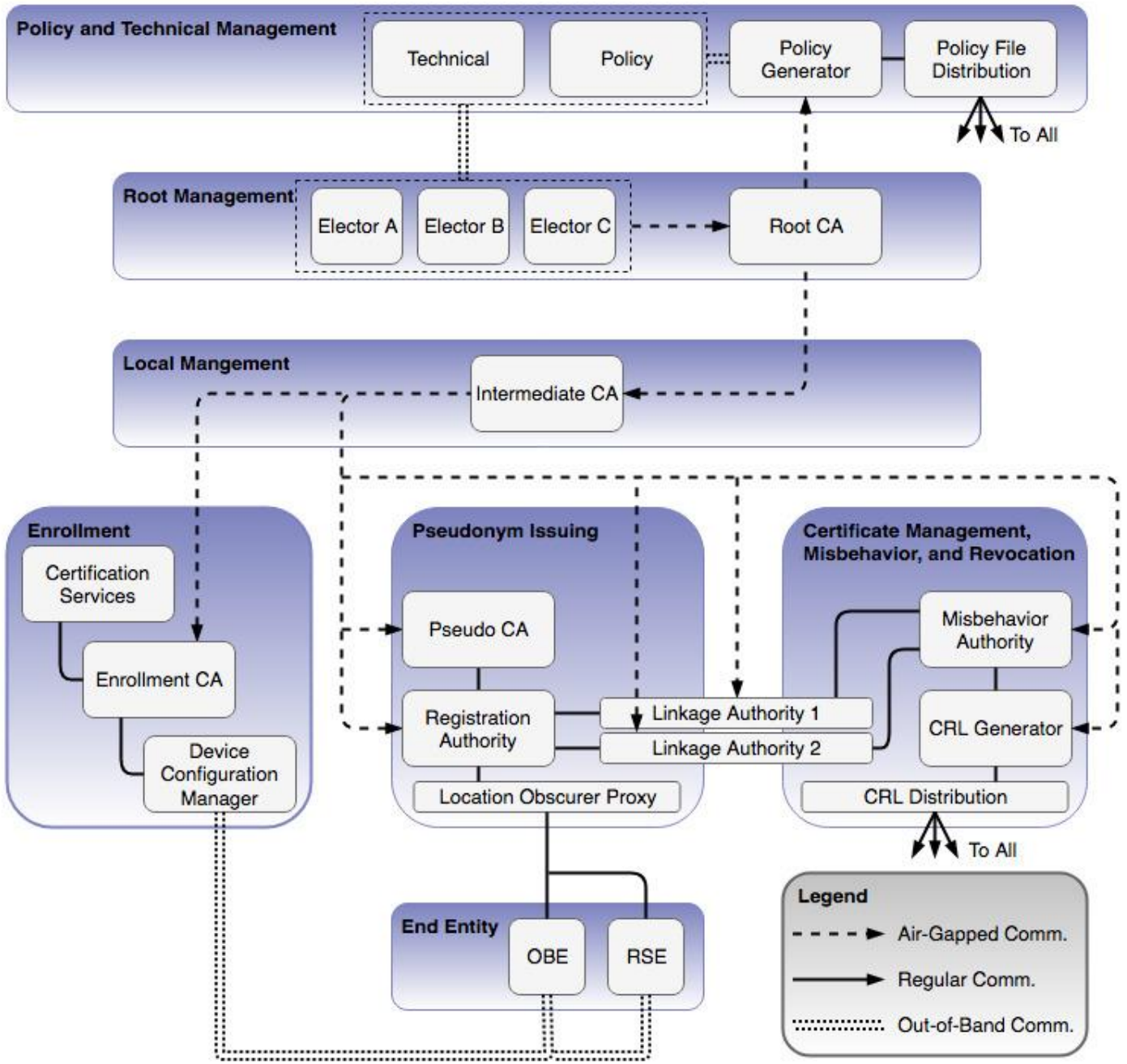
- Design the Security Credential Management System (SCMS)
- Develop a working prototype system
- Support the US Connected Vehicle (CV) pilots in New York, Florida, and Wyoming

