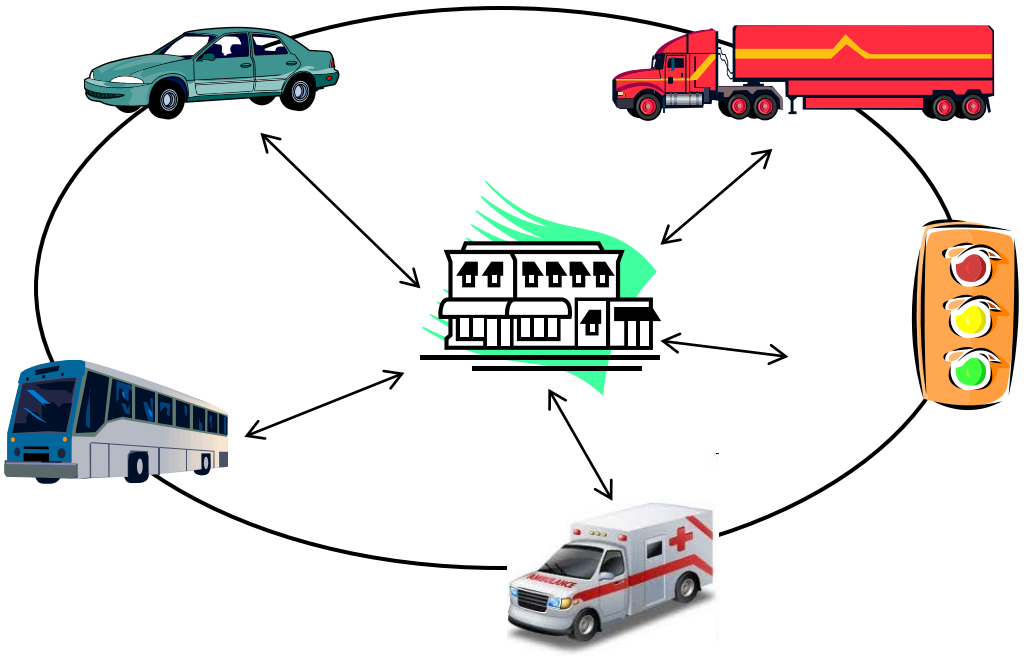
UNITED STATES
DEPARTMENT OF TRANSPORTATION

Connected Vehicle Security

ITS Advisory Committee
May 24, 2012

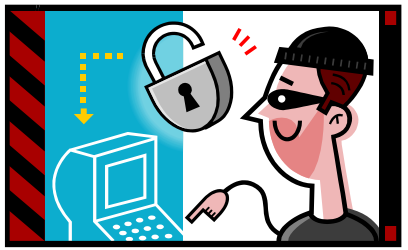
Valerie Briggs
ITS Joint Program Office, RITA, USDOT

