TODAY’S AGENDA

- Connected Vehicle Pilot Deployment Program Overview
- Communication Security Context
- Security and Credential Management System (SCMS) Overview
- USDOT SCMS Support of CV Pilots
- Stakeholder Q&A
Connected Vehicle Pilot Deployment Program Overview
PROGRAM GOALS

Spur Early CV Tech Deployment
Wirelessly Connected Vehicles

Measure Deployment Benefits
Safety

Resolve Deployment Issues
Technical

Mobile Devices

Infrastructure

Environment

Mobility

Institutional

Financial
ORGANIZING PRINCIPLES AND REQUIREMENTS

▪ Organizing Principles
  □ Problem-Driven
  □ Multiple Pilot Sites
  □ Large-Scale and Multi-Modal
  □ Multiple Applications Deployed Together

▪ Deployment Requirements
  □ Multiple Forms of Communication Technologies
  □ Data Capture and Sharing
  □ Quantifiable Performance Measures
  □ Security and Credentialing Management System (SCMS)
# Connected Vehicle Applications

## V2I Safety
- Red Light Violation Warning
- Curve Speed Warning
- Stop Sign Gap Assist
- Spot Weather Impact Warning
- Reduced Speed/Work Zone Warning
- Pedestrian in Signalized Crosswalk Warning (Transit)

## V2V Safety
- Emergency Electronic Brake Lights (EEBL)
- Forward Collision Warning (FCW)
- Intersection Movement Assist (IMA)
- Left Turn Assist (LTA)
- Blind Spot/Lane Change Warning (BSW/LCW)
- Do Not Pass Warning (DNPW)
- Vehicle Turning Right in Front of Bus Warning (Transit)

## Agency Data
- Probe-based Pavement Maintenance
- Probe-enabled Traffic Monitoring
- Vehicle Classification-based Traffic Studies
- CV-enabled Turning Movement & Intersection Analysis
- CV-enabled Origin-Destination Studies
- Work Zone Traveler Information

## Environment
- Eco-Approach and Departure at Signalized Intersections
- Eco-Traffic Signal Timing
- Eco-Traffic Signal Priority
- Connected Eco-Driving
- Wireless Inductive/Resonance Charging
- Eco-Lanes Management
- Eco-Speed Harmonization
- Eco-Cooperative Adaptive Cruise Control
- Eco-Traveler Information
- Eco-Ramp Metering
- Low Emissions Zone Management AFV Charging / Fueling Information
- Eco-Smart Parking
- Dynamic Eco-Routing (light vehicle, transit, freight)
- Eco-ICM Decision Support System

## Road Weather
- Motorist Advisories and Warnings (MAW)
- Enhanced MDSS
- Vehicle Data Translator (VDT)
- Weather Response Traffic Information (WxTINFO)

## Mobility
- Advanced Traveler Information System
- Intelligent Traffic Signal System (I-SIG)
- Signal Priority (transit, freight)
- Mobile Accessible Pedestrian Signal System (PED-SIG)
- Emergency Vehicle Preemption (PREEMPT)
- Dynamic Speed Harmonization (SPD-HARM)
- Queue Warning (Q-WARN)
- Cooperative Adaptive Cruise Control (CACC)
- Incident Scene Pre-Arrival Staging Guidance for Emergency Responders (RESP-STG)
- Incident Scene Work Zone Alerts for Drivers and Workers (INC-ZONE)
- Emergency Communications and Evacuation (EVAC)
- Connection Protection (T-CONNECT)
- Dynamic Transit Operations (T-DISP)
- Dynamic Ridesharing (D-RIDE)
- Freight-Specific Dynamic Travel Planning and Performance
- Drayage Optimization

## Smart Roadside
- Wireless Inspection
- Smart Truck Parking
### CV PILOTS DEPLOYMENT SCHEDULE AND RESOURCES

- **Proposed CV Pilots Deployment Schedule**

<table>
<thead>
<tr>
<th>Schedule Item</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regional Pre-Deployment Workshop/Webinar Series</td>
<td>Summer-Fall 2014</td>
</tr>
<tr>
<td>Solicitation for Wave 1 Pilot Deployment Concepts</td>
<td>Early 2015</td>
</tr>
<tr>
<td>Wave 1 Pilot Deployments Award(s)</td>
<td>September 2015</td>
</tr>
<tr>
<td>Concept Development Phase (up to 12 months)</td>
<td></td>
</tr>
<tr>
<td>Design/Build/Test Phase (up to 20 months)</td>
<td></td>
</tr>
<tr>
<td>Operate and Maintain Phase (18 months)</td>
<td></td>
</tr>
<tr>
<td>Solicitation for Wave 2 Pilot Deployment Concepts</td>
<td>Early 2017</td>
</tr>
<tr>
<td>Wave 2 Pilot Deployments Award(s)</td>
<td>September 2017</td>
</tr>
<tr>
<td>Concept Development Phase (up to 12 months)</td>
<td></td>
</tr>
<tr>
<td>Design/Build/Test Phase (up to 20 months)</td>
<td></td>
</tr>
<tr>
<td>Operate and Maintain Phase (18 months)</td>
<td></td>
</tr>
<tr>
<td>Pilot Deployments Complete</td>
<td>September 2020</td>
</tr>
</tbody>
</table>

- **Resources**
  - ITS JPO Website: [http://www.its.dot.gov/](http://www.its.dot.gov/)
  - CV Pilots Program Website: [http://www.its.dot.gov/pilots](http://www.its.dot.gov/pilots)
CV PILOTS
WEBSITE

http://www.its.dot.gov/pilots
Communication Security Context
UNIFIED IMPLEMENTATION OF CVRIA – REGIONAL SCALE

