Connected Vehicle Communications Security in the Southeast Michigan 2014 Project

(P14-6161)

Walton Fehr
USDOT Research and Innovative Technology Administration
ITS Joint Program Office
January 14, 2014

Highlights

In transportation-related applications, we understand that:

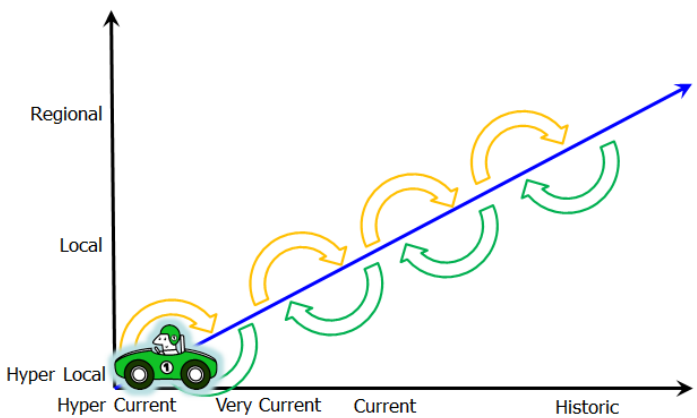
- Applications are satisfied by the exchange of small amounts of data.
- Operators of vehicles want to remain anonymous.
- Vehicles move all over the country.

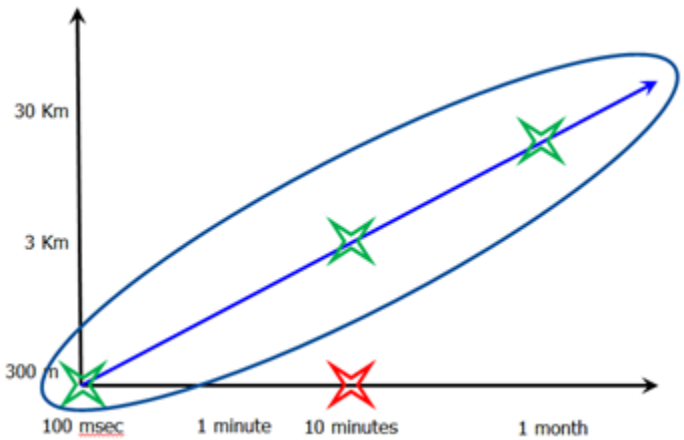
In the Southeast Michigan 2014 Project, we want to:

- Assure trust in data exchanged,
- Protect the confidentiality of certain data exchanged, and
- Protect the anonymity and privacy of individuals while
- Operating a Multi-Application, Multi-Industry, Multi-Medium Environment.