ESCRYPT is a security technical advisor to the SCMS design program

SCMS Systems View

Main functions of the SCMS

- **Policy & Technical Management**
  Manages overall system
- **Root Management**
  Establishes the system-wide "root of trust"
- **Local Management**
  Issues local CA certificates
- **Enrollment**
  Activates new devices in the system
- **Pseudonym Issuing**
  Delivers batches of pseudonym certificates
- **Misbehavior Detection**
  Identifies bad actors, creates and distributes a Certificate Revocation List



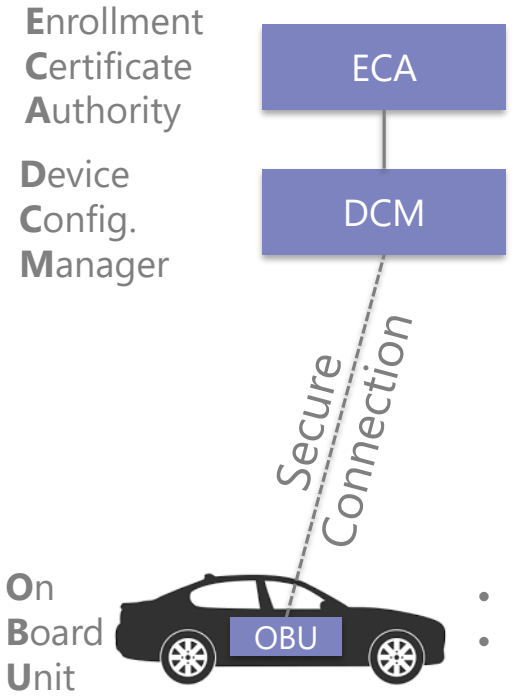
info@escrypt.com

Enrolment Process

Each vehicle must be enrolled during manufacturing

escrypt
SECURITY. TRUST. SUCCESS.

- A new OBU must be enrolled before it can participate in the SCMS
- An enrollment certificate acts as a trusted "ticket", used for accessing SCMS services and downloading files



- ECA issues enrollment certificates
- Every enrollment certificate is assigned to a specific RA
- ECA trusts that messages sent through the DCM came from a real OBU

- DCM needs to confirm that it is connected to a real OBU
- May perform software updates or integrity checks
- Installs a Local Certificate Chain File (LCCF) which includes a copy of the Root CA(s)
- Installs a Local Policy File (LPF) which defines security-critical policies

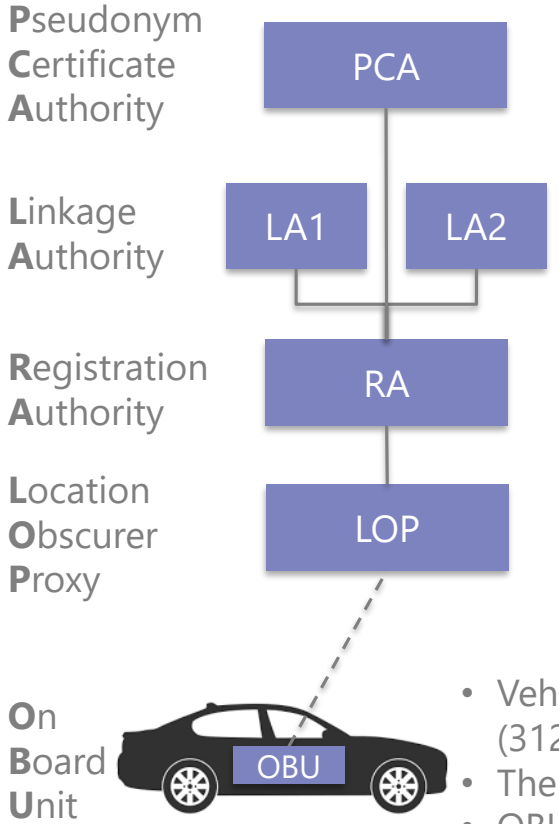
- An OBU can be enrolled before or after installation in a vehicle
- Recommended that each OBU generates it's own private key for enrollment (but secure key injection is allowed)

Pseudonym Certificate Download

Every vehicle must download batches of certificates from the RA

escrypt
SECURITY. TRUST. SUCCESS.