Need for Security



Trust

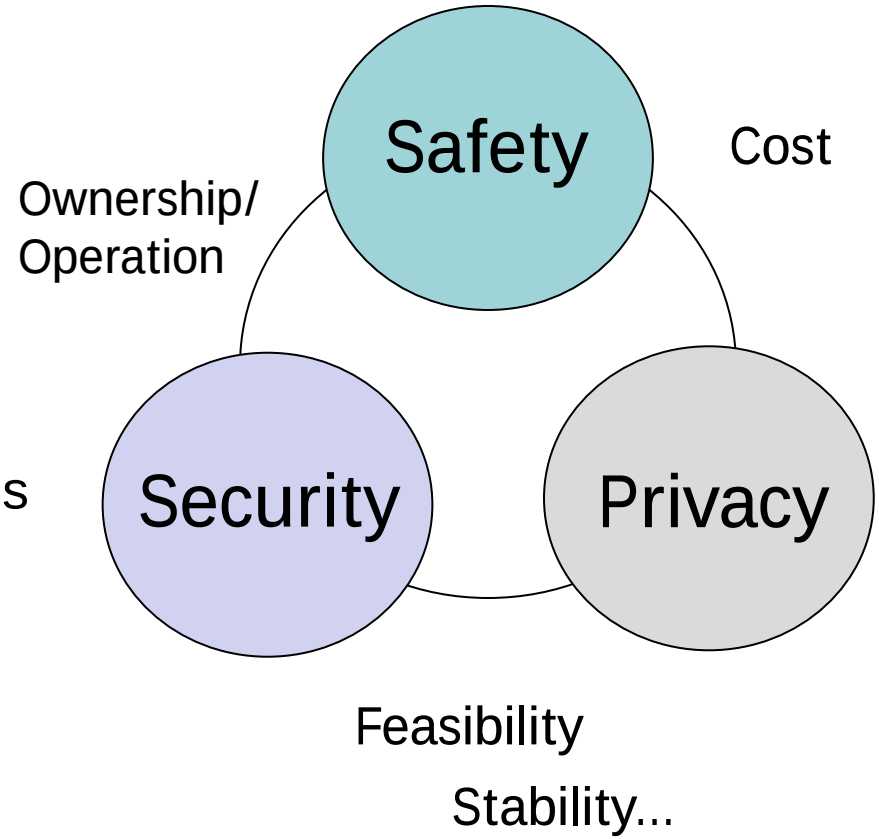
Message Validity



Defense Against Attacks

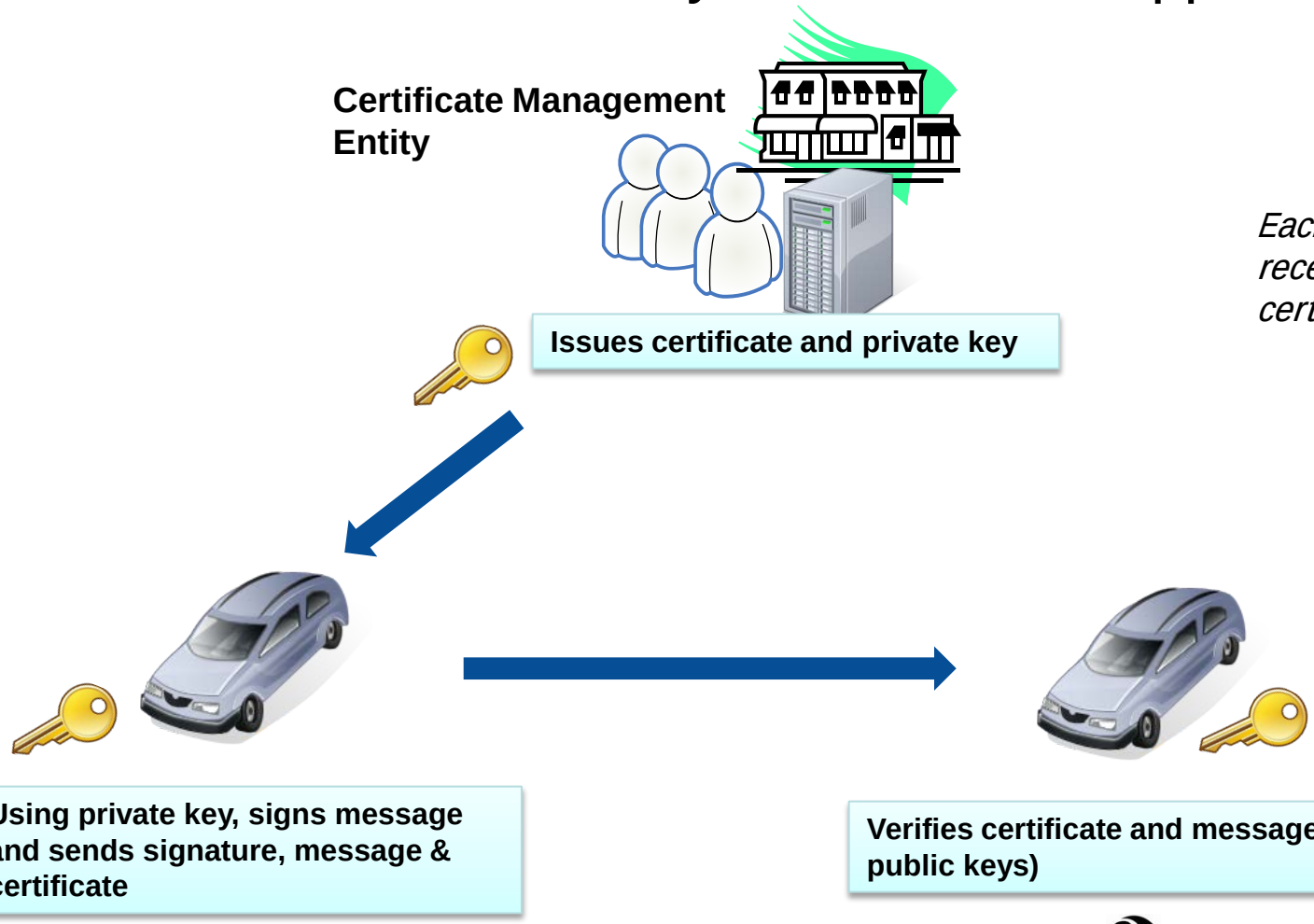
Goals for Security System

- ✓Trust
- ✓Message validity
- ✓Protection against attacks
- ✓Appropriate user privacy
