IEEE Communications Society – Denver Section

Service Management For ITS Using WAVE (1609) Networking

Tim Weil – CISSP, CISA, PMP
ITS Security Architect
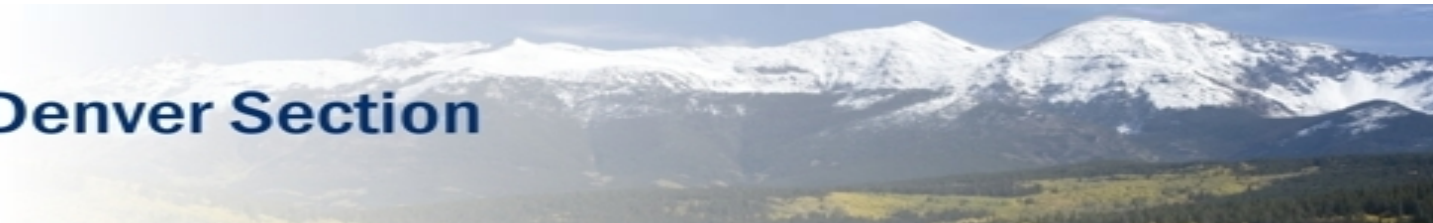
Denver, CO
19 May 2011

IEEE | Denver Section

Table of Contents

5/18/2011

Objectives of this Presentation

ITS Service Management Design Using WAVE Standards

-- ITS Models (ETSI, DOT VII/Intellidrive Use Cases, IEEE WAVE)

-- WAVE Standards – Architecture (1609.0) Security (1609.2), Networking (1609.3)

-- A Closer Look at the WAVE Approach – 2011 Modifications, WAVE nomenclature

Show real-world examples

-- SAE 2757 DSRC Messaging

-- VII/IntelliDrive Proof of Concept

-- Vehicle Public Key Infrastructure (V-PKI)

-- Identity Management Models for Service Management

Organizing Framework for Security Architecture

-- How to reduce Complexity for ITS Service Management Design

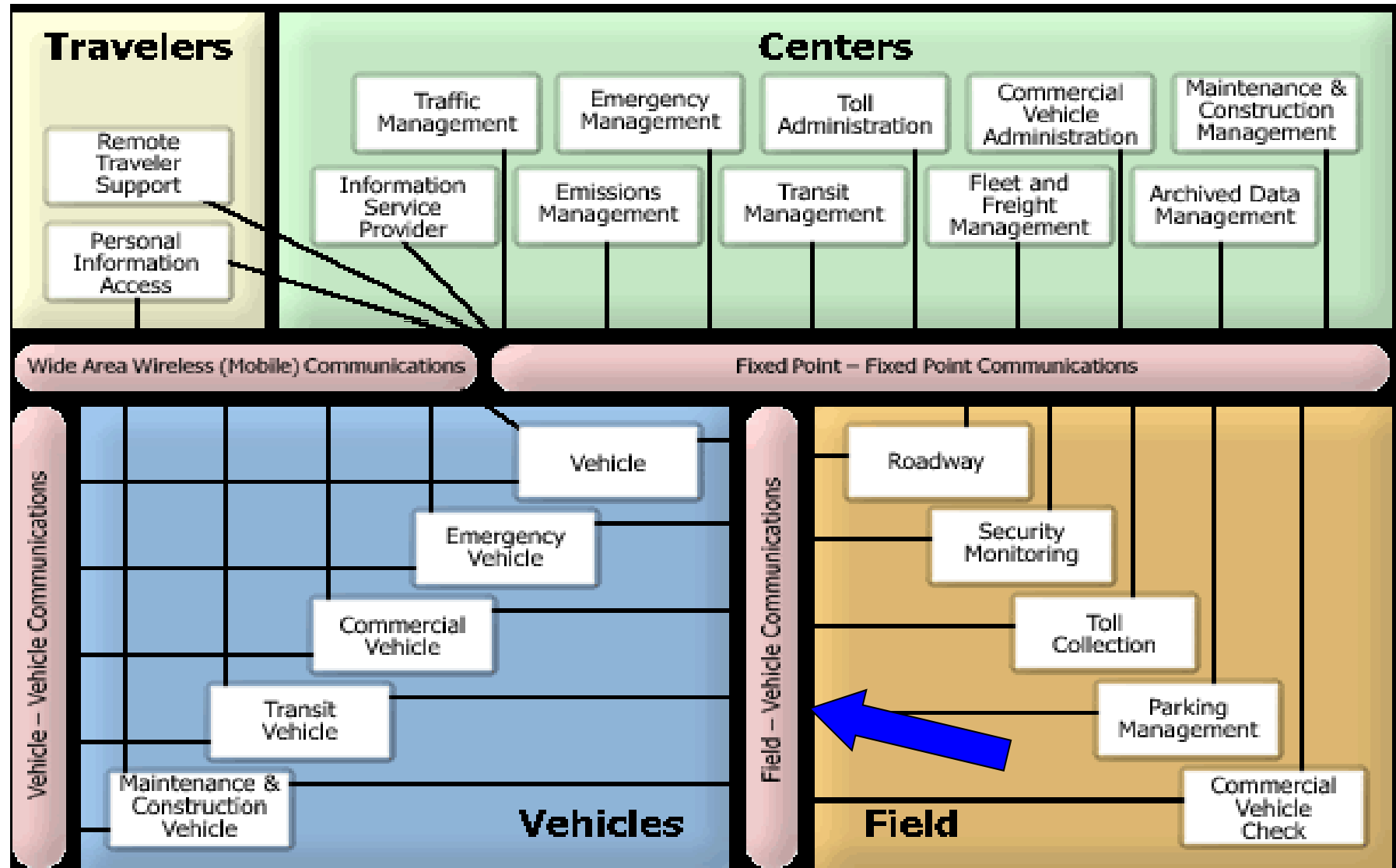-- How to Provide Repeatable Processes using the WAVE Approach
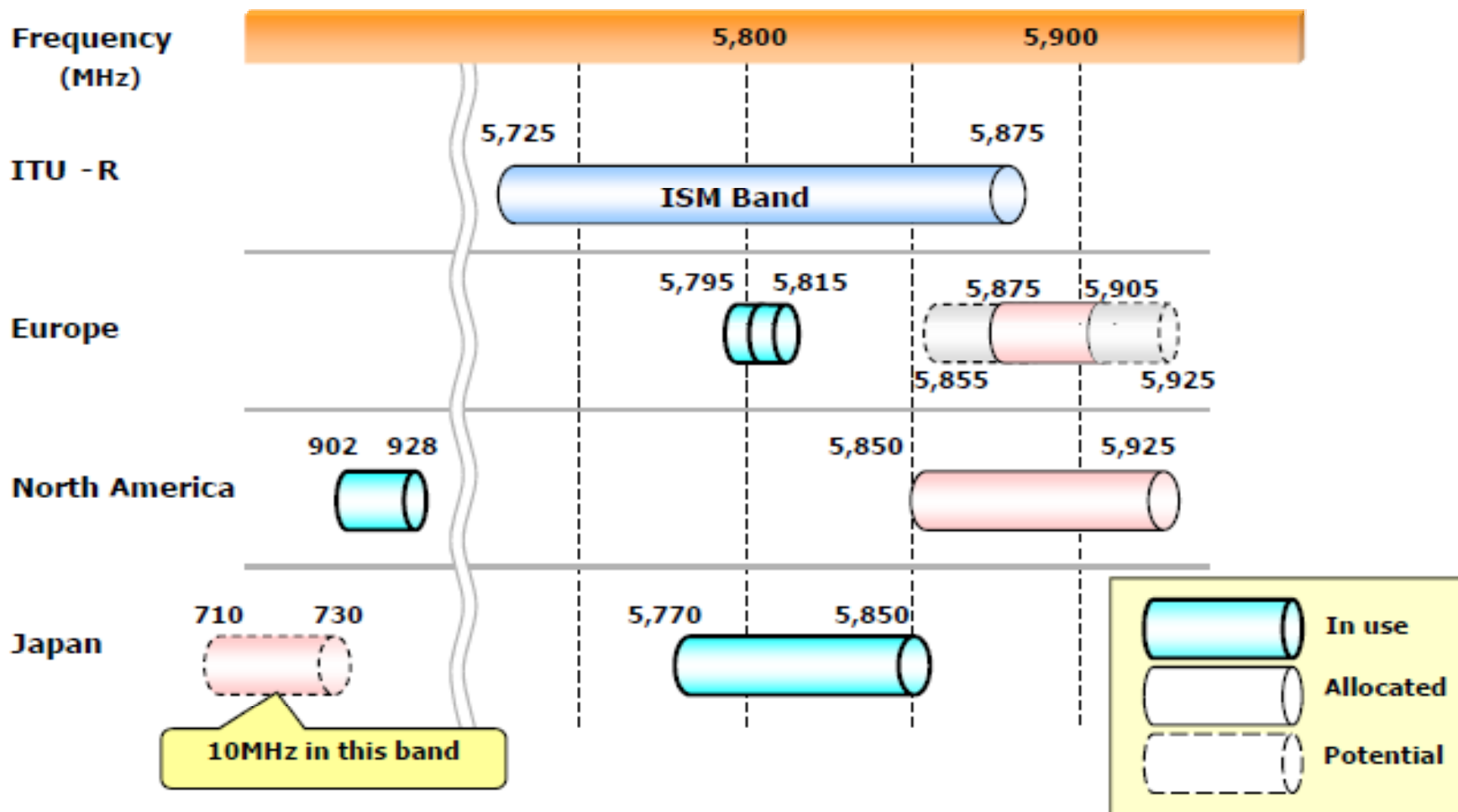
ETSI ITS Automotive Networking Model –

Introduction – USDOT ITS National Architecture (DSRC)
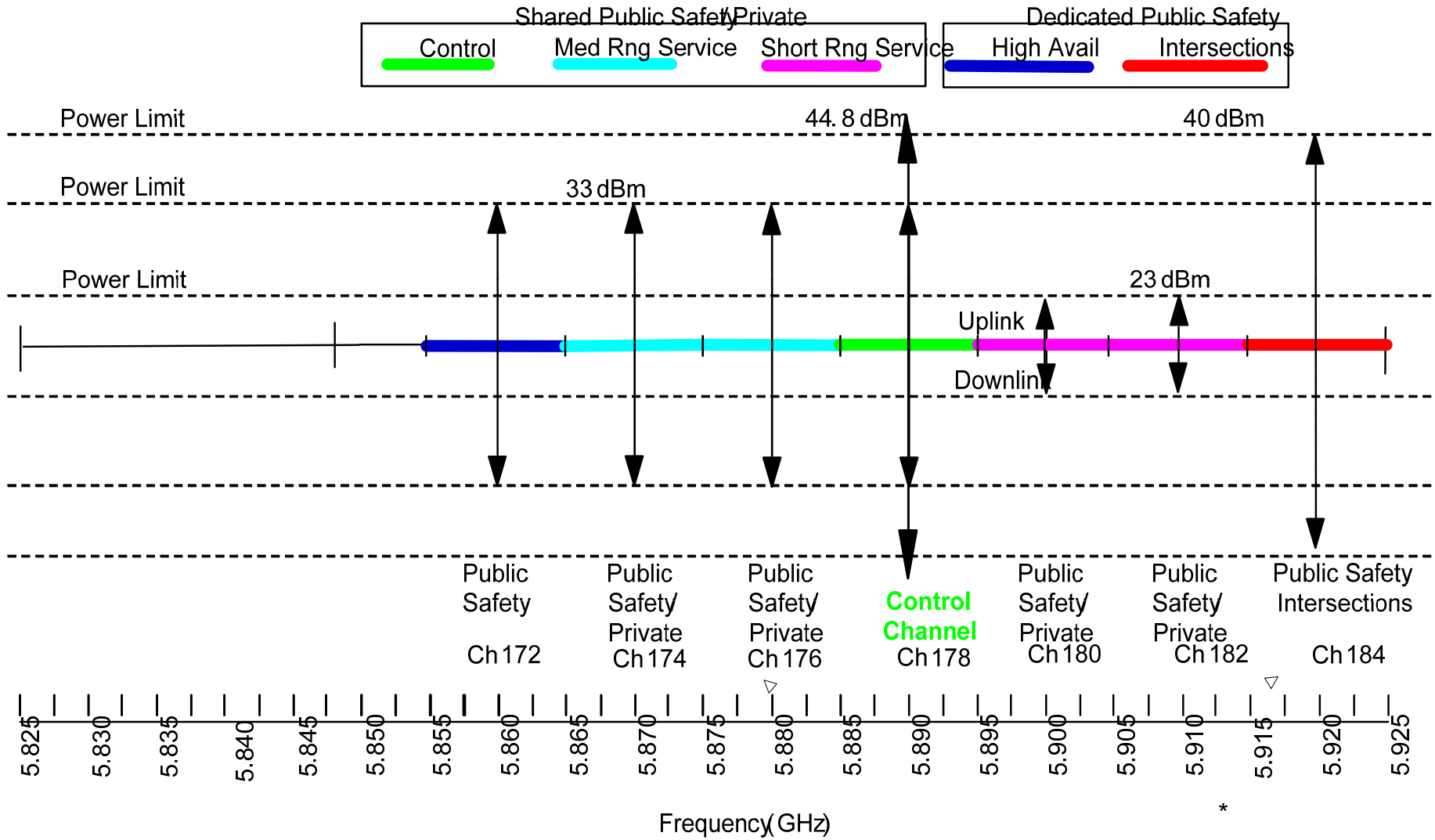**http://www.iteris.com/itsarch/html/entity/paents.htm**

DSRC frequency band specifications in Europe, North America and Japan

S. Oyama, "Activities on ITS Radio communications Standards in ITU-R and in Japan", slides presented during the 1st ETSI TC-ITS Workshop in Sophia Antipolis, France

5.9 GHz DSRC Band Plan

Introduction – ITS Use Cases Services and Applications

▸ **Traveler Information**

- Travel Times, Incident Alerts,
- Road Closures, Work Zones

▸ **In Vehicle Signage**

- Local Signage (School Zones, Stop Signs)
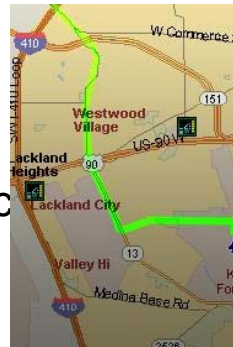- Highway Next Exit Services

▸ **Navigation**

- Off Board Navigation
- Reroute Information

▸ **Traffic Management**

- Ramp Metering
- Signal Timing Optimization
- Corridor Management Planning Assistance
- Corridor Management Load Balancing
- Pothole Maintenance

▸ **Weather Information**

- Traveler Notification (Icy Bridge Warning)
- Improved Weather Observing
- Winter Maintenance

▸ **Safety**

- Emergency Electronic Brake Light
- Traffic Signal Violation Warning
- Stop Sign Violation Warning
- Curve Speed Warning

▸ **Electronic Payment**

- Parking
- Toll Roads
- Gasoline

IEEE Standards Association Publications (WAVE) –

▸ **IEEE P802.11p**, Amendment to STANDARD FOR Information technology—Telecommunications and information exchange between systems—LAN/MAN Specific Requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications: Wireless Access in Vehicular Environments (WAVE).