Fundamentals

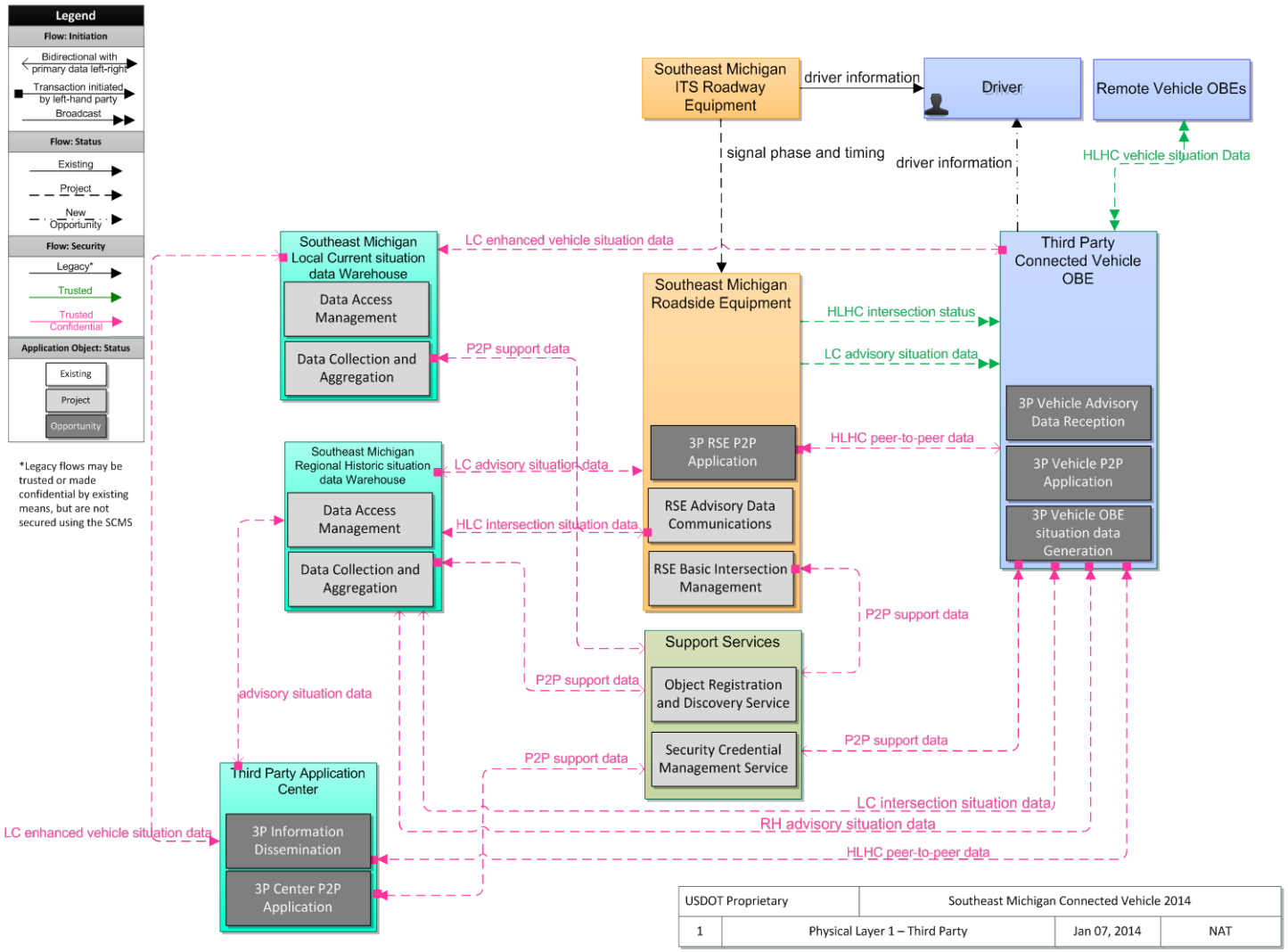
- **Situation Data**
  - The <u>state</u> of a key element of the system <u>at a specific time</u>
  - Defining the data <u>flow and evolution</u>
- **Time and Place** Context to Data and Information