  - ✓ Non-traceability for trips
  - ✓ Personal information protections
- ✓Implementable



Proposed Security Approach

Modified Public Key Infrastructure Approach



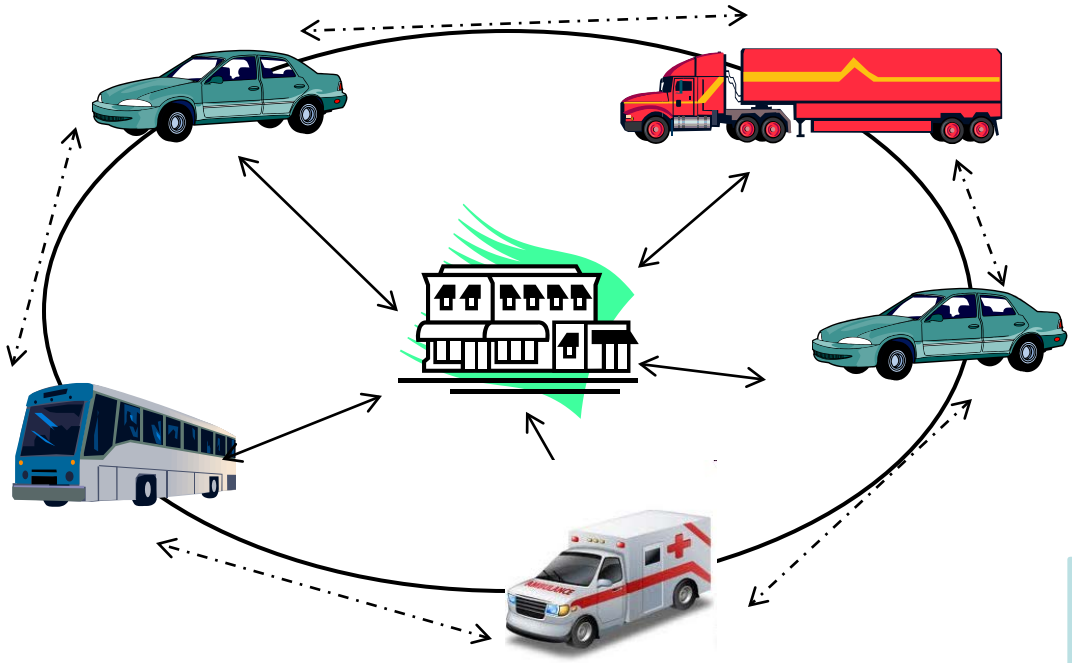
Each device potentially receives thousands of certificates per year