▸ IEEE Std 1609.0-2006 ™, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)—Architecture.

▸ **IEEE Std 1609.1-2006 ™**, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)—Resource Manager.

▸ **IEEE Std 1609.2-2006™**, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)—Security Services for Applications and Management Messages.

▸ **IEEE Std 1609.3-2010™**, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services.

▸ **IEEE Std 1609.4-2011™**,, IEEE Trial-Use Standard for Wireless Access in Vehicular Environments (WAVE)—Multi-Channel Operation.

▸ **IEEE Std 1609.11-2011™**, IEEE Draft Standard for Wireless Access in Vehicular Environments (WAVE)—Over-the-Air Data Exchange Protocol for Intelligent Transportation Systems (ITS) - Electronic Payment Service

ITS Standards Forum (DSRC Working Group) – http://serv4.itsware.net/bb/index.php

Prototype of DSRC Architecture and Components (OmniAir Consortium)
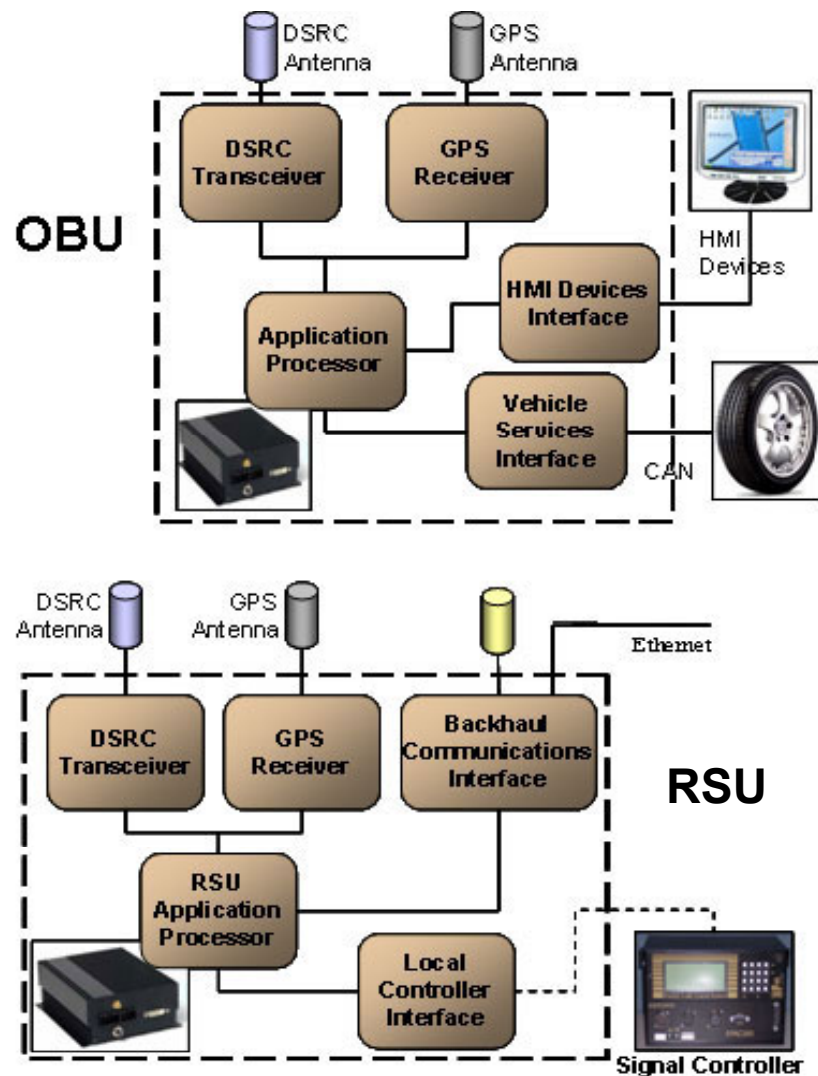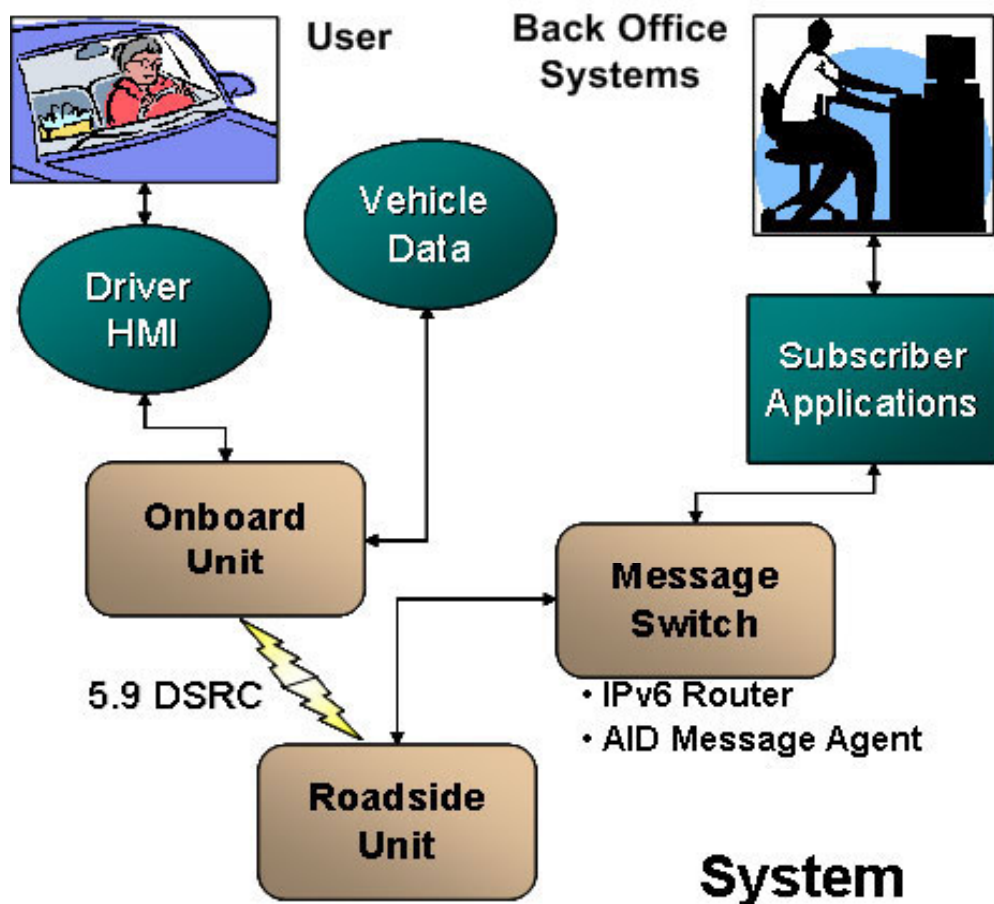
RSU and OBU Protocol Stacks (1609.3 Model)

RSU

UDP	
IPv6	WSM
Routing function	
LLC	LLC
802.3 MAC	WAVE MAC
100Base-T	WAVE PHY

Applications

To LAN/WAN   To Airlink

OBU

WSM	UDP	
	IPv6	
LLC	Filter function	LLC
WAVE MAC	Bridging function	802.3 MAC
WAVE PHY		100Base-T

Applications

To Airlink   To OVHI
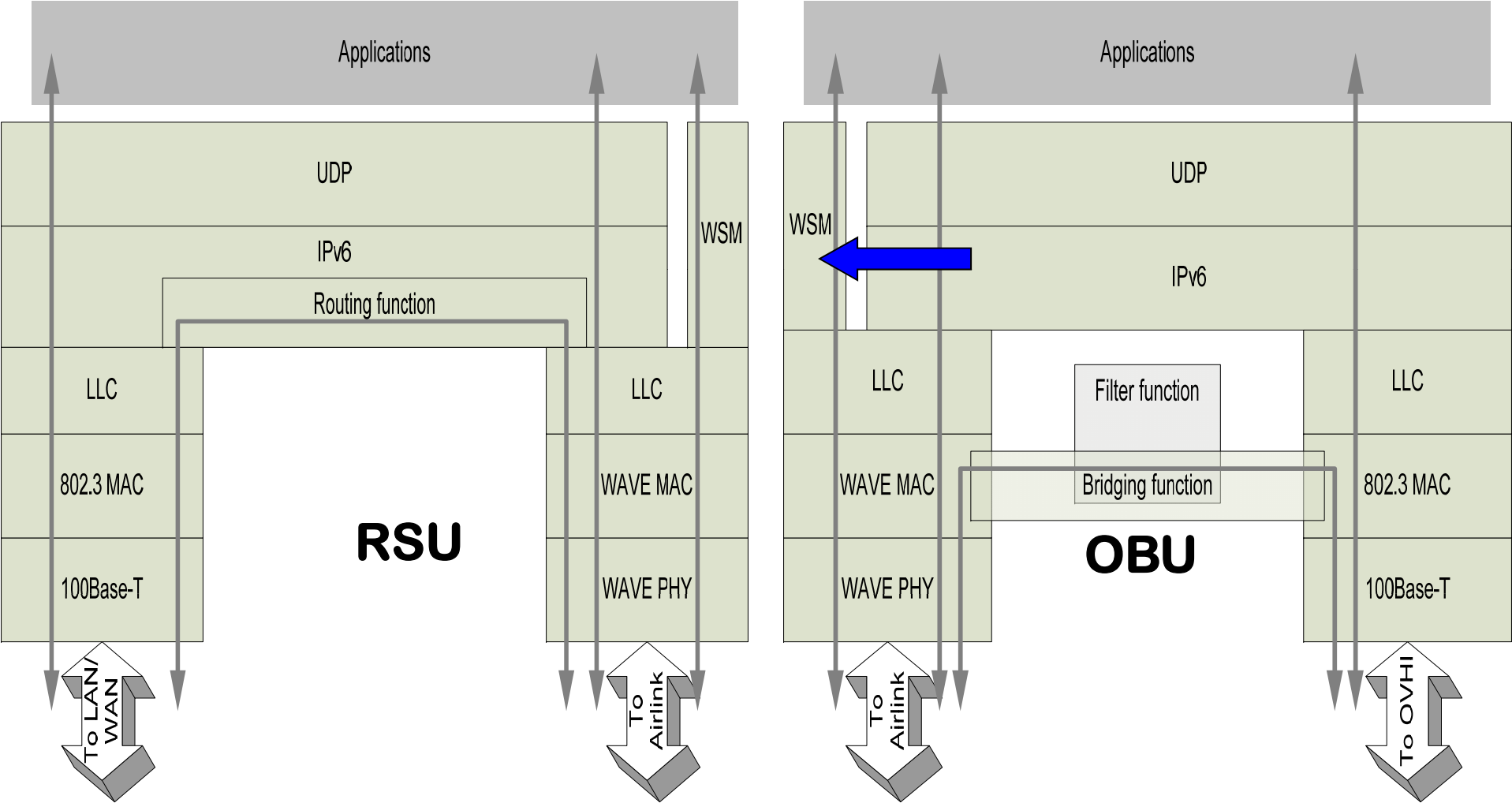
WSMP(WAVE Short Message Protocol - A protocol for rapid, reliable exchange of messages in a rapidly-varying RF environment where low-latency is also an important objective.

