Communication Context, Security Requirements, Something Big

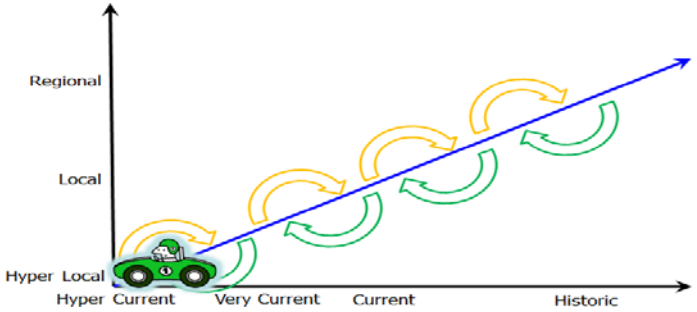
Time and Place Context,

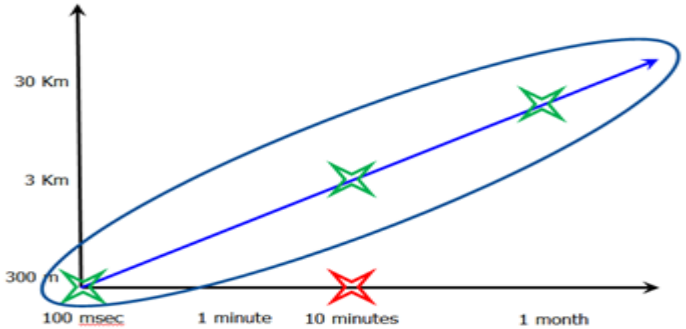
Preserving “Privacy by Design”