Generally, System Would Include:

- Security Network – for credentialing and certificate management
- Security Back Office (Certificate Management Entity) – operational functions that apply across any type of Security Network
- Applications Infrastructure – Infrastructure specifically for V2I safety (DSRC) or V2I mobility (other options)

All require sustainable funding

Overall Security System Components

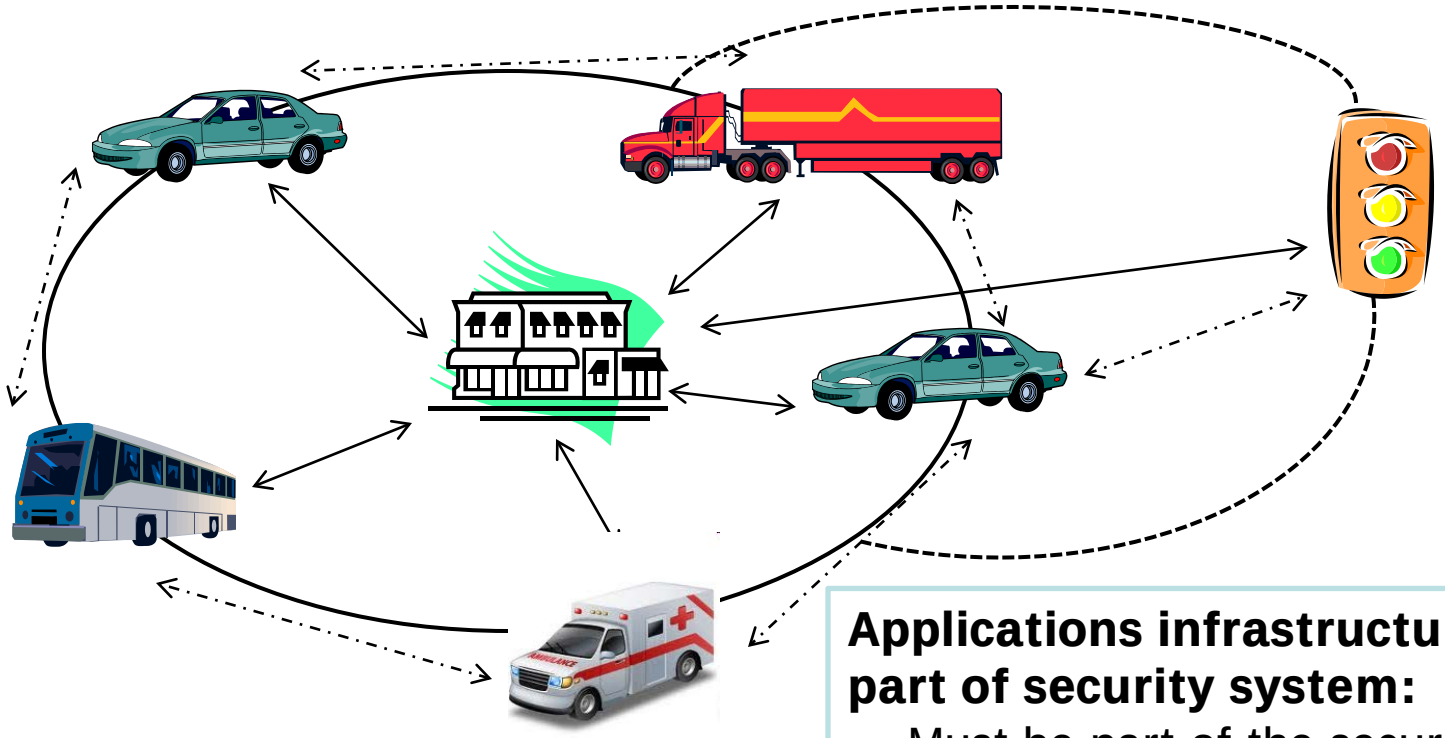


V2V communication via DSRC

Security Network Options:
- Cellular/hybrid
- DSRC
- Other

Security Back Office Functions
- Manage operations
- Certify processes & equipment
- Revocation