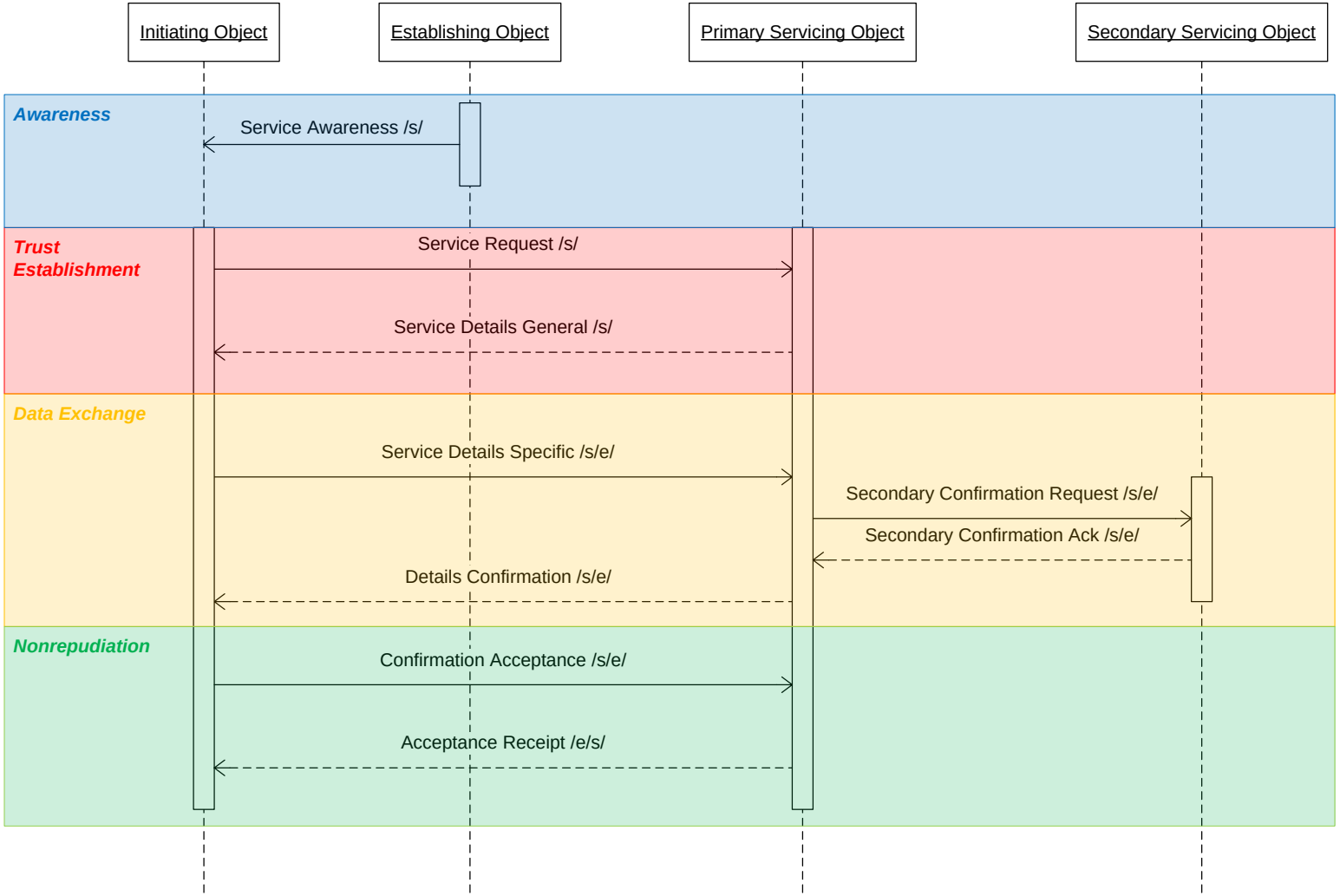
- **Data Flow and Evolution**, Independent of Medium
- **Common Cryptographic Processes** to Assure Trust and Protect Ownership