11

ITS Service Management Model (IntelliDrive Example)
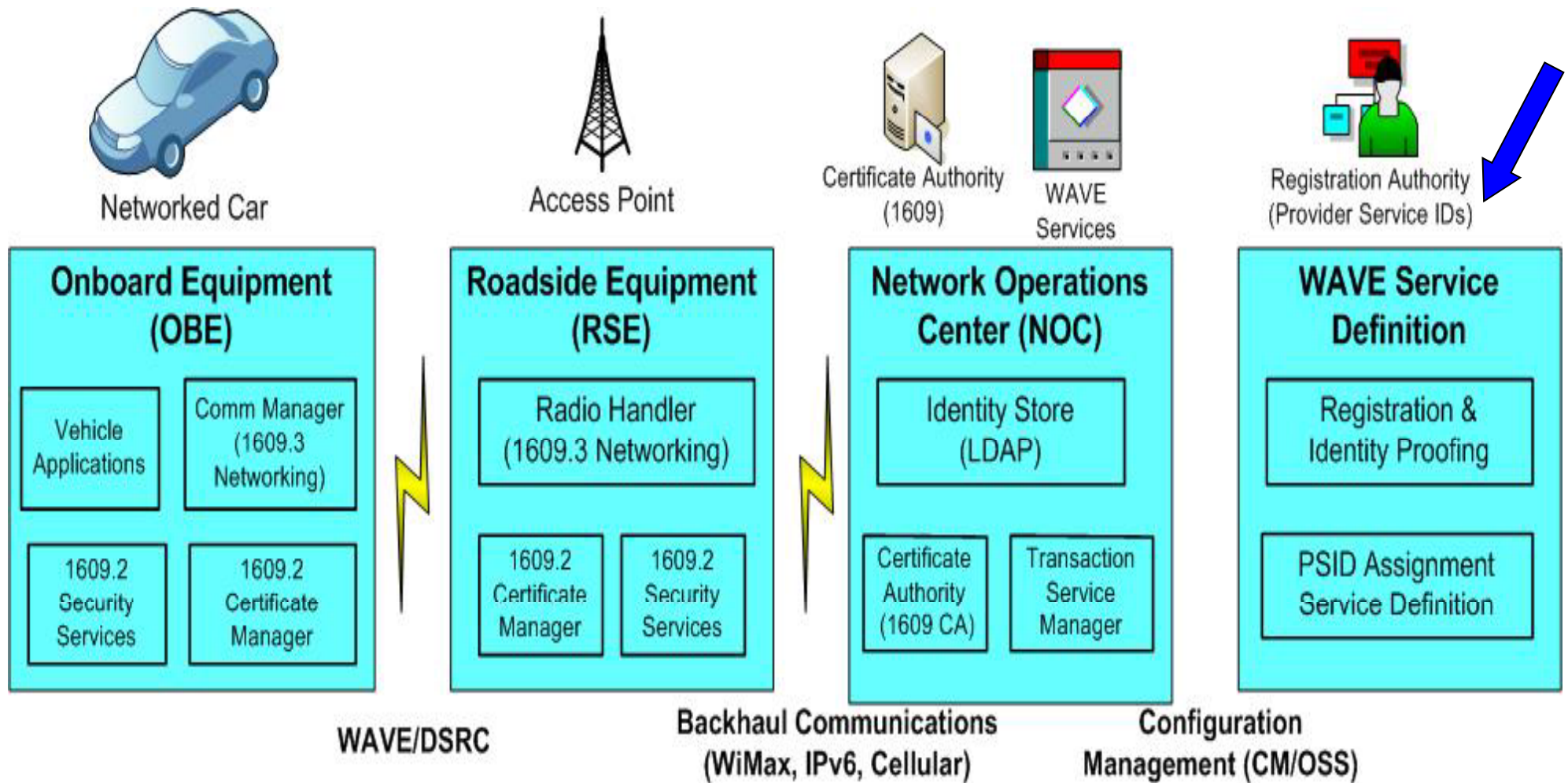
ITS Architecture using WAVE (1609.0) Architecture – Example of an operational system implemented using WAVE devices
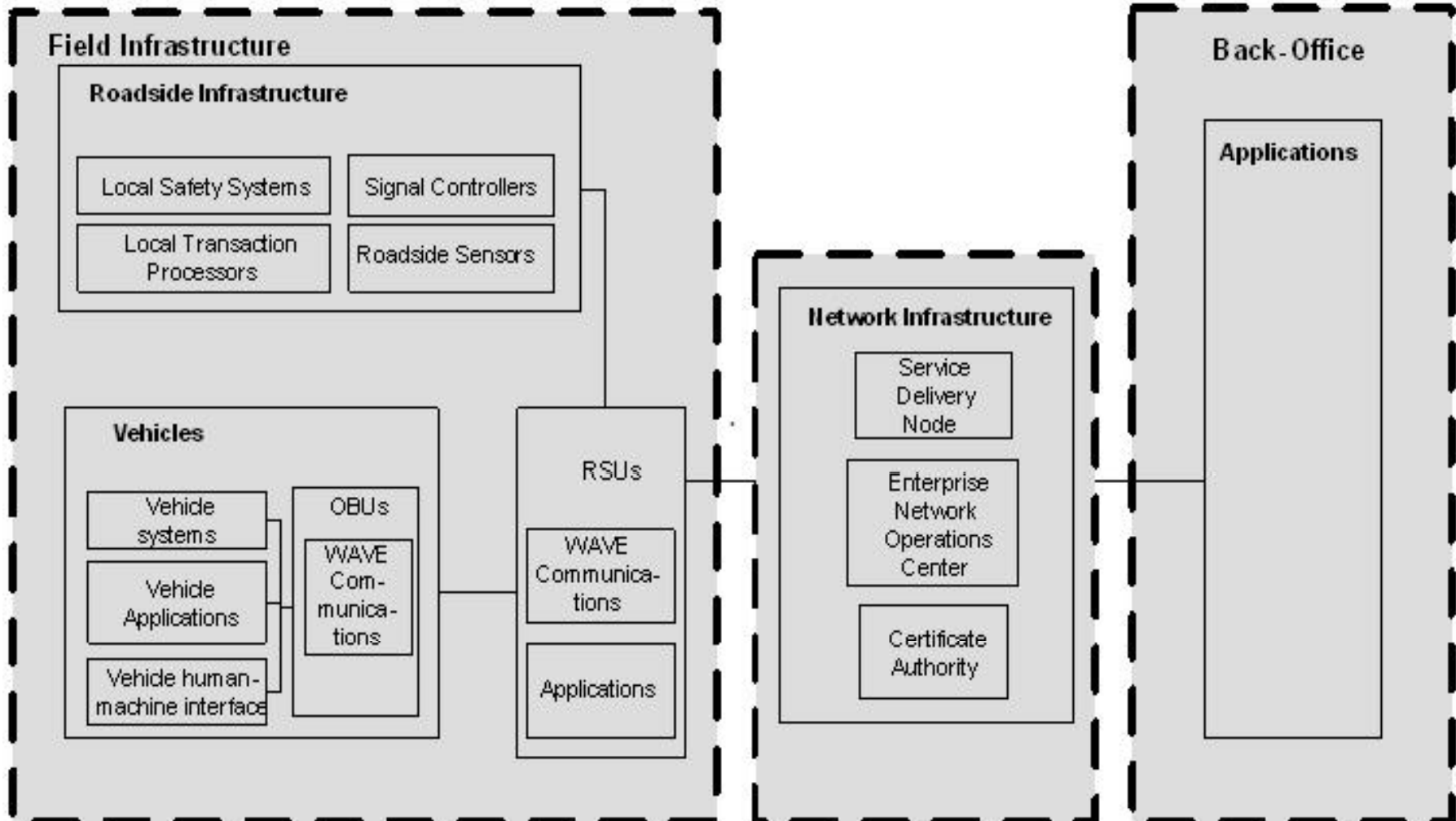
Intellidrive/VII ITS Architecture using WAVE Architecture –
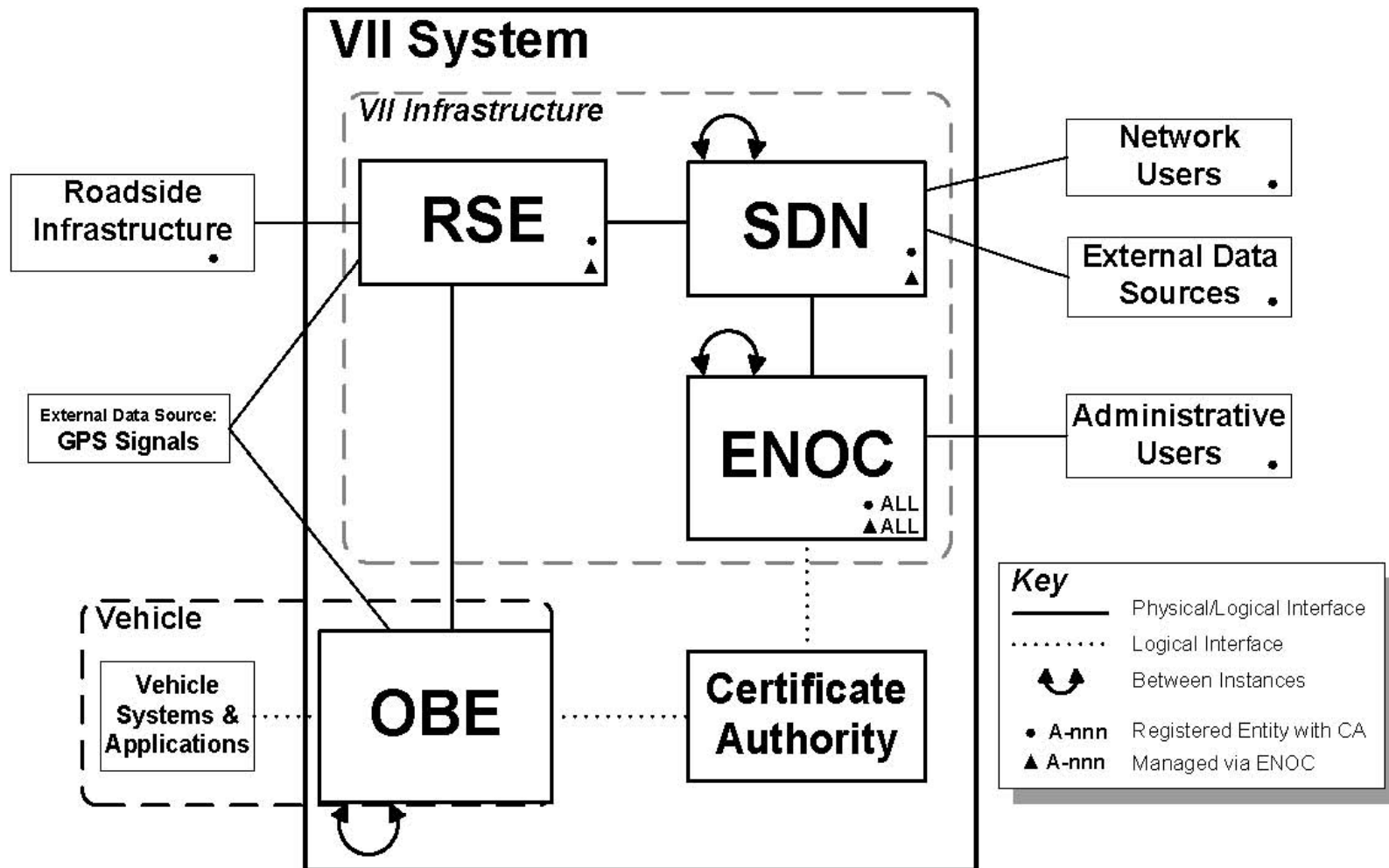
Table of Contents

▸ Introduction – ITS Service Management and WAVE

▸ The Evolution of the WAVE Standard (2009)

▸ ITS Services and OSS Architecture

▸ WAVE Service Provisioning, Identity Management and PKI

▸ A Security Model for Automotive Networking (ITS Services)

▸ Summary

Evolution of the IEEE 1609 Standards (2011) –

▶ **IntelliDrive Reports** on Vehicle Infrastructure Integration (VII) Proof of Concept tests
  – **VII POC Technical Description Vehicle Report** (DSRC Communications, OBE Software Services, Network Services Enabler Subsystem), Application Manager
  – **VII POC Technical Description Infrastructure Report** (DSRC Communications, Radio Handler, 1609.2 Security Libraries)

▶ **WAVE Protocol Enhancements**
  – 1609.0 WAVE Architecture, 1609.11 Electronic Payments, 802.11p amendments
  – Vendor Specific Action Frame (802.11p) - OID and Content Description Enhancements
  – 802.11p Sponsor Ballots (10/2009-6/2010)
  – WAVE Sponsor Ballots (3/2010-10/2010)

▶ **1609.3 Modifications (impact on Service Management)**
  – Service Management Model moved to 1609.0
  – Sending and Receiving unsigned WSAs (allow use of timing without signature verification)
  – Defined Security SAP to WME

▶ **1609.2 Modifications**
  – Alignment with changes in WAVE Networking Standard (1609.3)
  – Scope/Purpose Restatement
  – SAPS for sending and receiving secured messages and WSAs
  – Application Security Profiles (how applications call the MIB)
  – Anonymity and Privacy Guidelines

IntelliDrive/VII Final Reports – DSRC and Proof of Concept Tests
http://www.its.dot.gov/research_documents.htm

▸ **Final Report: Vehicle Infrastructure Integration Proof of Concept Executive Summary** — Vehicle - VII Consortium. May 2009.

  FHWA-JPO-09-003.   The executive summary is intended for executives and managers of organizations interested in the deployment of IntelliDriveSM. This report summarizes a program of work resulting from a Cooperative Agreement between USDOT and the VII Consortium to develop and test a Proof of Concept VII system based on DSRC wireless communication between an infrastructure and mobile terminals. It supports applications for improvement in safety and mobility and enables other commercial applications. Key findings and recommendations for further work are presented.

▸ Final Report: Proof of Concept Results of Findings Summary—Vehicle - VII Consortium. May 2009. FHWA-JPO-09-043.

  This final report describes the objectives and the approach to the testing of the VII Proof of Concept system. Summaries of the vehicle-related test results and findings for both the major system functions and the applications designed for the system.

▸ Final Report: Proof of Concept Technical Description—Vehicle* - VII Consortium. May 2009. FHWA-JPO-09-017.

▸ This report provides the technical description of the VII system developed for the Cooperative Agreement VII Program between the USDOT and the VII Consortium. The basic architectural elements are summarized, and detailed descriptions of the hardware and software systems are provided, along with the descriptions of the applications used to assess the system performance and operation.

▸ **Final Report: Proof of Concept Executive Summary—Infrastructure** - Booz Allen Hamilton. Feb. 2009.

  This document provides an overview of the key infrastructure-related findings and recommendations from the POC testing. This volume is intended for executives and managers of organizations interested in the deployment of IntelliDriveSM.

▸ **Final Report: Proof-of-Concept Technical Description—Infrastructure** - Booz Allen Hamilton. Feb. 2009.