Security System & Security Infrastructure



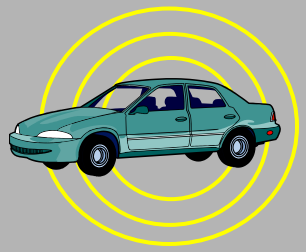
V2V communication
Via DSRC

Applications infrastructure as a part of security system:

- Must be part of the security network
- Adhere to performance requirements
- Adhere to system governance
- Adhere to certification requirements

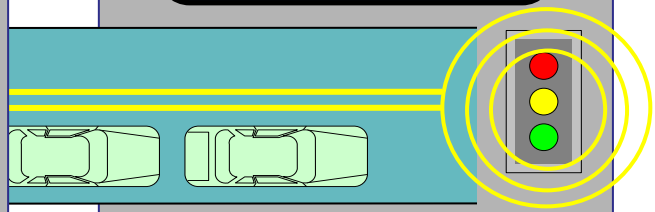
Connected Vehicle Communications Needs

Vehicle To Vehicle



- Safety messages
- Certificate exchanges

Vehicle To Infrastructure



- Many needs – safety and mobility application needs differ

Security Management

- Security credentials updating and management
- Volume of data may be substantial

Communication exchanges are distinct, which complicates a "one-size fits all" approach

Media Options for Communication Needs

Cellular	Wide area two-way mobile communications based on point to point mode (not broadcast)
	Voice and data oriented with high-speed data transfer rates; requires IP addressing
WiFi Technology	Provides internet access to devices in range of base station footprint (typical range 100 feet)
	Typically takes ~ 10 seconds to recognize devices in network (too slow for some CME functions?)
Dedicated Short-Range Communications (DSRC)	Designed specifically for communicating data with moving vehicles
	Allows terminals to broadcast to all other devices in radio range (range ~ 300 meters)

Study Scenario 1: Hybrid

Certificate Management	**Cellular**
V2I Mobility Data	**Cellular**
V2V and V2I Safety Data	**DSRC**

- Uses cellular data delivery for Certificate Management (CM) and V2I communications, and the DSRC network for the V2V communications
- Will examine potential efficiencies and costs of using two different networks for data delivery, and its ability to deliver CM functions

Study Scenario 2: Hybrid

Certificate Management	**Any and all opportunities: Cellular, WiFi and DSRC**
V2I Mobility Data	**Cellular and DSRC**
V2V and V2I Safety Data	**DSRC**

- Relies on the wireless ecosystem to provide certificate data exchange needs
- Must determine practicality: technical and deployment paths with data exchange functions important (e.g., OBE must have radio that can receive the right wireless connection)

Study Scenario 3: All DSRC

Certificate Management	**DSRC**
V2I Mobility Data	**DSRC**
V2V and V2I Safety Data	**DSRC**

- Relies on DSRC to provide the wireless data communications needed for each of the operational functions of the certificate data exchange system
- Need to determine incremental or additional costs of building DSRC network to deliver certificate communication needs

Ongoing Work

- Evaluating costs and organizational models for certificate management entities
  - Exploring private, or hybrid models
- Evaluating security network and communications options and costs
- Assessing how strategies effect security, privacy, and safety
- Assessing business/investment models for implementation and ongoing expenses
- Conducting a field test using prototype security system (Safety Pilot)

Questions?

For More Information

- http://www.its.dot.gov/connected_vehicle/connected_vehicle_policy.htm

www.its.dot.gov