- Once enrolled, the OBU can only connect with the RA
- The first task is to download the initial batch of pseudonym certificates



- PCA(s) signs and encrypts individual pseudonym certs
- Certificate includes encrypted LV

- Linkage Authorities provide an encrypted Pre-Linkage Value (PLV) that can link back to the identity of the vehicle (for revocation)

- RA Validates that each vehicle has a valid enrollment cert
- RA breaks apart the batch request, mixes CSRs from multiple cars

- LOP removes any information about the vehicle network connection that might give away location

- Vehicles request a batch of pseudonym certificates (3120 for initial batch)
- The initial request includes a single seed public key and an encryption key
- OBU downloads certificates as a set of ZIP files
- Certificates are decrypted, re-constructed, and validated as- needed

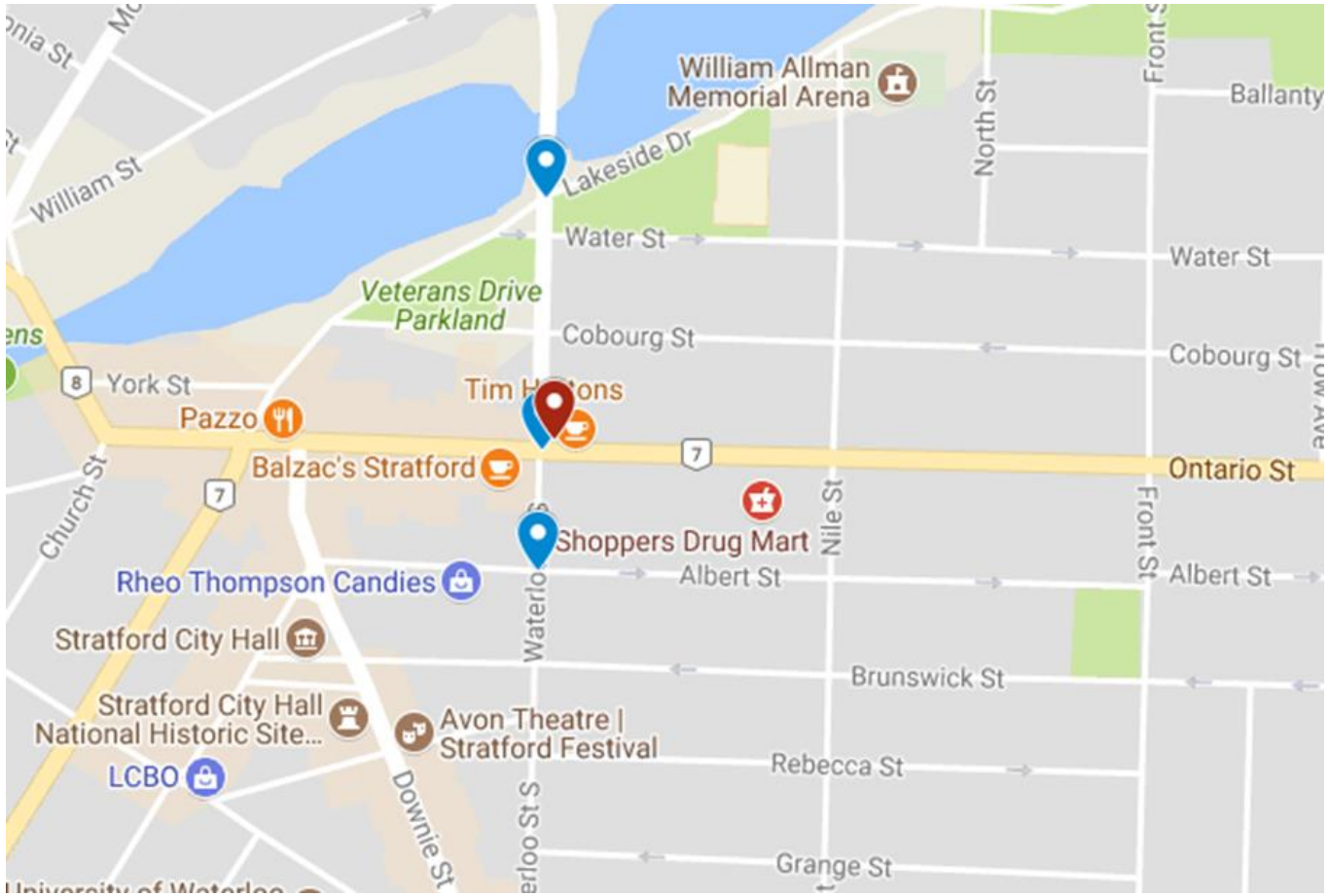
Component Knows
Certificate Content Only
Linkage Seed Only
Identity Only
Network Address Only

