

Connected Vehicle Implementation and Institutional Issues

Presentation to the ITS Program Advisory Committee
By Valerie Briggs, ITS JPO
October 11, 2012
Ann Arbor, MI

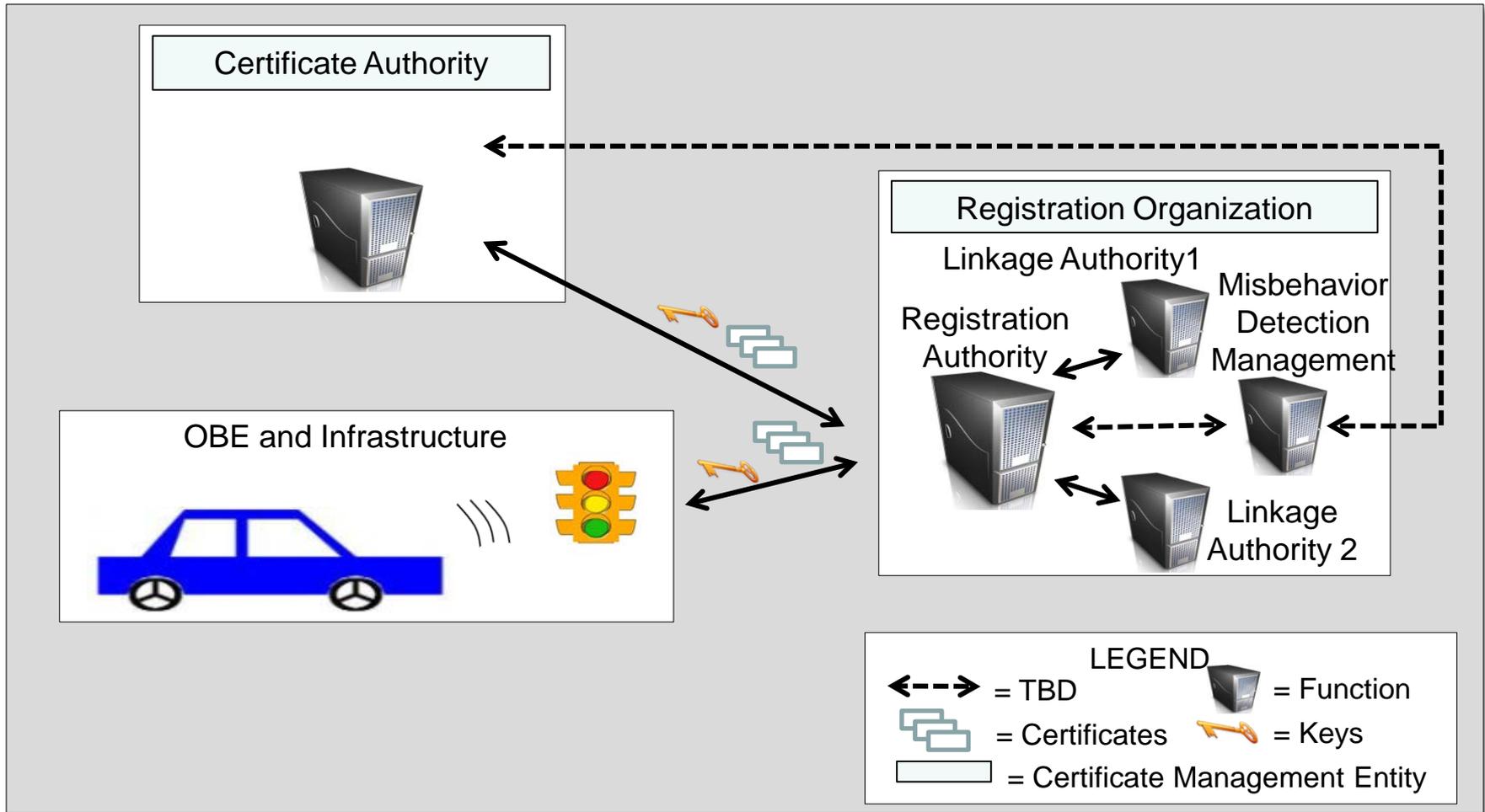
Implementation Needs

- Security Back Office Functions – For issuing and management of security credentials and certificate management
- Communications Network – Necessary after first three years for updating certificates and certificate revocation lists to all valid system users
- Applications Infrastructure – Infrastructure specifically for V2I safety (DSRC) or V2I mobility (other options)
- On Board Equipment – Interoperable equipment in vehicles to enable communication with the vehicle for above functions