Example: Southeast Michigan 2014, Physical View



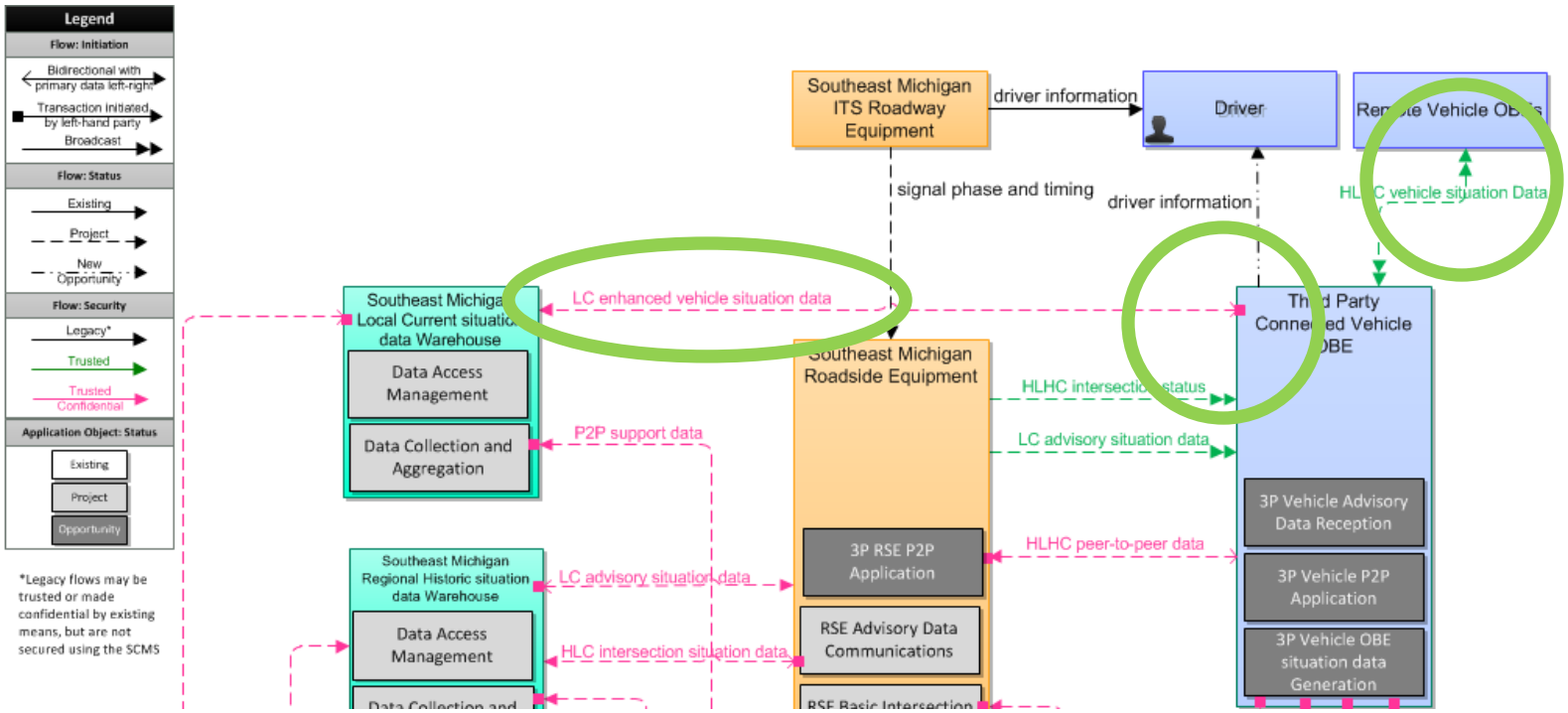
U.S. Department of Transportation
Research and Innovative Technology Administration

Message Sequence



Communication Security Concept

- Common cryptographic processes
- Independent of medium



Information Flow Definitions

LC enhanced vehicle situation data Message Sequence

2.3.1.1 1609.2

The VehicleServiceRequest Secured APDU is a 1609Dot2Data structure of type signed, containing a SignedData with the following fields:

- signer is always of type certificate and contains a certificate with PSID 0xAFE0
- unsigned_data has the following fields:
  - generation_time: included
  - psid=0xAFE0
  - expiry_time, generation_location, extensions, other_data: omitted
  - payload: a VehicleServiceRequest structure as defined in the next section.

2.3.1.2 VehicleServiceRequest message Details

The VehicleServiceRequest APDU detailed in Table 1.

```
VehicleServiceRequest ::= SEQUENCE {
      msgID        DSRCmsgID,        --msgID for VehicleServiceRequest is 0x8B
}
```

Table 1: VehicleServiceRequest APDU

Contact Information

- Walton Fehr
- walton.fehr@dot.gov http://www.its.dot.gov
- Tool: http://www.iteris.com/cvria/html/resources/tools.html

- **Affiliated Test Bed Program**
- **Watch for Plugfest information**
- **First face-to-face event January 29, 2014**