  This report describes the overall approach undertaken to prove the infrastructure-related VII concepts through a structured testing program. It describes the overall experimental design used in proving the VII concept by providing an overview of the system architecture and design of systems, subsystems, and components, as well as the public sector applications developed to prove some of the system concepts. This volume is intended for engineering managers and practicing engineers interested in the design and development of IntelliDriveSM systems and applications

IEEE 1609 Standards Working Group
(*http://vii.path.berkeley.edu/1609_wave*)

Welcome to the IEEE 1609 Working Group Public Site

The IEEE 1609 Family of Standards for Wireless Access in Vehicular Environments (WAVE) define an architecture and a complementary, standardized set of services and interfaces that collectively enable secure vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) wireless communications. Together these standards are designed to provide the foundation for a broad range of applications in the transportation environment, including vehicle safety, automated tolling, enhanced navigation, traffic management and many others. This web site is primarily for the convenience of the members of the IEEE 1609 Working Group who are developing and maintaining these standards, and includes open minutes and public presentations from their meetings. References to the presentations are given in the minutes. Materials are currently available from the following meetings:

- April 29-May 1, 2008, Los Angeles, California
  - Presentations
  - Minutes
  - Agenda
- August 26-27, 2008, Richmond, California
  - Presentations
  - Minutes
  - Agenda
- October 14-15, 2008, Albany, New York
  - Presentations
  - Minutes
  - Agenda

For more information about these standards and how they may be purchased, see the following reference:

http://vii.path.berkeley.edu/1609_wave/   11/3/2008

- **Fact Sheet about the IEEE 1609 Family of Standards for Wireless Access in Vehicular Environments**
  US Department of Transportation, Research and Innovative Technology Administration, Intelligent Transportation Systems (ITS) Standards Program

Other information of interest to those participating in IEEE 1609 development includes:

- **Selected Presentations from the "M5" Workshop**
  Chicago, USA, September 2008
- **CALM web site**
  includes minutes from the M5 Workshop posted in the publicly available area "Chicago Workshop" along with all the presentations.
- **Panel presentations on the commercialization of DSRC/WAVE**
  WiVec, Calgary, Alberta, Canada, September 2008

Draft revisions and other materials for members only can be found at the password protected "members only" site:

- **DSRC Messaging Standards**
  IEEE Vehicular Technology Society (VTS), Intelligent Transportation Systems

Site hosted by California PATH UC Berkeley

PATH

Maintained by Susan Dickey
Last modified: August 31, 2008

http://vii.path.berkeley.edu/1609_wave/   11/3/2008

18

1609.0 Purpose and Scope

▸ **WAVE Objectives** (System Components and Connectivity, Protocol Architecture, Interfaces, Channel Types, Communication Services, Device Roles, Priorities, Channel Coordination)

▸ **Relevant Standards** (National ITS Architecture, ASTM and FCC, IEEE WAVE Standards, IETF)

▸ **WAVE Systems Operation** (Communications Without a Service, Communications With a Service*, Time Synchronization and Channel Coordination, Addresses and Identifiers in WAVE**, Distribution System (DS) Portal at Roadside Unit, IPv6 Neighbor Cache)

▸ **Security Considerations - TBD** (Certificate Management, Encryption of User Traffic, Signature and Validation of User Management Traffic, Anonymity)

▸ **Annex** – Example System Configuration (WAVE Architecture)

* **Addresses and Identifiers** – (MAC Address, IPv6 Address, Protocols and Ports, Application Identification Using PSID and PSC)
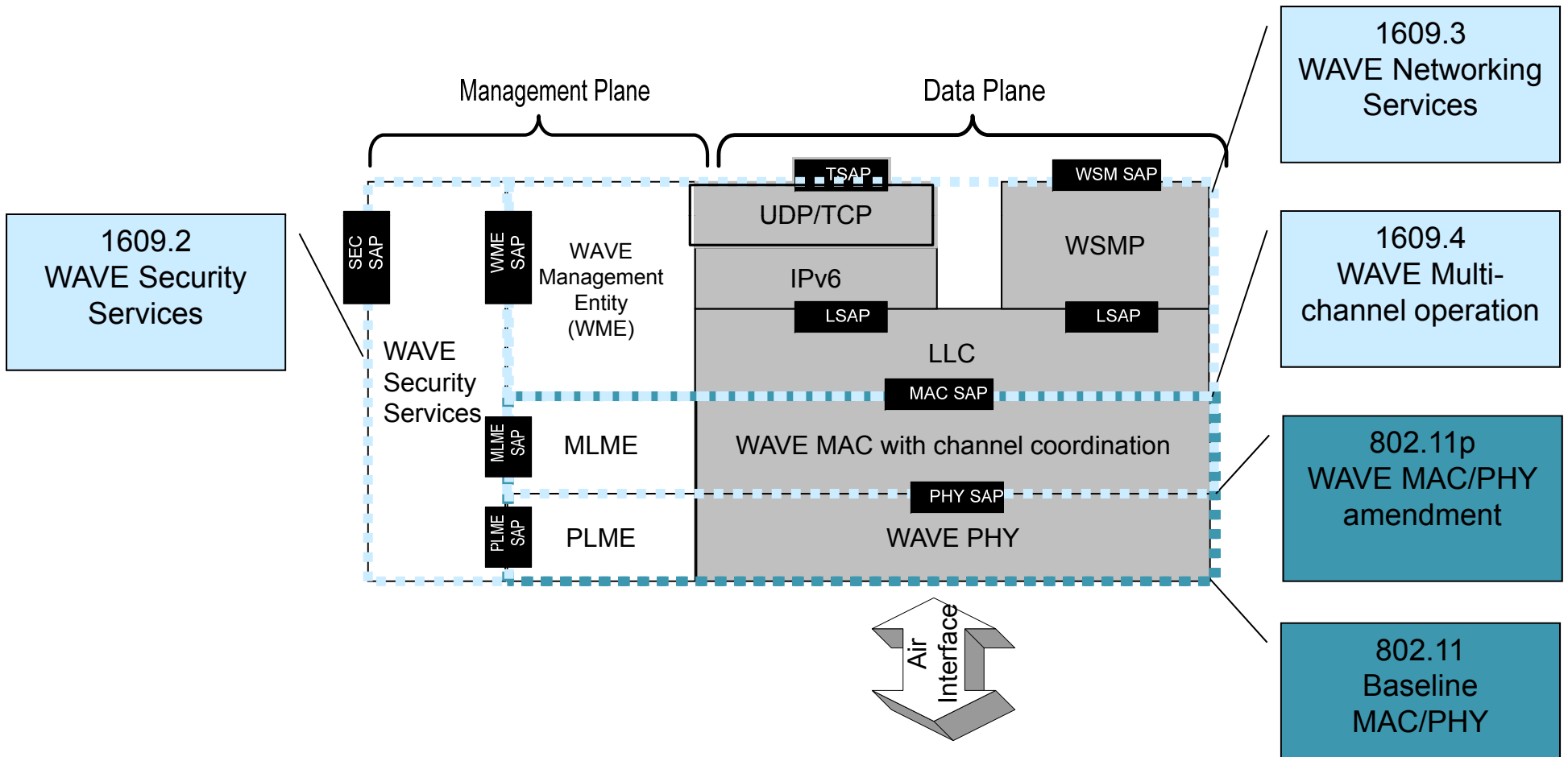
** **Communications With a Service** – (WAVE Service Advertisement, Service Initiation, Service Channel Communications, Service Termination, Adding and Subtracting Applications from an Advertisement

1609.3 Purpose and Scope

▸ **Data Plane Services** (LLC, IPv6, UDP, Other IP Protocols, WAVE Short Messages - WSMP)

▸ **Management Plane Services** (Service Requests and Channel Usage Assignment, Automatic Message Generation, Management Data Delivery on Receipt, WSA Monitoring, IPv6 Configuration)

▸ **Service Primitives** (WAVE Short Message Protocol SAP, WAVE Management Entity SAP, WAVE LSAP, MLME and MLMEX DAP, Security SAP)

▸ **Over the Air Formats** (WAVE Service Advertisement, WAVE Short Message, WSM Encoding)

▸ **Annexes** – WME MIB Table, ASN.1 Encoding of the WME MIB, Bibliography and Definitions, Protocol Implementation Conformance (PICS) proforma, Service Usage Examples)

▸ **Service Usage Examples (Annex E) –** (Provider Service Request, User Service Request with Automatic Channel Assignment, User Service Request with Notification, MIB Monitoring of User Service Request, Multi-Channel Operation)

1609.0 Protocol Model, Updated, with Standards and Access Points

The air interface allows WAVE devices to communicate with each other over the wireless medium. Interfaces between protocol components are accomplished via services access points (SAPs). SAPs are specified in the appropriate standard and are illustrated below. SAPs describe information exchanged, but do not specify the interface implementation. SAPs are comprised of "primitives," each of which is a logical message structure, generally containing a set of data elements for accomplishing a particular function.

Management Plane | Data Plane

1609.3 WAVE Networking Services

1609.2 WAVE Security Services

1609.4 WAVE Multi-channel operation

802.11p WAVE MAC/PHY amendment

802.11 Baseline MAC/PHY

SEC SAP · WME SAP · TSAP · WSM SAP

WAVE Management Entity (WME)

UDP/TCP · WSMP

IPv6 · LSAP · LSAP

WAVE Security Services

LLC

MLME SAP · MLME · MAC SAP

WAVE MAC with channel coordination

PLME SAP · PLME · PHY SAP

WAVE PHY

Air Interface

Networking and Service Managements Features addressed in the IEEE Standards (1609.0/.3)

Features of 1609.0 and 1609.3	Purpose
WAVE Services (1609.0)	A capability, provided by an application, that makes use of WAVE communication facilities. Services are classified as Persistent or Non-Persistent
WAVE Management Entity (WME)	A set of management functions required to provide WAVE Networking Services.
WAVE Service Advertisement (WSA)	A data structure containing information that announces the availability of a service. A VSA is composed of such structures
WAVE Short Message Protocl (WSMP)	A protocol for rapid, reliable exchange of messages in a rapidly-varying RF environment where low-latency is also an important objective.
ProviderServiceInfo (MIB Entry)	• WSA-Type ProviderServiceIdentifier Service Priority • ProviderServiceContext Regulatory Class ChannelSelection • Repeat Rate IP Service IPv6 Address • ServicePort Provider MAC AddressServiceStatus
Provider Service ID (PSID)	An octet string that identifies a service provided by a higher layer entity
Provider Service Context (PSC)	A field associated with a PSID containing supplementary information related to the service. The format of the PSC is PSID dependent.
Control Channel (CCH/)	**CCH** - A single radio channel, not a service channel, intended for exchange of management frames, including WAVE Service Advertisements, and WAVE Short Messages..
Service Channel (SCH)	**SCH** -Any channel that is not the control channel, intended for management frames and higher layer information exchanges WAVE Short Message [WSMs] and Internet Protocol version 6 [IPv6] packets).

In-Vehicle Signage DSRC Setup – SAE J2757 POC Message Set

WSM's broadcast from RSE to OBE's

UNSIGNED PSID's

▸ 0x02100001   Conditions Advisories: Traffic Delays & Status

▸ 0x02110001   Conditions Advisories: Weather Conditions

▸ 0x02120001   Convenience Advisories: Roadside Services

▸ 0x02130001   Convenience Advisories: Food Services

▸ 0x02140001   Convenience Advisories: Vehicle Services

▸ 0x02150001   Convenience Advisories: Lodging Services

SIGNED PSID's

▸ 0x02020001   Safety Advisories: Roadway Condition

▸ 0x02030001   Safety Advisories: Civil Emergency

▸ 0x02040001   Safety Advisories: Cautions

▸ 0x02010001   Safety Advisories: Road Incident

Message Priorities (SAE DSRC Message Framework Subcommittee DRAFT October 2008)
SAE DSRC Message Set & Priorities

Importance Level from USA FCC Policy	Description (When to apply a specific urgency level)	Description (When to apply a specific urgency level)
1 = Safety of Life Applies to those Messages and Message Sets associated with societal and/or safety impact related to human life.	Emergency Impact mitigation and injury avoidance/mitigation	Urgent warning of impending local situation
	Emergency Potential-event impact and/or injury mitigation and avoidance	Situation-based status information of uninvolved local interest
	Urgent Warning Events (Event Flags)	Intersection and vehicle safety status information
2 = Public Safety (Safety not in 1) Applies to Road Side Units (RSU) and On-Board Units (OBUs) operated by state or local governmental entities presumptively engaged in public safety priority communications. (Includes Mobility and Traffic Management Features)	Urgent public safety downloads (Intersection Information)	Semi-urgent public safety link establishment
	Urgent public safety downloads (Intersection Information)	Semi-urgent public safety data and application enabler
	Urgent public safety downloads (Intersection Information)	Semi-urgent public safety data and application enabler
	Public safety data transactions, exchanges	Important Traffic Management status information enabler
	Public safety geospatial context information	Important Announcement of WAVE Services
	Public safety geospatial context information	Non-urgent Traffic Management Foundational Data
	Public safety RTCM GPS correction information	
3 = Non-Priority Communications (Not in 1 or 2) Applies to Fleet Management, Traveler Information Services and Private Systems.	Urgent, private and commercial electronic transactions	Important, private and commercial electronic transactions
	Semi-Urgent, private mobility data and electronic transactions	Background, private mobility data downloads and upgrades

AuthN/AuthZ Features addressed in the IEEE 1609 Standards

Identity Management Features of 1609.2/1609.3	Purpose
Classes of Digital Certificates	There are **classes of certificates** identified by the *'subject_type'* field which describes what kind of entity owns the certificate. It is used to determine the scope of the certificate and the means of identifying the signer
Securing Transactions	Transactions are exchanges in which multiple messages are sent by one or both peers. Transactions are initiated when a user receives a Provider Service Table (PST) as advertised by a WSA
Securing Messages Structures	A secure message type is a published 1609.2 data structure with these options - *unsecured message*, *signed message* or *signed WSM*.
Bootstrapping Trust	All WAVE equipment are provisioned with a public key that can be used to validate root certificate updates. *OBEs* can generate their own key pairs.
Signed Messages	**ECDSA** signed messages provides authentication for WAVE multicast messages.
Encrypting Message Structures	The *EncryptedMessage* type is a subtype of the *SecuredMessage* type. A WAVE certificate contains one or two keys for either encryption, verification or both functions.
Provider Service ID (PSID)	**A** signed number that identifies a service provided by an application and announced in the WAVE Service Announcement (WSA) PSID
Certificate Requests	Device provisioning with certificates use either 'push' or 'pull' model. 'Pull Model' is supported with a CSR message type in 1609.2.
Certificate Revocation Lists	1609.2 defines a CRL type. The 'Security Manager' annex describes the CRL functionality on a 1609 device (i.e. OBE)
Anonymity	Broadcast transmissions from a vehicle operated by a private citizen should not leak information that can be used to identify that vehicle to unauthorized recipients.

