U.S. Department of Transportation

Connected Vehicle PlugFest

Communication Context, Security Requirements

Time and Place Context,

Preserving “Privacy by Design”

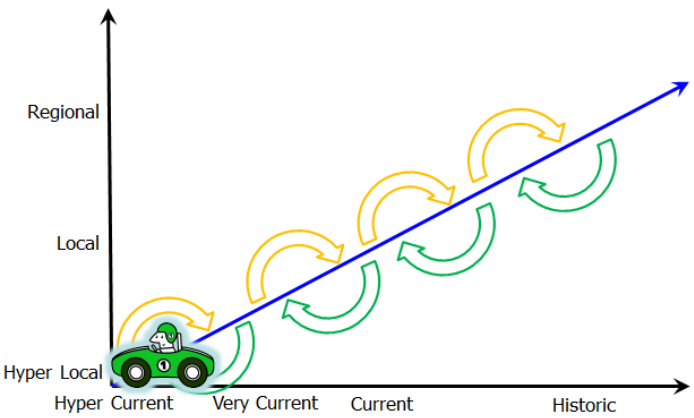
PlugFest

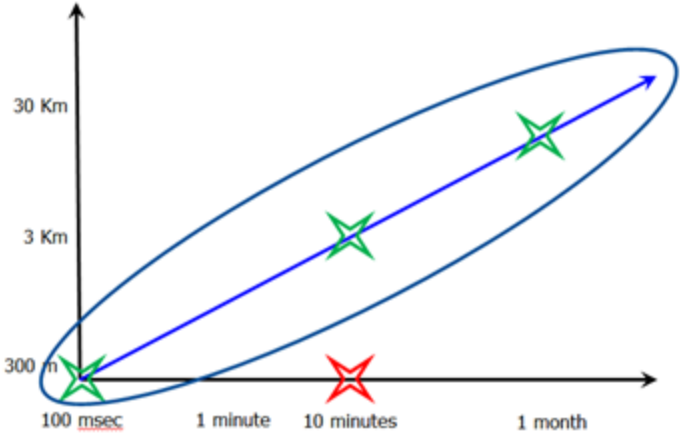
May 13 - 15, 2014

Southeast Michigan

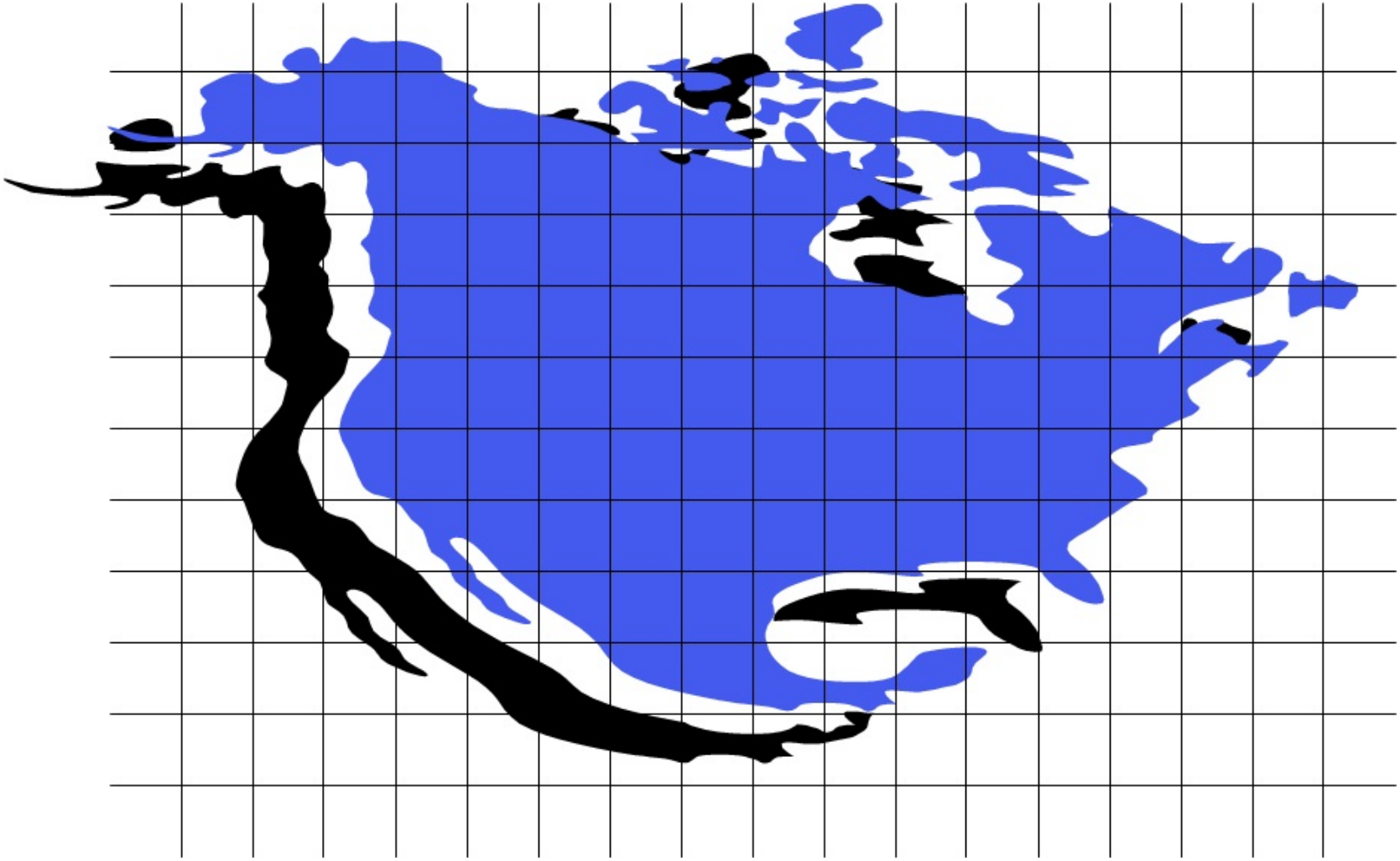
Time and Place Context

- **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





Uniform Implementations



Source: USDOT

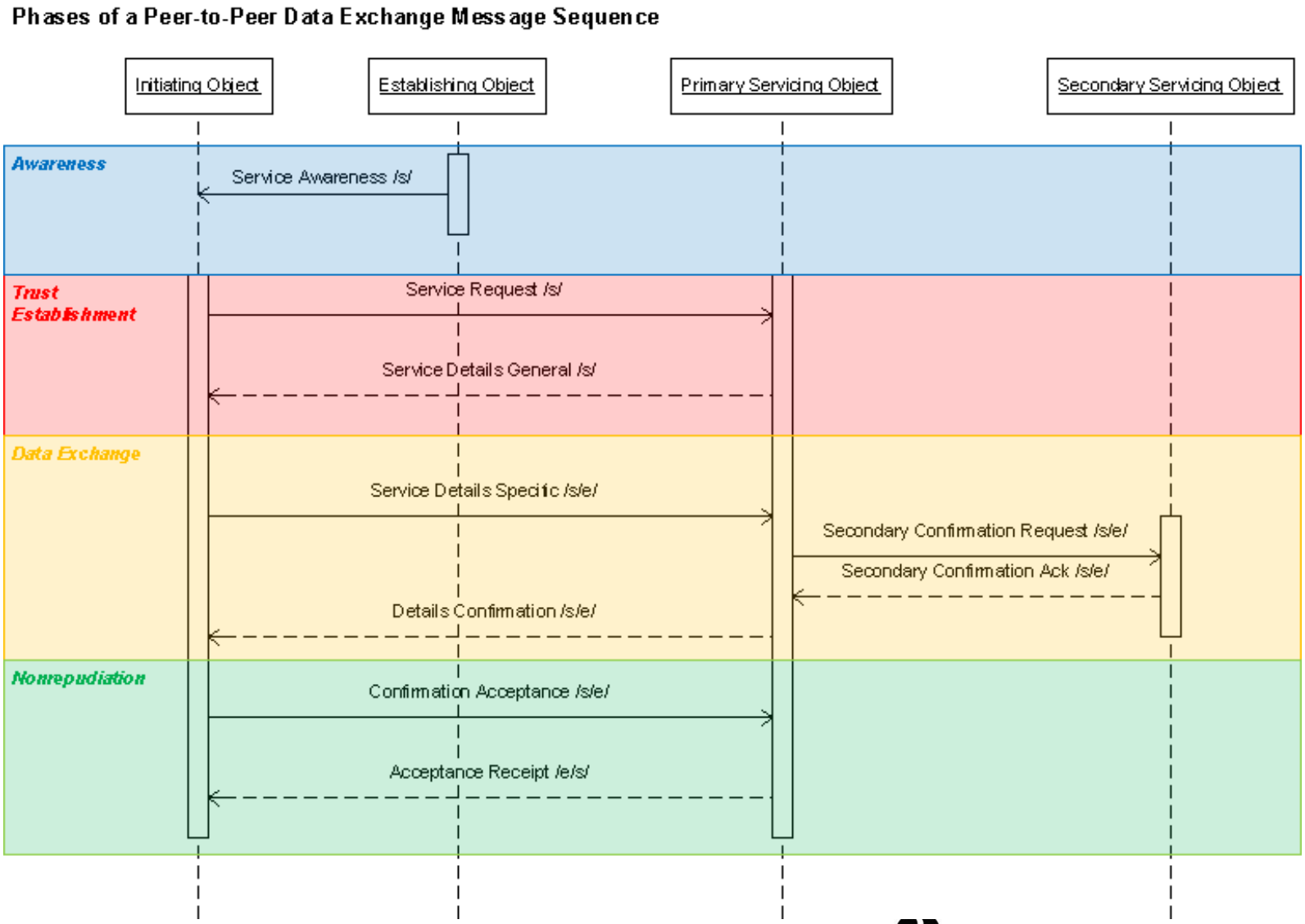
Communication Types

- Two types of communication patterns that support applications:
  - Broadcast and
  - Transactional. (Peer-to-Peer)
- Broadcast-
  - Sent unencrypted, Intended to be consumed by any receiver in the vicinity.
  - Examples of broadcast communications are BSM, SPaT, MAP.
  - *NOTE: All broadcast messages will be signed immediately before the final transmission. In other words, if a APDU originates at a server and is sent to an RSE for broadcast, it will be signed by the RSE as part of the complete message.*
- Transactional-
  - Between two objects for the purposes of carrying out some transaction.
  - Small data transfers (up to approx. 10 Kbytes).
  - *NOTE: Does not cover larger data transfers that need to be handed off between multiple RSU sessions.*
- *Does not consider groupcast communications.*
- *Does not consider the need for device physical security.*
- *Does not address data protection at endpoints, for example encryption of databases. Assumed that endpoints that store Personal Identifiable Information (PII) shall take appropriate measures to protect that PII.*

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.

Transactional Unicast Communications



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**

Broadcast Communications

- **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**