info@escrypt.com

City of Stratford Project

Next Steps

escrypt
SECURITY. TRUST. SUCCESS.



APMA
LEAD. REACH. CONNECT.

Stratford
ONTARIO CANADA

escrypt
SECURITY. TRUST. SUCCESS.

info@escrypt.com

ESCRYPT Canada
419 Phillip Street
Waterloo, ON
N2L 3X2
Canada

info@escrypt.com
www.escrypt.com

Certificate Types

There are 4 types of certificates used by vehicles and roadside units

escrypt
SECURITY. TRUST. SUCCESS.

- Enrollment Certificate
  - Issued to an vehicle in manufacturing, long validity period (~6 years)
  - Used as “password” to access the SCMS
  - Does not contain any identifiable information about the vehicle or owner
  - A vehicle has only one valid enrollment certificate at a time
- Pseudonym Certificate
  - Generated in batches, downloaded by the vehicle on the road, used to sign V2V or V2I messages
  - A vehicle typically has 20 valid pseudonym certs at one time, valid for 1 week
  - Revoked by publishing the linkage seed and blacklisting the enrollment certificate
- Identity Certificate
  - Issued to a vehicle through a registration process (by an RA), may have a long life
  - Used for special applications - emergency, commercial, military, etc.
  - May contain specific identification information or permissions (such as a geo-fence)
- Application Certificate
  - Issued to roadside equipment to enable V2I applications
  - Typically has a short life (1 day or 1 week), replaced when needed
  - Revoked by blacklisting the enrollment certificate