1609.2 Security Subsystem Diagram

Legend

- ◆ Fully Specified SAP
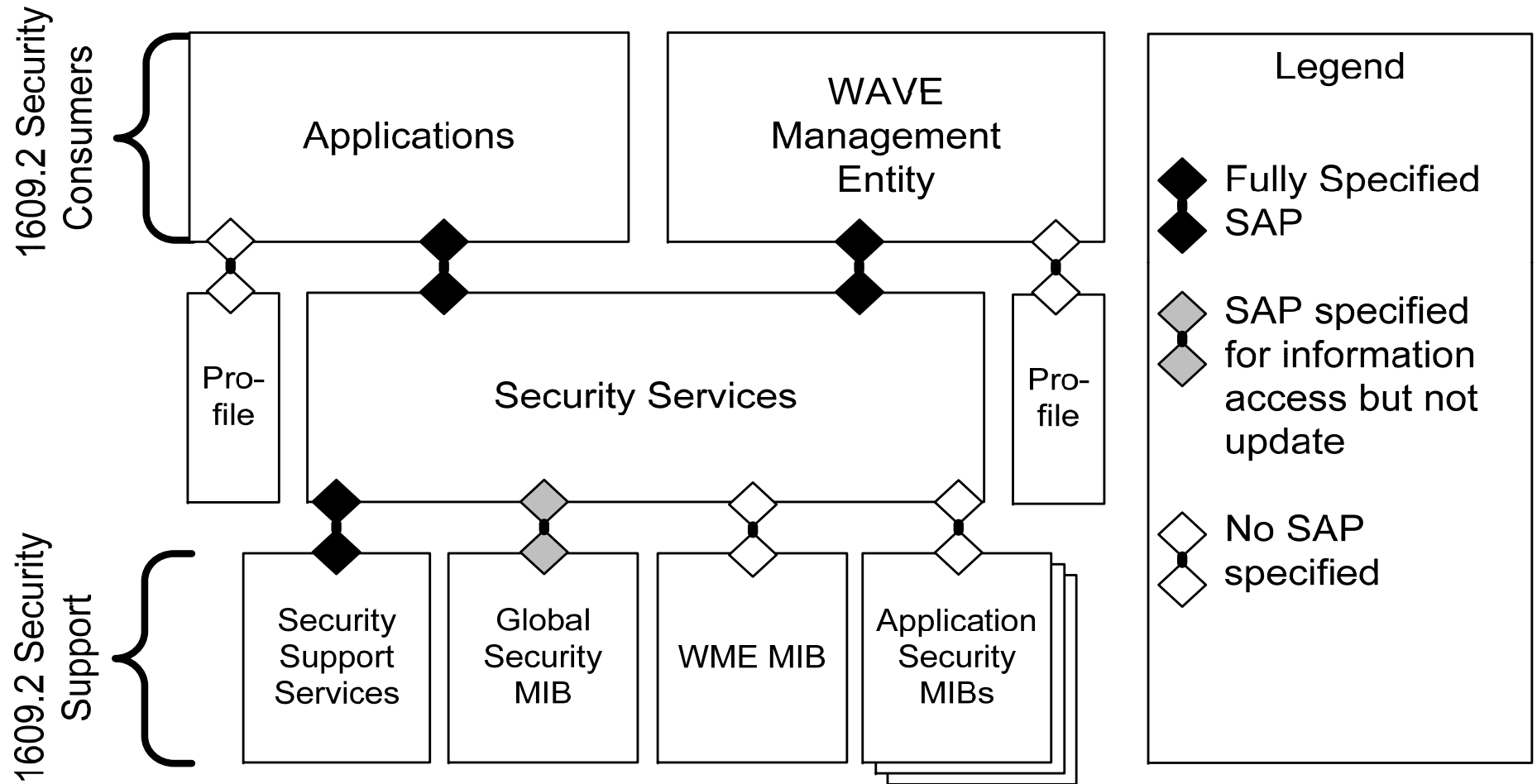- ◆ (grey) SAP specified for information access but not update
- ◇ No SAP specified

26

Table of Contents

▶ Introduction – ITS Service Management and WAVE

▶ The Evolution of the WAVE Standard (2009)

▶ Securing ITS Services with WAVE (OSS Architecture)

▶ WAVE Service Provisioning, Identity Management and PKI

▶ A Security Model for Automotive Networking (ITS Services)

▶ Summary

ITS Security and Privacy – Data You Can Trust
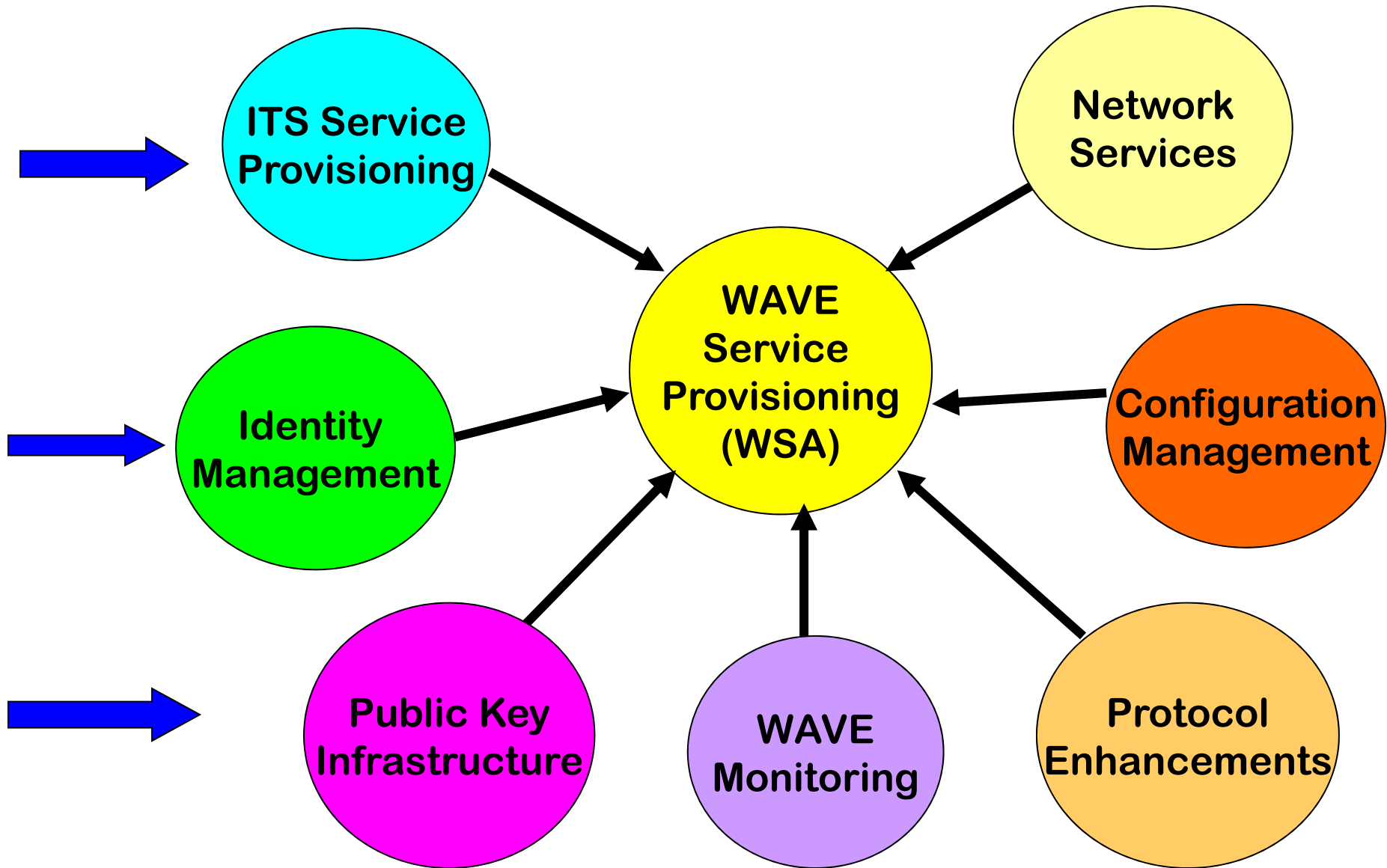

Privacy

Confidentiality
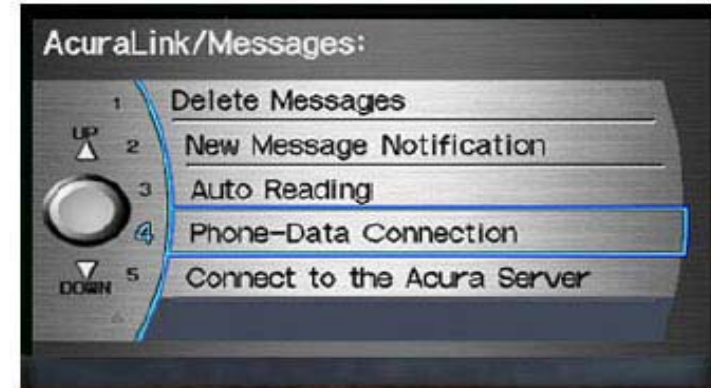
Integrity

Availability

Security Architecture (EPFL V-PKI – J.Hubaux et. al.)

Services (e.g., toll payment or infotainment)

Certificate Authority

Secure positioning

Secure multihop routing

Tamper-proof device

Event data recorder

Data verification

Authenticated message

≈ 100 bytes | ≈ 140 bytes

| Safety message | Cryptographic material |

{Position, speed, acceleration, direction, time, safety events}

{Signer's digital signature, Signer's public key PK, CA's certificate of PK}
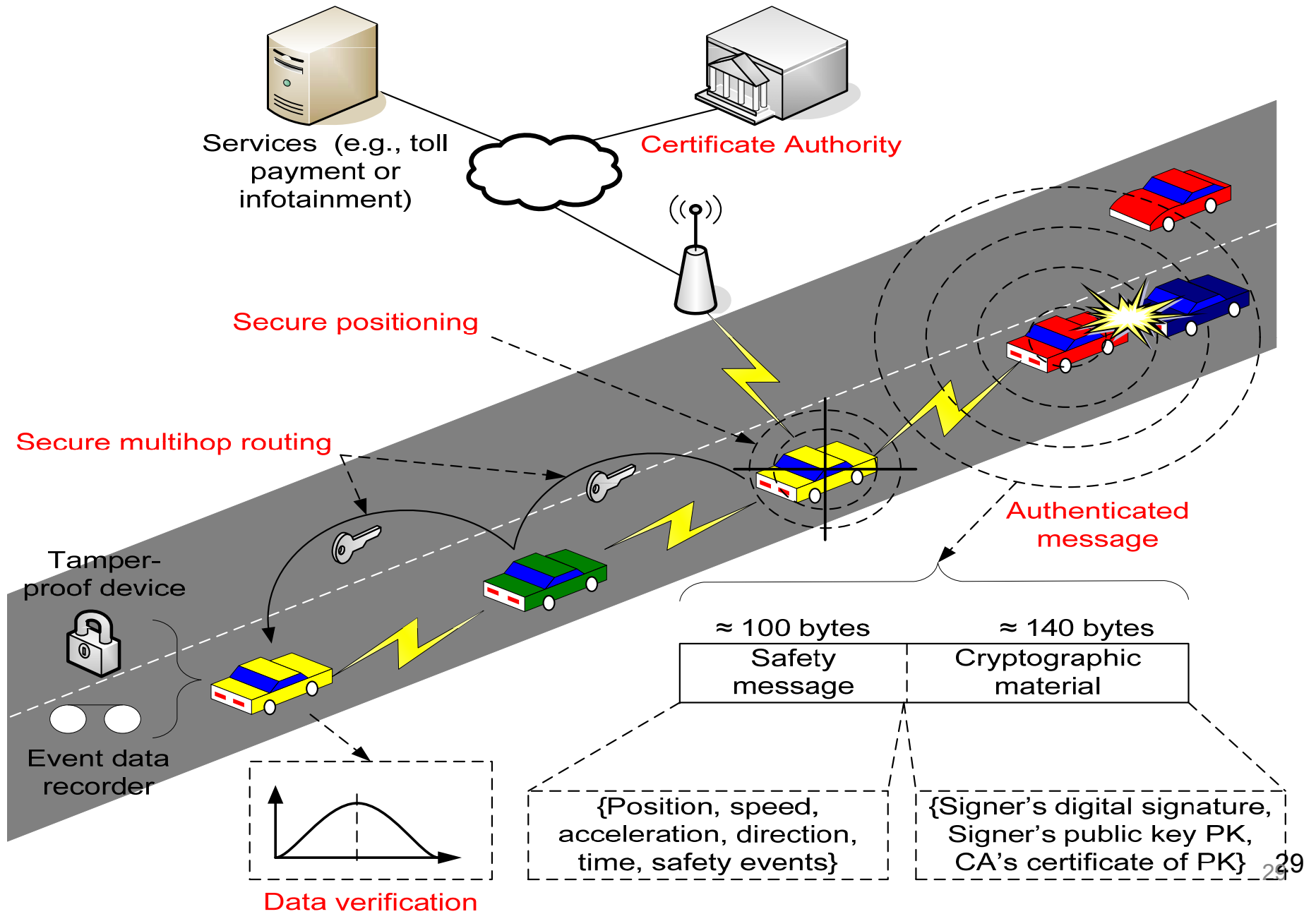
WAVE Architecture Integration − Component Services (1609.2/1609.3)

WAVE Architecture Integration − Component Services (1609.2/1609.3)

▶ **ITS Service Provisioning**
- Service Creation
- PSID Registration
- PSID Advertisement
- PSID Security
- RSE Attributes (MIB)

▶ **Identity Management**
- RSE Naming Convention
- PSID Format
- 1609.2 Credentials
- Anonymous Certificates
- Directory Services (LDAP)

▶ **Public Key Infrastructure**
- 1609.2 Certificate Authority
- 1609.2 Certificate Manager (RSE)
- 1609.2 Certificate Manager (OBE)
- Identity Based Encryption (IBE)