All require sustainable funding

Security Credential Management System (SCMS)

SCMS represents the entire system, and CMEs house the functions



Organizational Implications of the SCMS

Organizational, Institutional, and Policy Considerations

- ▶ Different organizational models are being considered for the system
- ▶ Current analysis based on new design
- ▶ Major cost drivers of SCMS:
 - Hardware and software needs (~50-60% of total costs)
 - Numbers of physical locations of functions and organizations
 - Choice of organizational model – oversight, management, and efficiency
- ▶ Various ownership options being analyzed
 - Public-private partnership, all private
 - Will impact organizational models and costs
- ▶ If or how PII may be collected as part of registration into the system is being analyzed
- ▶ Internal controls and policies needed to protect security and privacy are being analyzed

Communications System for Security

- **Four scenarios currently exploring:**
 - Mostly cellular system
 - Mostly cellular with some installation of DSRC RSE
 - “All DSRC”
 - CAMP Phased Deployment Scenarios

- All findings based on preliminary consultant analysis.

Communications System for Security

▪ Cost Drivers:

- Communications costs appear to be substantially greater than the costs of operating the certificate management entity.
- **On-Board Equipment (OBE):** significant cost in all scenarios
 - Interaction with security system requires different cellular modem in the vehicles than exist today
 - DSRC network requires two DSRC radios
 - Costs vary slightly for each scenario due to differing subcomponents and power consumption needs

Communications System for Security

▪ **Cost Drivers (Continued):**

- **Cellular:** significant cost in scenarios that rely on it for delivery of certificates and revocation lists
 - Highly sensitive to changes in misbehavior rate, data size, and peak pricing
 - Insufficient coverage in rural and some other areas
 - Appears to have significantly higher cost than other scenarios
 - Biggest cost driver: delivery of the certificate revocation list
- **Satellite Radio:**
 - Broadcast capability only
 - Potentially lowers cellular costs when used to distribute the CRL

Communications System for Security

- **Cost Drivers (Continued):**

- **Roadside Equipment (RSE):** significant cost in the “all DSRC” scenario

- For an “All DSRC” scenario, the number of RSEs nationwide depends on risk tolerance and coverage requirements:

- Estimates vary from 1300 RSEs to 150,000 RSEs

- Unanswered Questions:

- What level of coverage is acceptable?

- How frequently must a vehicle interact with the system?

- **CAMP Phased Deployment Scenario**

- Delays costs but doesn't necessarily change ultimate needs

Communications System for Security

- **Technical Performance and Implementation Challenges**
 - **Certificate Revocation List Distribution**
 - Technically demanding for DRSC scenario (increases CME back office costs but not necessarily DSRC network costs)
 - Most significant cost driver for cellular cost scenarios
 - “Misbehavior” rate determines size of CRL
 - **DSRC RSE Installation, Operation and Maintenance**
 - Significant challenges for DRSC options
 - Placement in state or locally owned equipment cabinets and rights-of-way would require a significant implementation permitting, coordination and system integration effort
 - Placement of RSE on private property may be an alternative but would also require a strategy for implementation



Applications Infrastructure

- Needs for V2I Safety Applications
- Needs for Mobility and Environmental Applications
- AASHTO National Connected Vehicle Field Infrastructure Footprint Analysis
 - Preliminary concept for field infrastructure deployed by state & local agencies
 - Could be used by private consortia to design, build, operate, finance
 - Compelling justification of agency value
 - Provide tools for engaging state agencies
 - Bring into focus applications that are of the greatest value to agencies

Legal Policy - Scope of Authority

- NHTSA has authority to support:
 - Key aspects of V2V communications
 - Regulation of critical equipment, messages and applications if related to safety
 - Provision of the security required to support a V2V rule by a non-Federal entity, as through a procurement or other form of agreement or indirectly via a V2V regulation
- FHWA does not have authority to require installation of roadside infrastructure



Questions

- Does a secure system for two-way data communication to vehicles have value for commercial purposes as well as for safety?
- What factors influence this value?
- What are potential business models to support a security system for active safety?