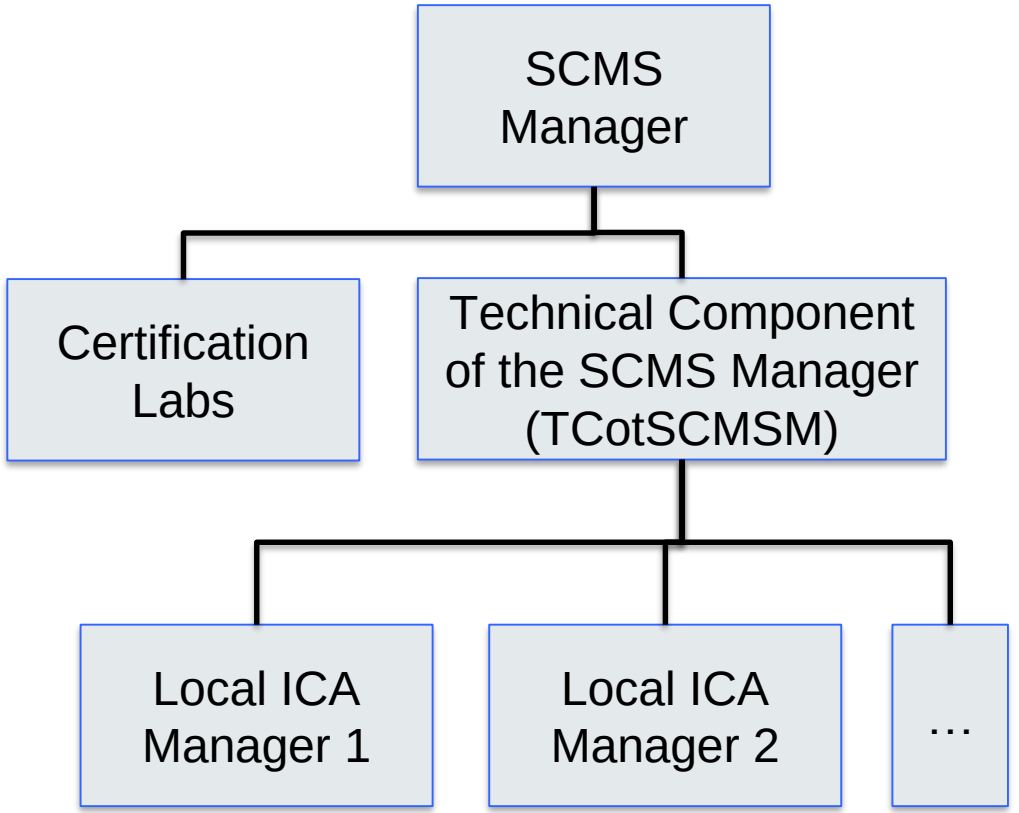
info@escrypt.com

SCMS Management Structure

Both policy and technical support is needed to maintain the SCMS

escrypt
SECURITY. TRUST. SUCCESS.

- The production version of the SCMS allows for “local” management
  - ICA manager can issue a Local Policy File (LPF)
  - ICA manager will provide a Local Certificate Chain File (LCCF)
- The only central function is Misbehavior Authority (MA) and CRL distribution