WAVE Provisioning (WSA)
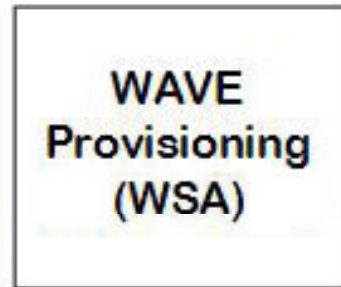
▶ **Network Services**
- IPv6 Infrastructure (address and routes)
- Firewall Protection
- Ports and Services
- Virtual Private Network Access

▶ **Configuration Management**
- RSE and OBE SW Version Control
- Software Development Tools
- 1609.2 Security Libraries

▶ **Protocol Enhancements**
- Vehicular Datagram Transaction Layer Security (VDTLS)
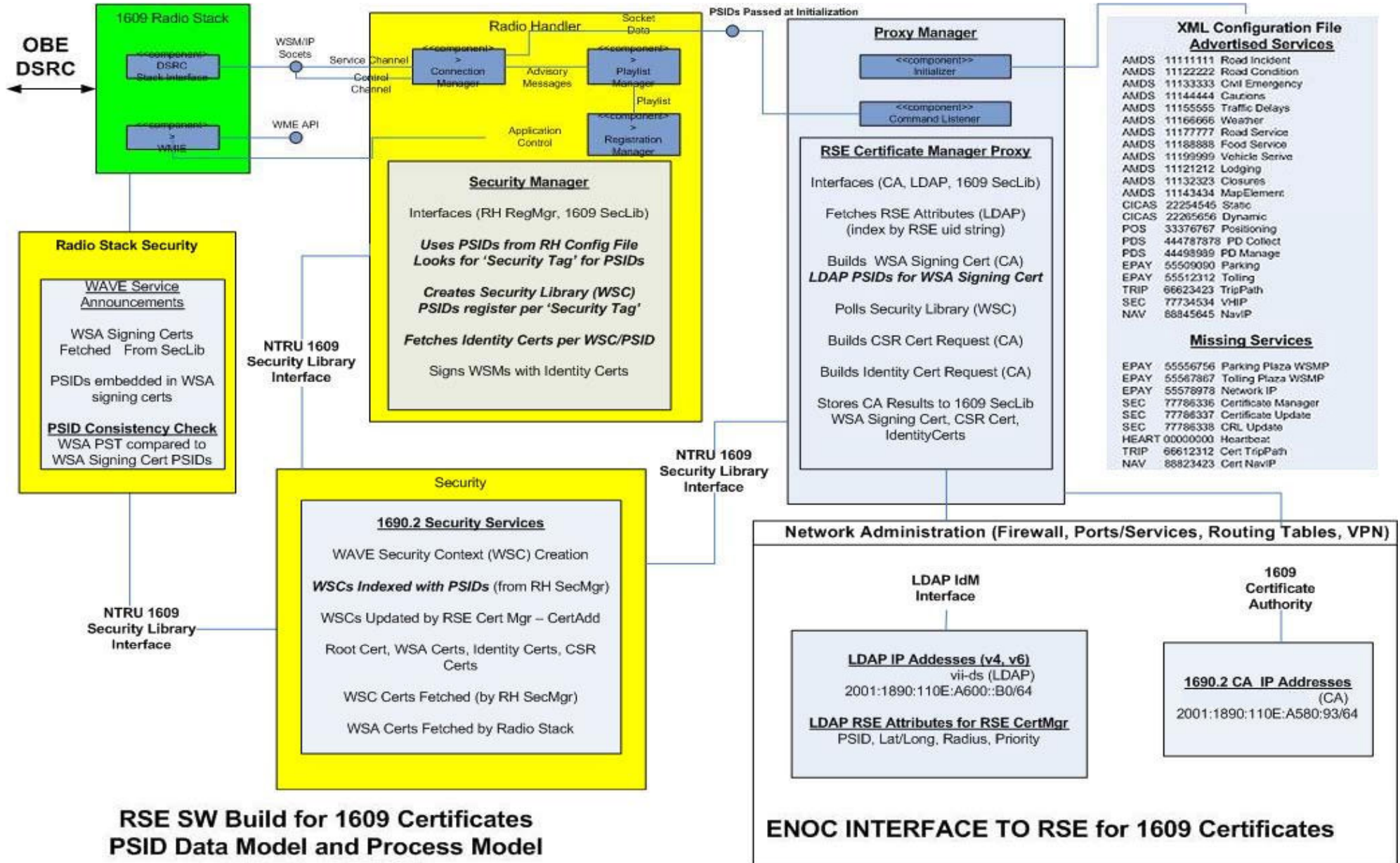- Vehicular Host Internet Protocol (VHIP)

▶ **WAVE Monitoring**
- Logging and Fault Tracking

Table of Contents

▶ Introduction – ITS Service Management and WAVE

▶ The Evolution of the WAVE Standard (2009)

▶ Securing ITS Services with WAVE (OSS Architecture)

▶ WAVE Service Provisioning, Identity Management and PKI

▶ A Security Model for Automotive Networking (ITS Services)

▶ Summary

WAVE Architecture Integration (Network and Security Services)

1609 Radio Stack

<<component>> DSRC Stack Interface

<<component>> WMIE

OBE DSRC

WSM/IP Sockets

WME API

Service Channel
Control Channel

PSIDs Passed at Initialization

Radio Handler

<<component>> Connection Manager

Advisory Messages

<<component>> Playlist Manager

Playlist

<<component>> Registration Manager

Socket Data

Application Control

Security Manager

Interfaces (RH RegMgr, 1609 SecLib)

Uses PSIDs from RH Config File
Looks for 'Security Tag' for PSIDs

Creates Security Library (WSC)
PSIDs register per 'Security Tag'

Fetches Identity Certs per WSC/PSID

Signs WSMs with Identity Certs

Proxy Manager

<<component>> Initializer

<<component>> Command Listener

RSE Certificate Manager Proxy

Interfaces (CA, LDAP, 1609 SecLib)

Fetches RSE Attributes (LDAP)
(index by RSE uid string)

Builds WSA Signing Cert (CA)
LDAP PSIDs for WSA Signing Cert

Polls Security Library (WSC)

Builds CSR Cert Request (CA)

Builds Identity Cert Request (CA)

Stores CA Results to 1609 SecLib
WSA Signing Cert, CSR Cert, IdentityCerts

XML Configuration File
Advertised Services

AMDS 11111111 Road Incident
AMDS 11122222 Road Condition
AMDS 11133333 Civil Emergency
AMDS 11144444 Cautions
AMDS 11155555 Traffic Delays
AMDS 11166666 Weather
AMDS 11177777 Road Service
AMDS 11188888 Food Service
AMDS 11199999 Vehicle Serive
AMDS 11121212 Lodging
AMDS 11132323 Closures
AMDS 11143434 MapElement
CICAS 22254545 Static
CICAS 22265656 Dynamic
POS 33376767 Positioning
PDS 444787878 PD Collect
PDS 44498989 PD Manage
EPAY 55509090 Parking
EPAY 55512312 Tolling
TRIP 66623423 TripPath
SEC 77734534 VHIP
NAV 88845645 NaviIP

Missing Services

EPAY 55556756 Parking Plaza WSMP
EPAY 55567867 Tolling Plaza WSMP
EPAY 55578978 Network IP
SEC 77786336 Certificate Manager
SEC 77786337 Certificate Update
SEC 77786338 CRL Update
HEART 00000000 Heartbeat
TRIP 66612312 Cert TripPath
NAV 88823423 Cert NaviIP

Radio Stack Security

WAVE Service Announcements

WSA Signing Certs Fetched From SecLib

PSIDs embedded in WSA signing certs

PSID Consistency Check
WSA PST compared to WSA Signing Cert PSIDs

NTRU 1609 Security Library Interface

NTRU 1609 Security Library Interface

NTRU 1609 Security Library Interface

Security

1690.2 Security Services

WAVE Security Context (WSC) Creation

WSCs Indexed with PSIDs (from RH SecMgr)

WSCs Updated by RSE Cert Mgr – CertAdd

Root Cert, WSA Certs, Identity Certs, CSR Certs

WSC Certs Fetched (by RH SecMgr)

WSA Certs Fetched by Radio Stack

Network Administration (Firewall, Ports/Services, Routing Tables, VPN)

LDAP IdM Interface

1609 Certificate Authority

LDAP IP Addesses (v4, v6)
vii-ds (LDAP)
2001:1890:110E:A600::B0/64

LDAP RSE Attributes for RSE CertMgr
PSID, Lat/Long, Radius, Priority

1690.2 CA IP Addresses
(CA)
2001:1890:110E:A580:93/64

RSE SW Build for 1609 Certificates
PSID Data Model and Process Model

ENOC INTERFACE TO RSE for 1609 Certificates

The Identity Repository (LDAP) creates and manages the assignment of RSE attributes for certificates (including PSIDs)

11111111,11122222,11133333,11144444,11155555,11166666,11177777,11188888,11199999,11121212,11123232,11143434,22254545,22265656,33376767,444787878,44498989,55509090,55512312,66623423,77734534,88845645,55556756,55567867,55578978,77786336,77786337,77786338,00000000,66612312,88823423 ← PSID Provisioning String

PSID Definition is WAVE(1609.3) Configurable data element published in the RSE Identity Certificate

Certificate Information

Database Data
Certificate ID: 3020
CertificateType: CSR
PSID: { 2, 22, 0, 1 }
PSID numeric: 34996225
Application Data: { 82, 69, 80, 76, 65, 67, 69, 95, 77, 69 }
CertID8: { -4, -19, 8, 98, -123, 125, -55, -74 }
CertID10: { -95, 124, -4, -19, 8, 98, -123, 125, -55, -74 }
Expired: false
Expiration Date: 2008-06-14 03:29:30
Revoked: false

Certificate Data
Certificate Type: CSR_SIGNER
Version: 1
Expiration Date: 2008-06-14 03:29:30
CRL Series: 2
Application PSIDs: 34668545, 33619969, 16842753, 34799617, 33751041, 83886337, 34930689, 35061761, 50266112, 16777217, 50331649, 34603009, 67108865, 34734081, 33685505, 17039361, 34865153, 33816577, 67371009, 34996225
Application and Priorities:
Tf Types: RSU
Scope Types: RSU
Opaque (Application Data): { 82, 69, 80, 76, 65, 67, 69, 95, 77, 69 }
Opaque (Application Data) String: REPLACE_ME
Region: Circular Region
Radius: 5 Latitude: 82 Longitude: 42
CertID8: { -4, -19, 8, 98, -123, 125, -55, -74 }
CertID10: { -95, 124, -4, -19, 8, 98, -123, 125, -55, -74 }
Verification Key: { 1, 3, -78, -51, -26, 50, 87, -91, 67, 9, -124, -67, -43, 14, -9, 19, 27, -37, 44, -78, -122, 11, 87, 48, 107, 53, -50, 22, 2, 52, -84, -84, -83, -30 }
Encryption Key: null

A Certificate Signing Request (CSR) is used to request RSE Identity Certificates
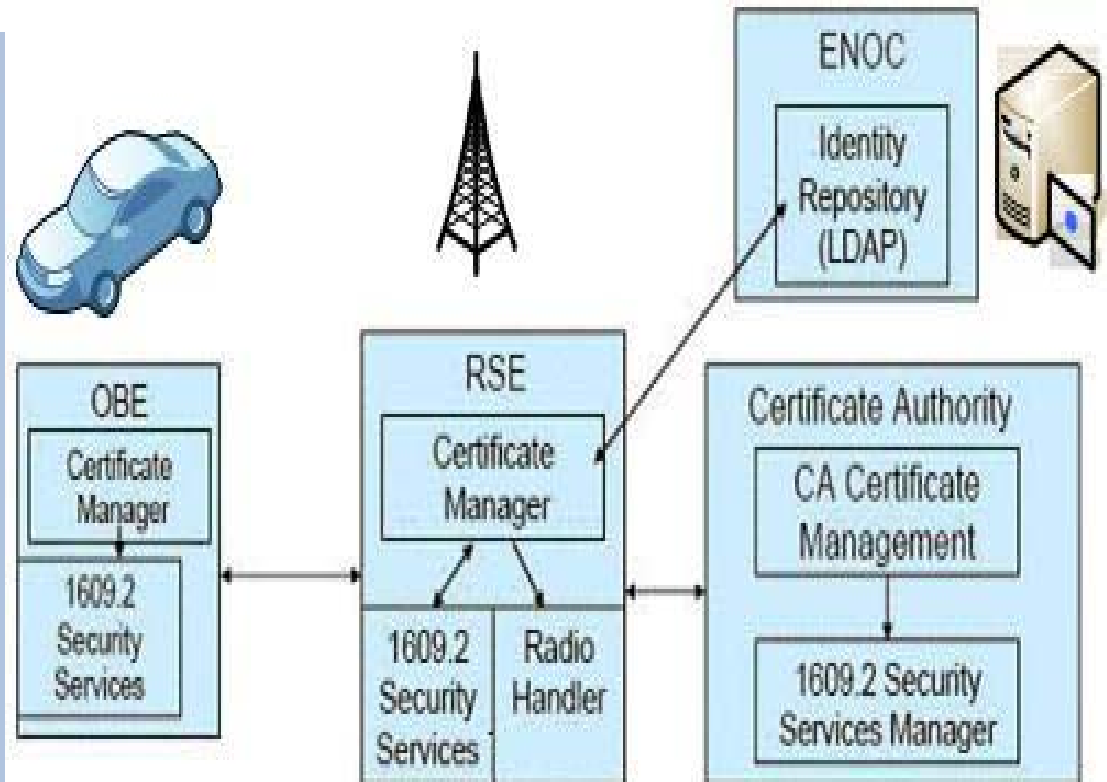
The **RSE Certificate Manager** provides management of the certificates within an RSE required to secure the communications of Identifying applications over the WAVE radio access network. The RSE Certificate Manager communicates with the Certificate Authority to acquire and replace certificates and to process certificate revocations .