- **Architecture**

- **Concept of Operation** – *Preserving privacy by design*

- **Design Elements** – Agreement on standards usage, common communication security practice
  - **Vehicle Situation Data, Field Situation Data**
    - Broadcast and bundle-based
    - Intersections and other roadside infrastructure installations
  - **Traveler Situation Data**
    - Multiple delivery media
  - **Peer-to-Peer Data Exchanges**
    - Maintenance, Management, Enforcement, Commercial
COMMON PARTS, COMMON TOOLS

- Architecture
- Concept of Operation
- Design Elements
  - Objects
  - Information Flows
  - Relationships
CONNECTED VEHICLE VISION – COMMUNICATION SECURITY

- Complete System

- Comprehensive Communication Security
  - Common Cryptographic processes

- Trust Establishment, Confidentiality Protection
  - Independent of medium or message
LEGACY COMMUNICATIONS

- Legacy communication protocols are allowed.
- It will be up to the implementer to show that trust is established and confidentiality (privacy) is maintained.
Physica1 Security

- Each object MUST have adequate physical security.

- Communication security does not assure physical security.
OPPORTUNITY FOR A COMMON EXPERIENCE

- Started with crash avoidance
- Extending to interaction with field devices and data to/from back offices
Security and Credential Management System (SCMS) Overview
PRIVACY/ANONYMITY CONCERNS

- Formulated to **protect the privacy** of the users to the highest possible degree possible.

- Challenging In a multi-application setting, because
  - The user may have higher privacy requirements than a specific application does,
  - There is an additional threat to the privacy of the user from **correlations between applications**.

- Some applications by their nature will have to reveal sensitive or user-specific information: for example, BSMs reveal vehicle location.
  - This makes it all the more important to ensure that **applications do not reveal this information** unless it is absolutely necessary, as revealing the information within **application A will allow it to be correlated with information from application B**.

- Further discussion of privacy and security for the multi-application setting can be found in EU-US ITS Task Force Standards Harmonization Working Group Harmonization Task Group 1 report 1-1, “Current Status of Security Standards”, section 14 and Annex C.
**SERVICE DISCOVERY**

- Authorization
  - The definition of “authorized to use the service” will be application specific.

**PRIVACY**

- **Not** require either party to reveal sensitive information unencrypted.
- **Not** contain the User’s location information unless this is necessary as part of service.
- **Not** use identifiers that can be straightforwardly linked to the User’s real-world identity (VIN, license number, etc.).
- Use temporary and one-time identifiers. Separate instances of the exchange shall not use identifiers (USER MAC address, UE-ID (IMEI), IP address, certificate, temporary ID, session ID, etc.) that have been used in a previous instance of the exchange.

**INTEGRITY**

- Replay / message order
- Non-repudiation / Audit

**PERFORMANCE**

- Removal of Misbehaving Objects
TRANSACTIONAL UNICAST COMMUNICATIONS, CONT.

- **Service Discovery**
- **Authorization**
  - The definition of “authorized to use the service” will be application specific.
- **Privacy**
  - Not require either party to reveal sensitive information unencrypted.
  - Not contain the User’s location information unless this is necessary as part of service provision or necessary for the server to verify that the user is authorized to use the service.
  - Not use identifiers that can be straightforwardly linked to the User’s real-world identity (VIN, license number, etc.).
  - The exchange shall, as far as practical, use temporary and one-time identifiers. Separate instances of the exchange shall, as far as practical, not use identifiers (USER MAC address, UE-ID (IMEI), IP address, certificate, temporary ID, session ID, etc.) that have been used in a previous instance of the exchange.
- **Integrity**
- **Replay / message order**
- **Non-repudiation / Audit**
- **Performance**
- **Removal of Misbehaving Objects**
COMMUNICATION SECURITY

- Common communication security approach

- 1609.2 will be used between mobile objects and field and center objects

- USDOT will provide the Security Credential Management System
SCMS IN THE CV PILOTS

- **Definition**
  - A system to ensure the trusted communications between mobile devices and other mobile devices and/or roadside devices and back offices, and protect the confidentiality and integrity of data as it moves through a variety of media.

- **CV Pilots Requirements**
  - Develop a security management operating concept to describe the underlying needs of the pilot deployment to ensure secure operations, and outline a concept that addresses these needs.

- **USDOT’s Role on SCMS**
  - USDOT will provide a prototype national-level SCMS system. The security management operating concept must include an interface with this capability.
STAKEHOLDER FEEDBACK ON SCMS

What we heard from the stakeholders during the CV Pilots Workshop on April 30, 2014

- Should USDOT provide a working security design?
  - Consensus: Yes, sites need this level of support. Also, there should be commonality across the pilots. Some commented that some flexibility for innovative approaches should be allowed
- Consider specifying existing standards for physical security (e.g., FIPS-140 level 2); also must consider security interconnected legacy systems
- Are the goals of the CV pilots to test applications (only), security (only), or both in combination? This drives some of the SCMS answers
- Consider running a separate series of tests for alternative security approaches
USDOT SCMS Support of CV Pilots
CURRENT PROJECT SUPPORT PROCESS

- The Test Bed team supports creation and distribution of cryptographic material for mobile and fixed equipment.
  - “5 minute” and “pooled” certificates for mobile; fixed time certificates for fixed devices.
- Reference code for back office installations.
- Submit the completed form to Rhian.M.Merris@leidos.com, using a signed email. (A signed email is required so encrypted email can be used to provide to you the RSU Certificates.)
FOR MORE INFORMATION

Virtual Plug Fests – October to December 2014

Walton Fehr
Program Manager, Systems Engineering
ITS Joint Program Office
USDOT
walton.fehr@dot.gov
Stakeholder Q&A