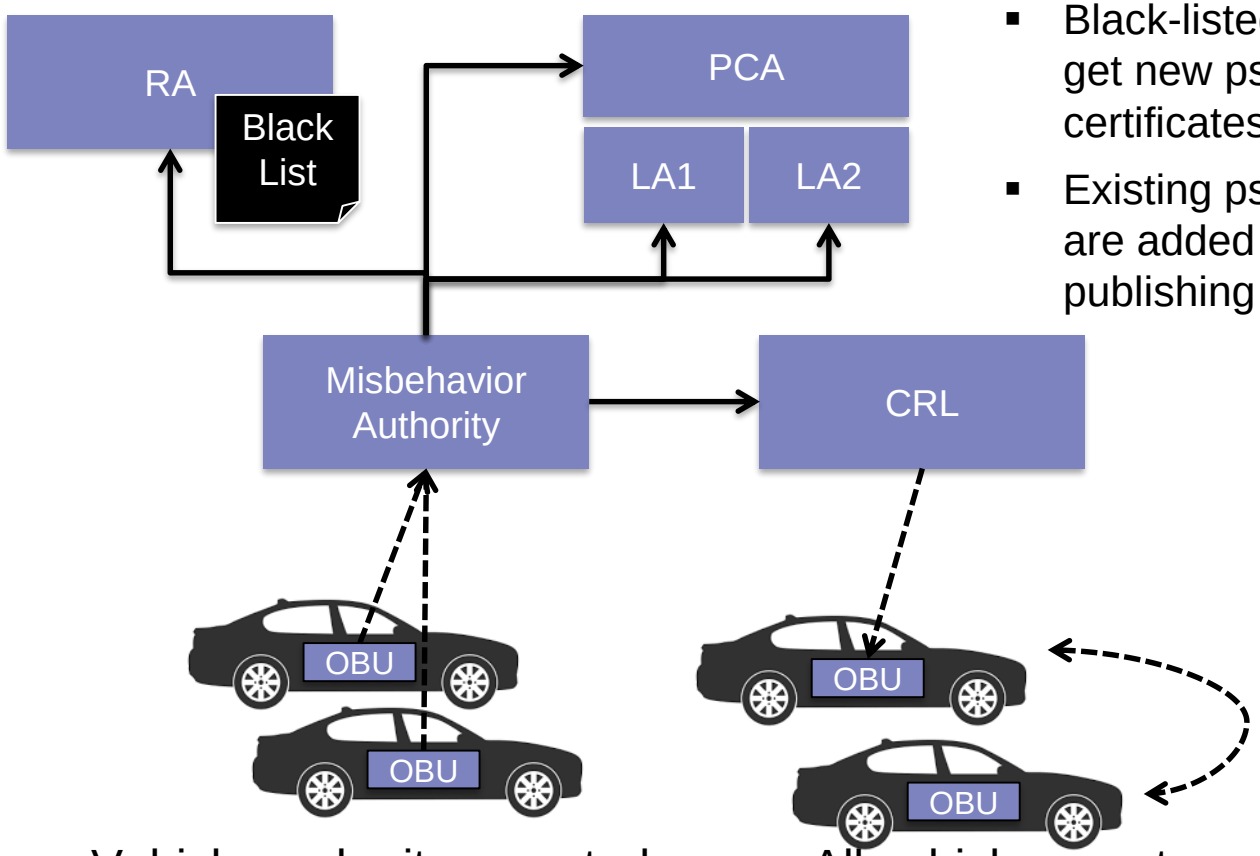


Misbehavior Reporting and Revocation

Any vehicle can report misbehavior

escrypt
SECURITY. TRUST. SUCCESS.

- Reports are encrypted and signed by the vehicle
- RA routes encrypted reports to MA without viewing the contents
- MA can break privacy only when there is strong evidence of misbehavior
  - MA, RA, PCA, and LAs must collaborate to revoke a vehicle
- The RA blacklist prevents revoked vehicles from getting new pseudonyms
- Once revoked, a vehicle will become “invisible” to other systems



- Black-listed OBUs can not get new pseudonym certificates
- Existing pseudonym certs are added to the CRL by publishing the LV

Vehicles submit encrypted misbehavior reports

All vehicles must acquire the latest CRL – download or P2P

Stages in Misbehavior Processing

There are 4 stages in detecting and processing misbehaivor

escrypt
SECURITY. TRUST. SUCCESS.

Detection:
- Primarily done “on the road” by an OBE or RSE
- Cars may compare local sensors against V2V messages to decide what is “real”

Reporting:
- Devices submit signed misbehaviour reports to the MA

Investigation:
- MA looks for patterns to identify specific devices that are causing problems

Revocation:
- MA determines that a vehicle is misbehaving, the vehicle is added to the CRL which is distributed to all other vehicles

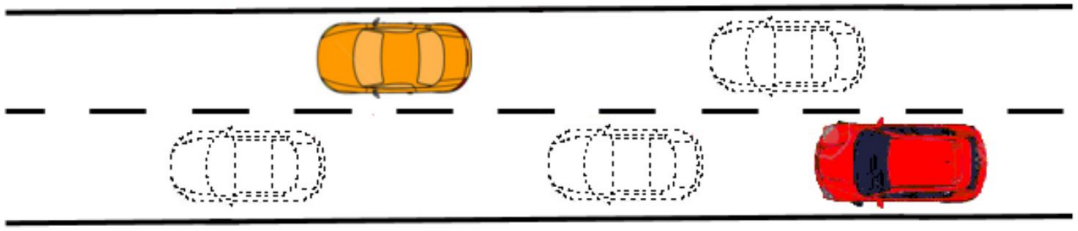
Local Misbehavior Detection (LMbD) performed by vehicle