Public Key Infrastructure - Certificate Authority Architecture
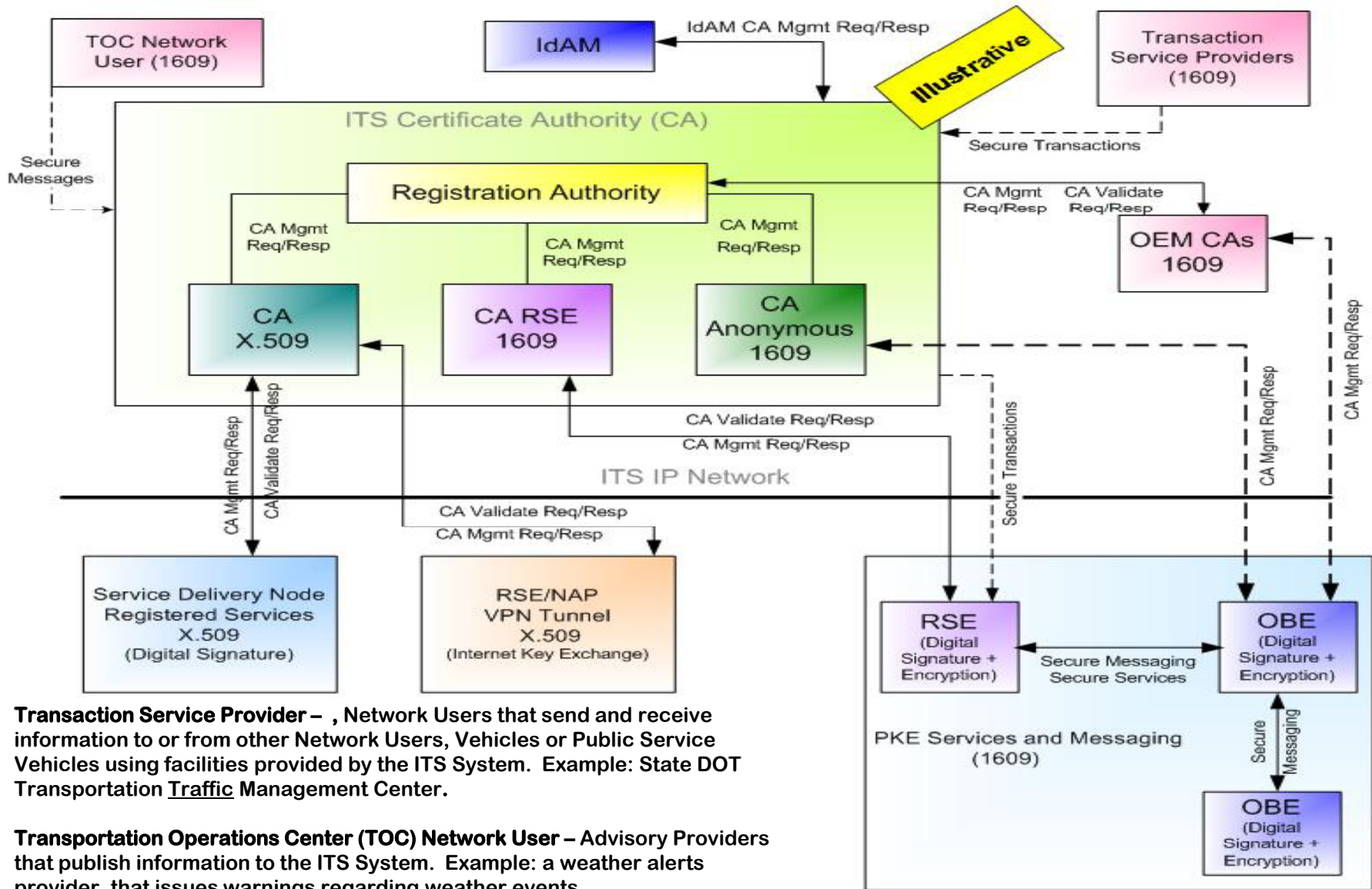
Transaction Service Provider – , Network Users that send and receive information to or from other Network Users, Vehicles or Public Service Vehicles using facilities provided by the ITS System. Example: State DOT Transportation Traffic Management Center.

Transportation Operations Center (TOC) Network User – Advisory Providers that publish information to the ITS System. Example: a weather alerts provider, that issues warnings regarding weather events

Illustrative mapping of 1609.2 Authentication Scenarios
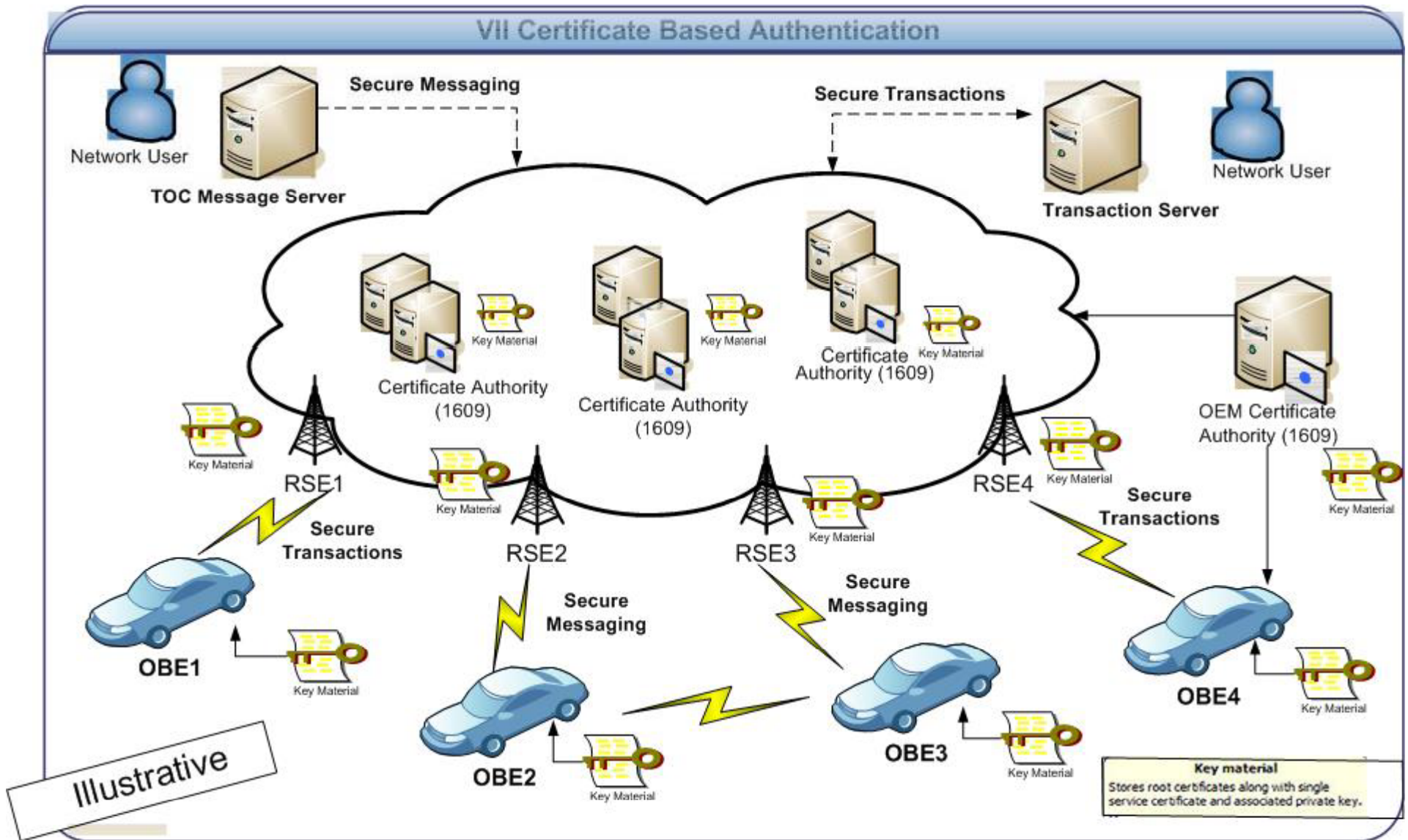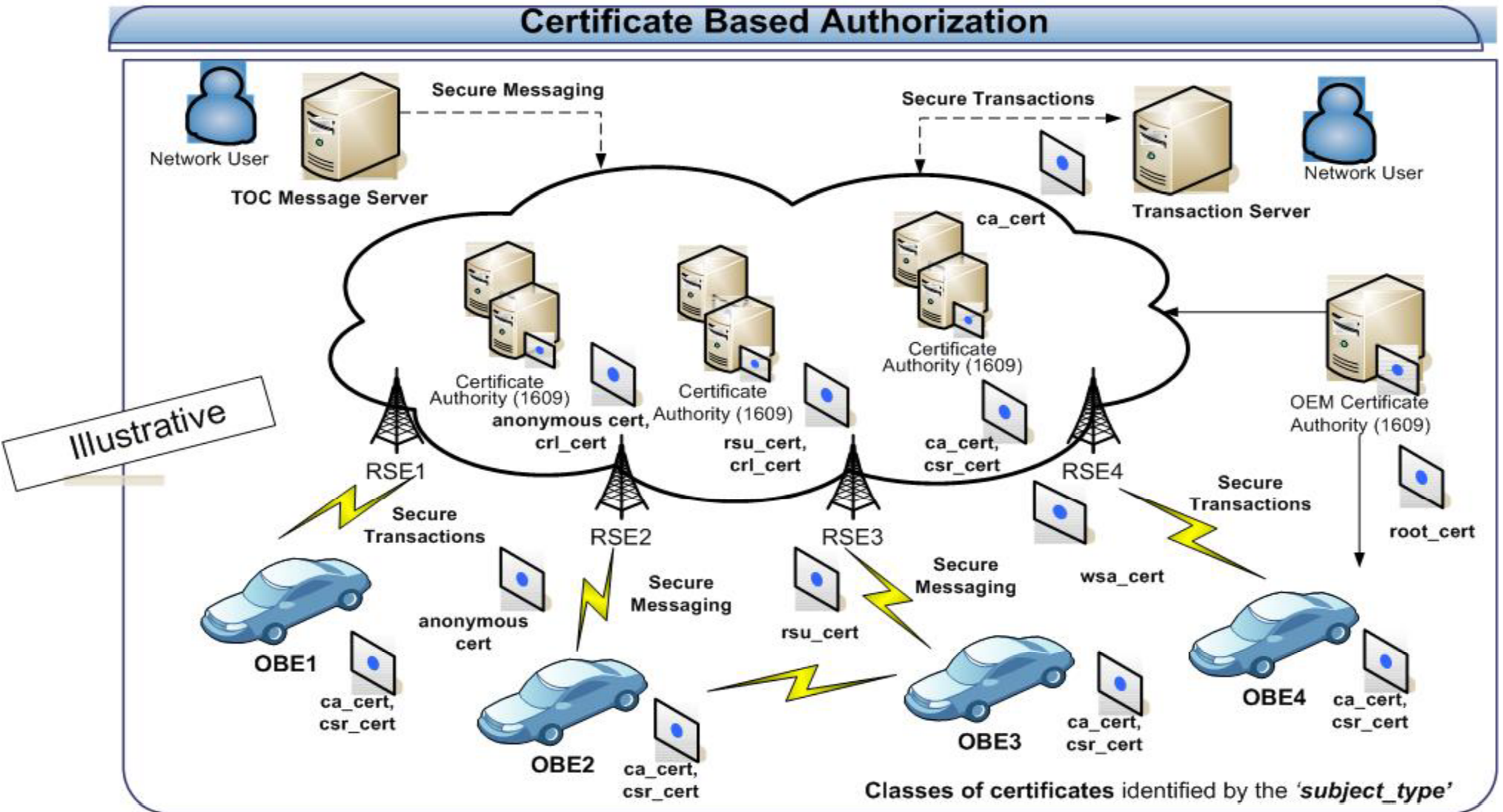
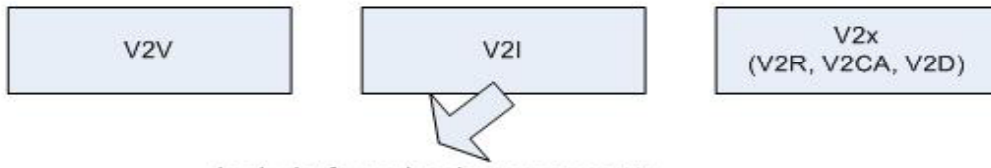# Illustrative Mapping of 1609.2 Authorization Scenarios

Table of Contents

The ITS Automotive Networking Landscape

ILLUSTRATIVE

ITS Services and Applications

- Safety Services
- Commercial Services
- Convenient/Comfort Services

Communication Platform

- V2V
- V2I
- V2x (V2R, V2CA, V2D)

Include fours basic components

Road Side Units (RSU)	On Board Units (OBU)
Back Office (Services, Infrastructure)	Devices and Sensors (Probe Data, HMI, Mobility)

- Basic Architecture (Illustrative of V2V, V2R, V2x)
- Scale Up Architecture (Realistic Deployment)
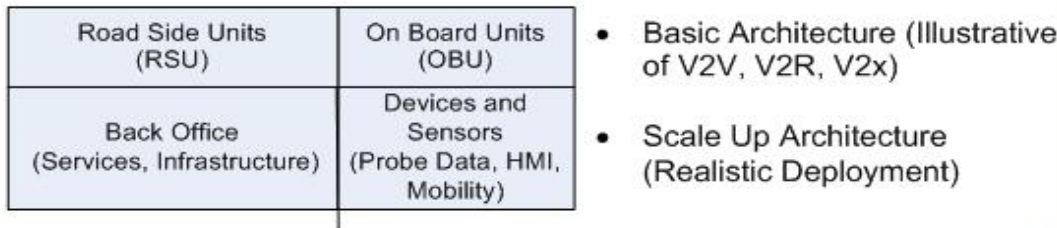
Platform Characteristics across V2V, V2I, V2x
(Why it is different and more challenging from traditional network platform?)