Fitting into the Big Picture

Time and Place Context

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

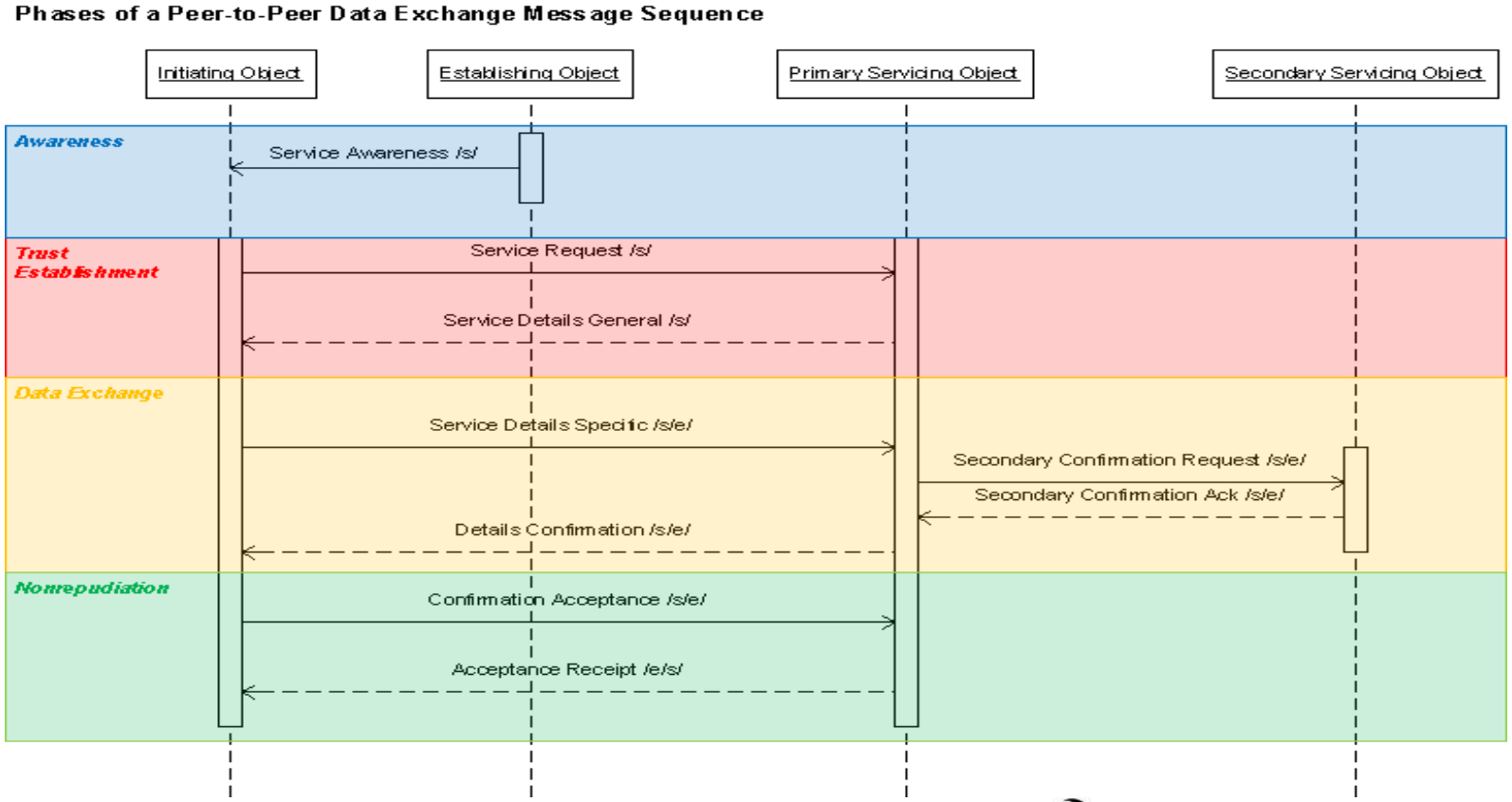




Privacy/Anonymity Concerns

- 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**

Internet of Something Big