Global Misbehavior Detection (GMbD) performed by MA

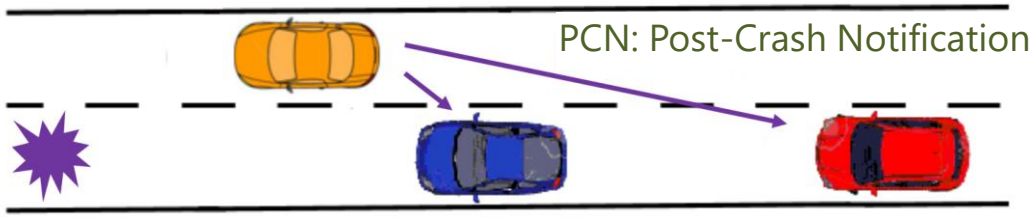
Examples of Misbehavior

escrypt
SECURITY. TRUST. SUCCESS.

- Misbehavior may be malicious, selfish, or due to faulty equipment
- Sybil Attack
  - A “selfish” car may send messages making it appear that it is in multiple locations, creating the appearance of congestion or causing other cars to clear the lane.



- False Alert
  - A car may indicate an accident ahead to divert traffic or induce an accident



Other Participants

escrypt
SECURITY. TRUST. SUCCESS.

Car Owners

- Details of the SCMS should be invisible to owners
- The system may notify owners if the system requires service or network connectivity

New and Used Car Dealers

- No need to "register" a device with an owner
- May be required to certify that safety systems are operating correctly before selling a vehicle

Repair Shops

- May need to trouble-shoot OBU problems
- Some may be authorized to re-enroll a revoked OBU

Commercial Fleet Operators

- May have a role in managing special applications for their own vehicles (overweight, hazardous freight, platooning, etc)

Regional DOTs and ITS Operators

- May run a local instance of SCMS under their own ICA
- Encouraged to enforce strict constraints on infrastructure devices (i.e. geo-fencing)

Law Enforcement

- Privacy protection puts limits on the use of BSMs for tracking of identification
- May use special equipment to identify revoked devices

Physical Security Requirements

All security components require FIPS 140-2 Level 3

escrypt
SECURITY. TRUST. SUCCESS.

- The Federal Information Processing Standard (FIPS) document number 140-2 is a standard that devices physical security and access control.
  - It defines 4 levels of physical security
- Currently, all SCMS back-end components must be compliant with FIPS 140-2 Level 3 security requirements
  - Level 3 requires strong “tamper resistance”
  - “compliant” is not the same as “certified”, may require less testing
  - Most V2X chipsets from leading vendors will meet this requirement

Special Restrictions for RSEs

Roadside equipment certificates apply special security constraints

escrypt
SECURITY. TRUST. SUCCESS.

- RSE certificates can have multiple constraints
  - **Application**: The RSE certificate defines what specific applications the device is allowed to support
  - **Validity Period**: Like all certificates, an RSE application can have a time-bounded validity period
  - **Operating Region**: An application certificate may define a geographic region (geo-fence) where the device is authorized to operate
- Trade-off of risk vs. complexity
  - Tight control of permissions reduces risk, but increases operational complexity

Is this sign valid in this location?

Does it have a valid application?

Has the application certificate expired?

Status of the V2X Mandate in the USA

The industry is still waiting for a mandate from the US DOT

escrypt
SECURITY. TRUST. SUCCESS.