- Vehicular AdHoc Networks (VANET)

Communication and Platform Technologies

- Broadcast, Unicast, Geocast Protocols
- LTE, Satellite, Cellular, WiMax, RFID, Bluetooth
- Operating System Firmware
- WAVE/DSRC ETSI/ITU, ISO CALM
- 802.11p/802.11x
- Backhaul (3G, WiMax, IPv6)
- Automotive Messaging

ITS Implementations

- C2C-CC, CVIS, SAFESPOT, COOPERS, SeVeCom
- Intellidrive/VII, VSC
- Japan ITS/MLIT ITS (ETC, AHS, VICS)
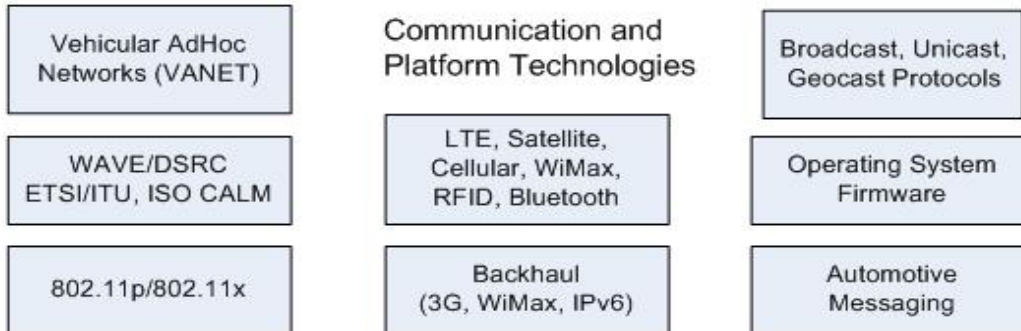
Security and Privacy Framework

Threat Models and Risk Assessment (What are the risks and impact if security and privacy of a specific ITS Service is compromised?)

Assurance Levels (Defined criticality levels)

Security and Privacy Requirements (What needs to be done?)

- ITS Service specific Requirements
- General Security and Privacy Principles (e.g. SeVeCom, VII, No Security)

Security Architecture (Solution Decision Blueprint)

Architecture Principle (e.g. SeVeCom, OSI, Intellidrive)

Architecture Components

- Identity Management
- Secure Comm
- Tamper Proof Devices
- Anonymity & Psudonymity
- Secure Messaging
- Secure Applications
- Privacy

, and more ...

Component Relationships (How do Architecture Components compose the overall architecture?)

Technical Solutions (incl. research contributions)

- PKI (1609, X.509, Anonymous)
- Protocols (V-HIP, V-DTLS, SAE J2735)
- Encryption (ECDSA, RSA ECIES, IBE)

, and more ....

Security Testing Methods

Table of Contents

▸ Introduction – ITS Service Management and WAVE

▸ The Evolution of the WAVE Standard (2009)

▸ Securing ITS Services with WAVE (OSS Architecture)

▸ WAVE Service Provisioning, Identity Management and PKI

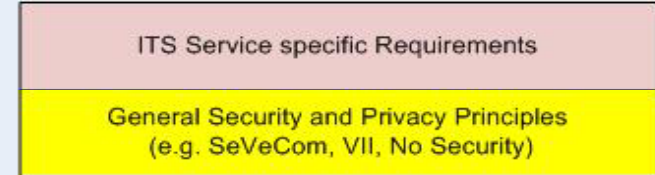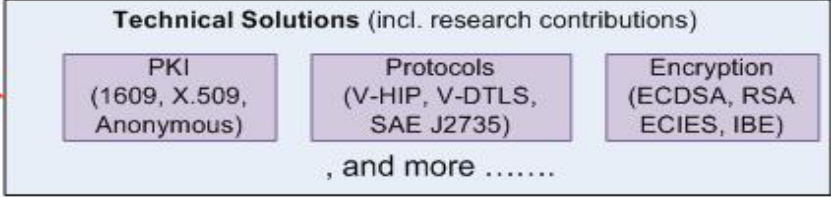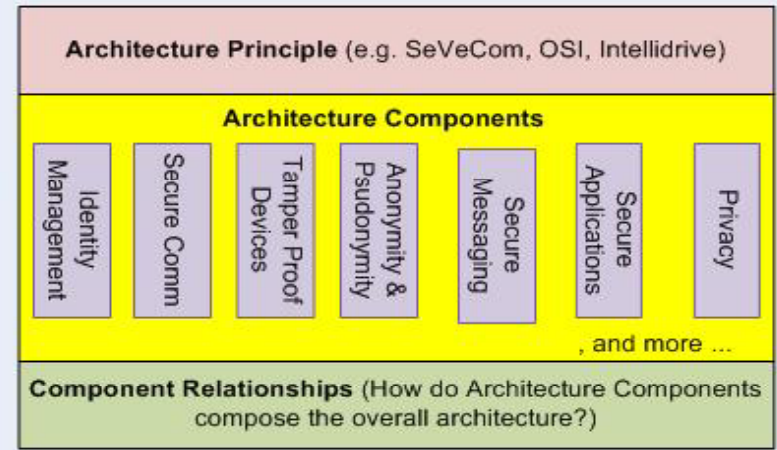▸ A Security Model for Automotive Networking (ITS Services)

▸ Summary

Thank you for joining us!

Security for ITS Websites – **http://securityfeeds.com/tweil/dwd.html**

WAVE Networking Services – Secure WAVE Service Advertisement (1609.0)

The WME generates a WAVE Service Advertisement, which will be transmitted to potential service users. The WME collects the application information describing the services being offered, previously registered in its MIB, and channel characteristics, also from the MIB, and inserts them into the WAVE Service Advertisement as Service Information. In addition, if the service is IP-oriented the IP network configuration information (WRA) from the MIB is included.
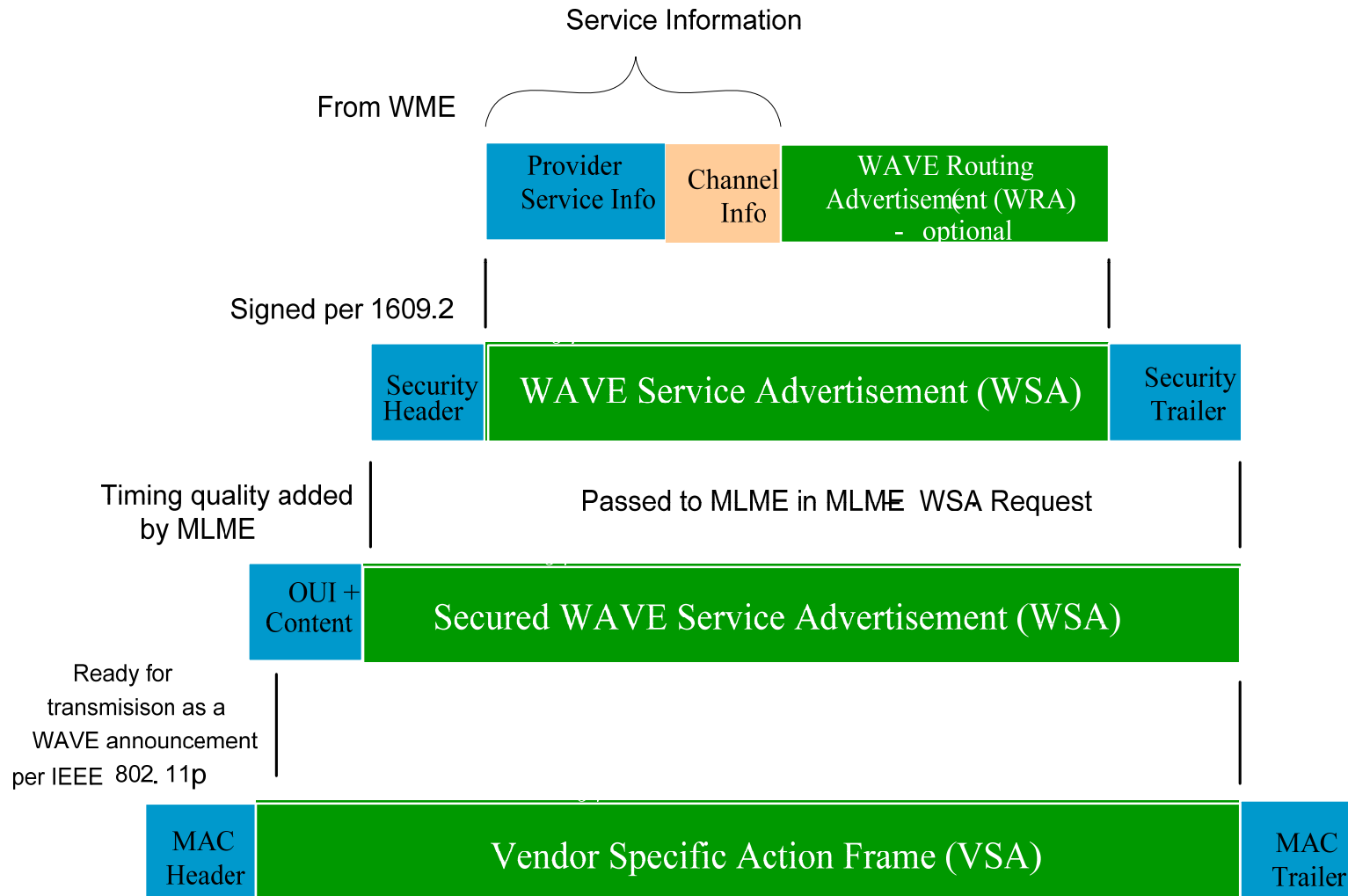
WAVE Advertisement – Communication with a service (1609.0)

A WAVE service is supported by time and frequency (channel) resources allocated at some set of participating devices within communication range, in support of one or more applications. The service is initiated at the request of the application at one device (the provider), and announced on the CCH.

Applications offering services to potential user applications are announced on the air interface via an advertisement inside a WAVE management frame.
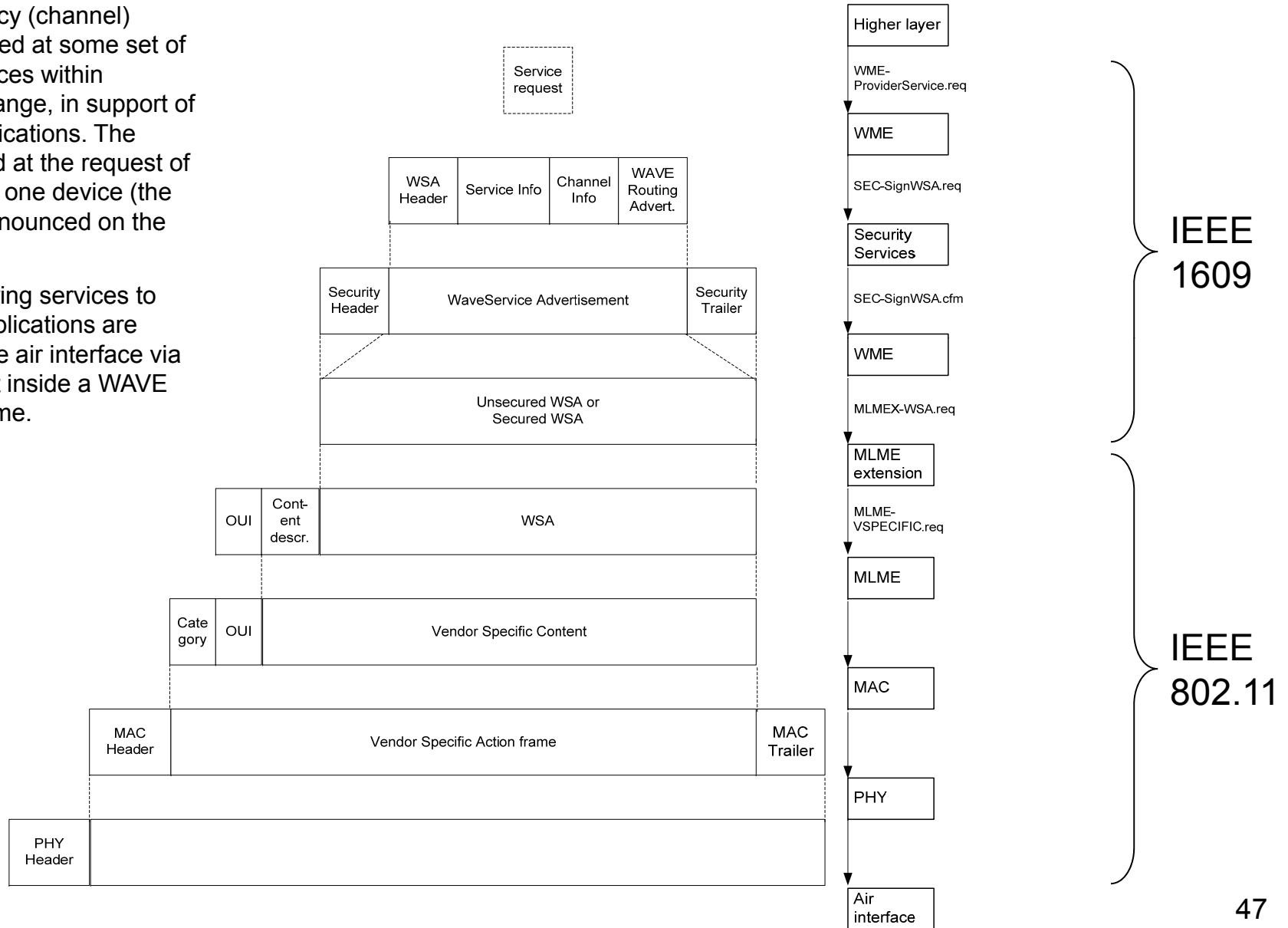
WAVE Networking Services – WAVE Service Advertisement (new format)

Streamlines message.   Makes more consistent use of WAVE Element IDs and Extension (optional) fields.

1	Var.	Var.		
WAVE version/ change count	Extension fields	Service Info	Channel Info	WAVE Routing Advertisement

Header

1	Var.	1	1	Var.
WAVE Element ID=1	PSID	Service Priority	Channel Index	Extension fields

May be repeated

1	1	1	1	1	1	Var.
WAVE Element ID=2	Operat-ing Class	Channel Number	Adapt-able	Data Rate	Transmit Power Level	Extension fields

May be repeated

KEY

(shaded box)	Optional Field

Lengths in octets

1	2	16	1	16	6	16	Var.
WAVE Element ID=3	Router lifetime	IpPrefix	Prefix length	Default gateway	Gateway MAC address	Primary DNS	Extension fields

48