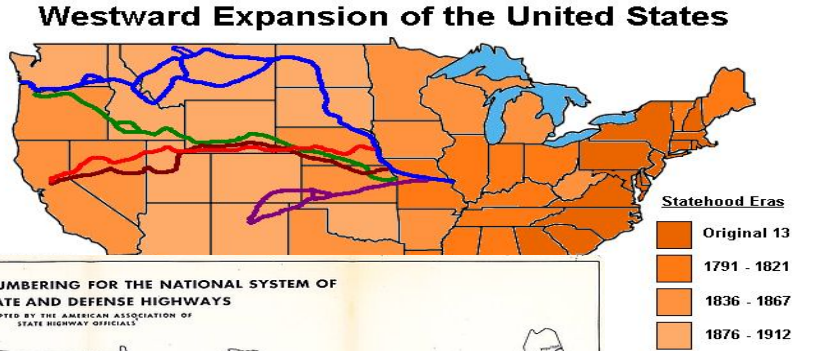
Internet of things

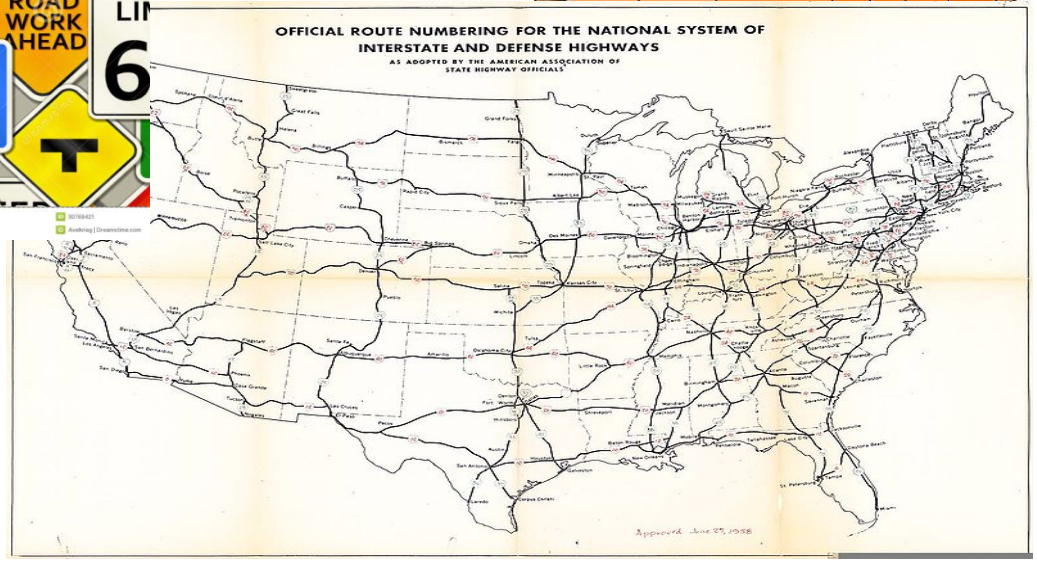
Many
Different
Local

Internet of Something Big

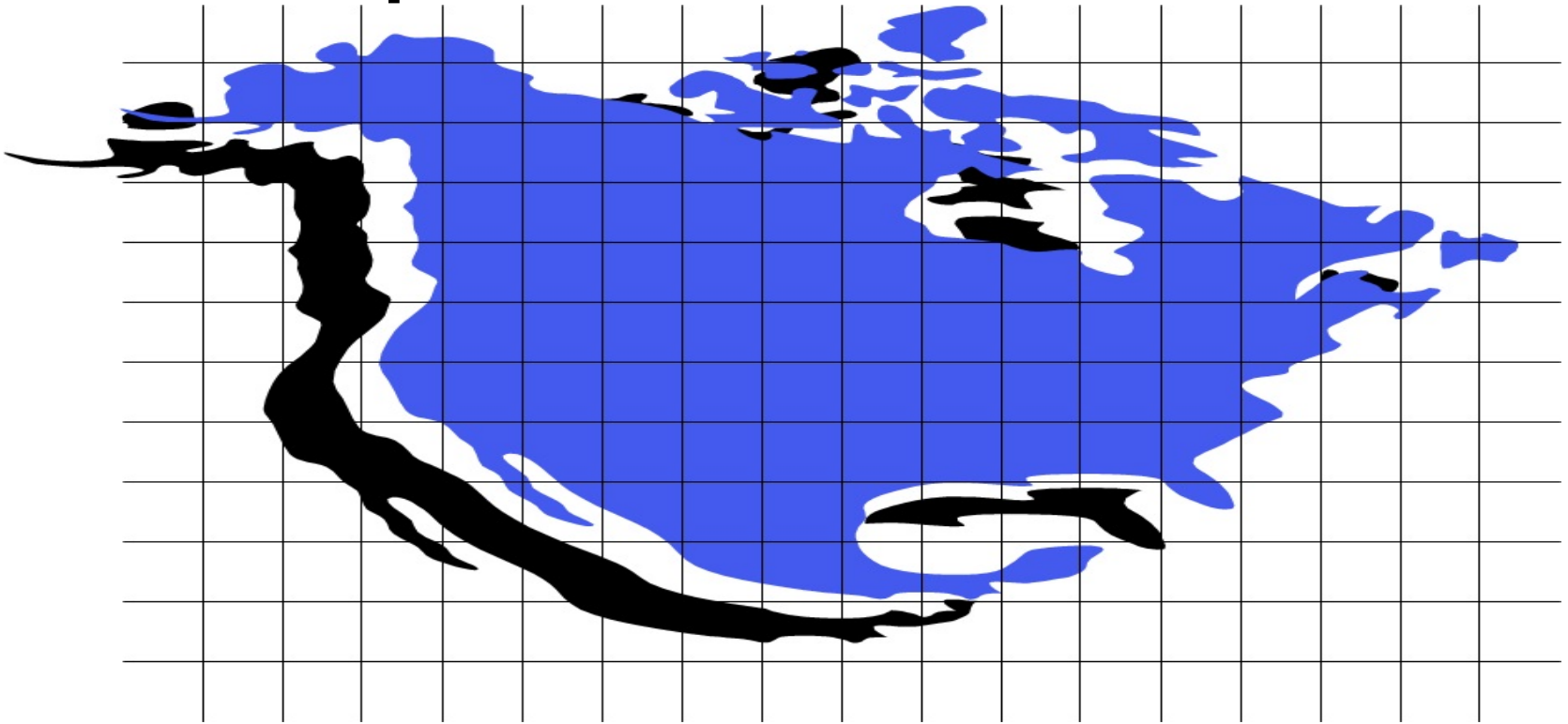
One
Standards
Continental

Examples of Something Big





Uniform Implementations



Source: USDOT