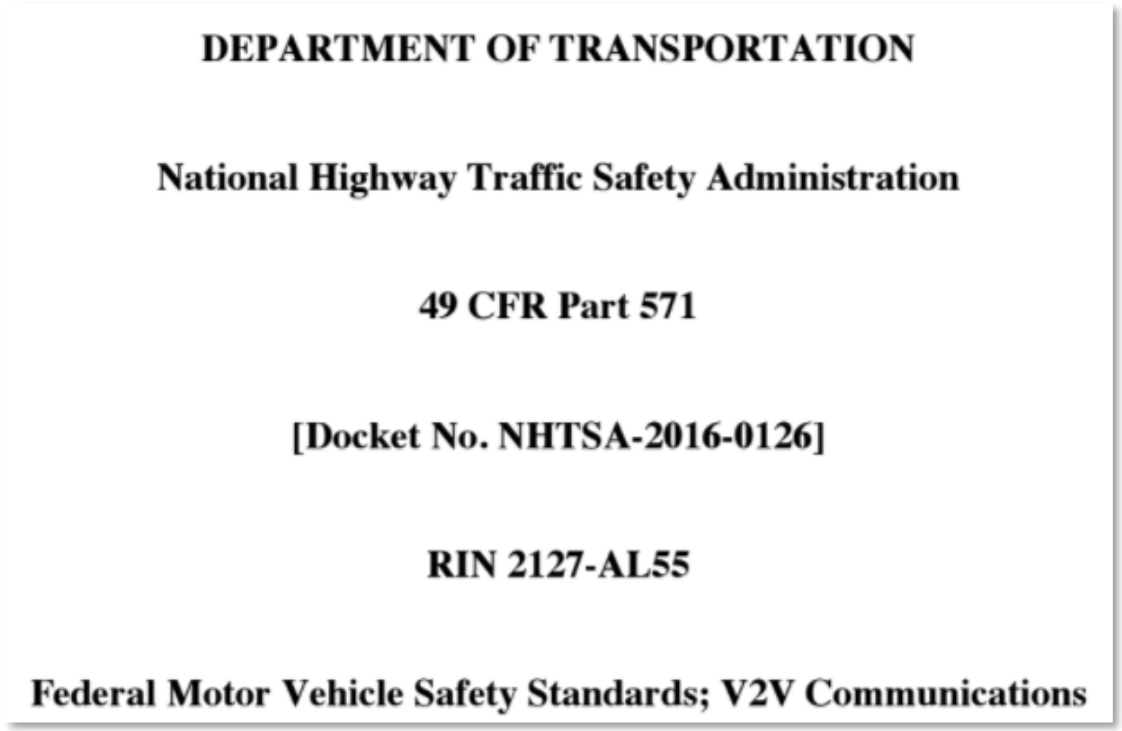
NPRM: Notice of Proposed Rule-Making

- Typically the last step before a new regulation is introduced
- Published in December, 2016
- Detailed review of past research and public comments
- Reference for nearly all aspects of V2X and the SCMS design
- The actual mandate has not yet been issued

5-Year Phase-in Period:

Table VIII-1 Proposed Lead Time and Phase-In Schedule

Time Period	Percentage of Vehicles
1 year after final rule	0%
2 years after final rule	0%
3 years after final rule	50%
4 years after final rule	75%
5 years after final rule	100%



DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

49 CFR Part 571

[Docket No. NHTSA-2016-0126]

RIN 2127-AL55

Federal Motor Vehicle Safety Standards; V2V Communications

Current Status of the SCMS

The US DOT supports 3 versions of the SCMS today

escrypt
SECURITY. TRUST. SUCCESS.

- There are 3 distinct instances of the SCMS:
  - Production (PROD) – supports production vehicles
  - Proof of Concept (POC) – intended for PoC pilot use only
  - Development (DEV) – intended only for ongoing development and testing

- The DoT has a goal of migrating CV Pilot devices and vehicles over to the PROD environment after the end of the pilot phase.
  - Details on how to do this are still being worked evaluated

SCMS Test System Online

escrypt
SECURITY. TRUST. SUCCESS.

- ESCRYPT hosts a test platform for validating SCMS transactions:
  - https://scms.trustpoint.ca

- System provides reference documentation and sample data with a live API interface