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
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
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 –
http://www.etsi.org/WebSite/document/Technologies/ETSI-ITS.jpgg
Introduction – USDOT ITS National Architecture (DSRC)

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) –


<table>
<thead>
<tr>
<th>Topics</th>
<th>Replies</th>
<th>Author</th>
<th>Views</th>
<th>Last Post</th>
</tr>
</thead>
<tbody>
<tr>
<td>Announcement: From NTOC Newsletter</td>
<td>0</td>
<td>tkurhara</td>
<td>221</td>
<td>Thu Aug 31, 2006 9:27 pm tkurhara D</td>
</tr>
<tr>
<td>Sticky: Finding download files in the DSRC forum</td>
<td>0</td>
<td>DC Kelley</td>
<td>618</td>
<td>Thu Jul 07, 2005 2:30 pm DC Kelley D</td>
</tr>
<tr>
<td>Re: P1609.3 updates from Albany discussions</td>
<td>2</td>
<td>AMalkray at IVHS.COM</td>
<td>26</td>
<td>Mon Oct 23, 2006 9:17 am John Morino D</td>
</tr>
<tr>
<td>Fwd: TC204: Upcoming Ballot Items for November 6th</td>
<td>0</td>
<td>tkurhara</td>
<td>20</td>
<td>Sun Oct 22, 2006 3:43 pm tkurhara D</td>
</tr>
<tr>
<td>Dot3 Review</td>
<td>0</td>
<td>tkurhara</td>
<td>41</td>
<td>Fri Oct 20, 2006 3:49 pm tkurhara D</td>
</tr>
<tr>
<td>P1609.3 updates from Albany discussions</td>
<td>0</td>
<td>John Morino</td>
<td>36</td>
<td>Fri Oct 20, 2006 2:26 pm John Morino D</td>
</tr>
</tbody>
</table>
Prototype of DSRC Architecture and Components (OmniAir Consortium)
RSU and OBU Protocol Stacks (1609.3 Model)

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.
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
  - 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

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.


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.


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.


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.


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.
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
  - 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

IEEE 1609 (WAVE) Working Group

- 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
  WiWe, 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

Maintained by Susan Dickey
Last modified: August 31, 2008

http://vii.path.berkeley.edu/1609_wave
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)
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.
### Networking and Service Managements Features addressed in the IEEE Standards (1609.0/.3)

<table>
<thead>
<tr>
<th>Features of 1609.0 and 1609.3</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WAVE Services (1609.0)</strong></td>
<td>A capability, provided by an application, that makes use of WAVE communication facilities. Services are classified as Persistent or Non-Persistent</td>
</tr>
<tr>
<td><strong>WAVE Management Entity (WME)</strong></td>
<td>A set of management functions required to provide WAVE Networking Services.</td>
</tr>
<tr>
<td><strong>WAVE Service Advertisement (WSA)</strong></td>
<td>A data structure containing information that announces the availability of a service. A VSA is composed of such structures</td>
</tr>
<tr>
<td><strong>WAVE Short Message Protocol (WSMP)</strong></td>
<td>A protocol for rapid, reliable exchange of messages in a rapidly-varying RF environment where low-latency is also an important objective.</td>
</tr>
<tr>
<td><strong>ProviderServiceInfo (MIB Entry)</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Provider Service ID (PSID)</strong></td>
<td>An octet string that identifies a service provided by a higher layer entity</td>
</tr>
<tr>
<td><strong>Provider Service Context (PSC)</strong></td>
<td>A field associated with a PSID containing supplementary information related to the service. The format of the PSC is PSID dependent.</td>
</tr>
<tr>
<td><strong>Control Channel (CCH)</strong></td>
<td><strong>CCH</strong> - A single radio channel, not a service channel, intended for exchange of management frames, including WAVE Service Advertisements, and WAVE Short Messages.</td>
</tr>
<tr>
<td><strong>Service Channel (SCH)</strong></td>
<td><strong>SCH</strong> - 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.</td>
</tr>
</tbody>
</table>

- **WSA-Type**
- **ProviderServiceIdentifier**
- **Service Priority**
- **Regulatory Class**
- **ChannelSelection**
- **IP Service**
- **IPv6 Address**
- **Provider MAC**
- **AddressServiceStatus**
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
<table>
<thead>
<tr>
<th>Importance Level from USA FCC Policy</th>
<th>Description (When to apply a specific urgency level)</th>
<th>Description (When to apply a specific urgency level)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 = Safety of Life Applies to those Messages and Message Sets associated with societal and/or safety impact related to human life.</td>
<td>Emergency Impact mitigation and injury avoidance/mitigation</td>
<td>Urgent warning of impending local situation</td>
</tr>
<tr>
<td></td>
<td>Emergency Potential-event impact and/or injury mitigation and avoidance</td>
<td>Situation-based status information of uninvolved local interest</td>
</tr>
<tr>
<td></td>
<td>Urgent Warning Events (Event Flags)</td>
<td>Intersection and vehicle safety status information</td>
</tr>
<tr>
<td>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)</td>
<td>Urgent public safety downloads (Intersection Information)</td>
<td>Semi-urgent public safety link establishment</td>
</tr>
<tr>
<td></td>
<td>Urgent public safety downloads (Intersection Information)</td>
<td>Semi-urgent public safety data and application enabler</td>
</tr>
<tr>
<td></td>
<td>Urgent public safety downloads (Intersection Information)</td>
<td>Semi-urgent public safety data and application enabler</td>
</tr>
<tr>
<td></td>
<td>Public safety data transactions, exchanges</td>
<td>Important Traffic Management status information enabler</td>
</tr>
<tr>
<td></td>
<td>Public safety geospatial context information</td>
<td>Important Announcement of WAVE Services</td>
</tr>
<tr>
<td></td>
<td>Public safety geospatial context information</td>
<td>Non-urgent Traffic Management Foundational Data</td>
</tr>
<tr>
<td></td>
<td>Public safety RTCM GPS correction information</td>
<td></td>
</tr>
<tr>
<td>3 = Non-Priority Communications (Not in 1 or 2) Applies to Fleet Management, Traveler Information Services and Private Systems.</td>
<td>Urgent, private and commercial electronic transactions</td>
<td>Important, private and commercial electronic transactions</td>
</tr>
<tr>
<td></td>
<td>Semi-Urgent, private mobility data and electronic transactions</td>
<td>Background, private mobility data downloads and upgrades</td>
</tr>
</tbody>
</table>
## AuthN/AuthZ Features addressed in the IEEE 1609 Standards

<table>
<thead>
<tr>
<th>Identity Management Features of 1609.2/1609.3</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Classes of Digital Certificates</strong></td>
<td>There are <strong>classes of certificates</strong> identified by the <code>subject_type</code> 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.</td>
</tr>
<tr>
<td><strong>Securing Transactions</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Securing Messages Structures</strong></td>
<td>A secure message type is a published 1609.2 data structure with these options - <strong>unsecured message, signed message</strong> or <strong>signed WSM</strong>.</td>
</tr>
<tr>
<td><strong>Bootstrapping Trust</strong></td>
<td>All WAVE equipment are provisioned with a public key that can be used to validate root certificate updates. <strong>OBEs</strong> can generate their own key pairs.</td>
</tr>
<tr>
<td><strong>Signed Messages</strong></td>
<td><strong>ECDSA</strong> signed messages provides authentication for WAVE multicast messages.</td>
</tr>
<tr>
<td><strong>Encrypting Message Structures</strong></td>
<td>The <code>EncryptedMessage</code> type is a subtype of the <code>SecuredMessage</code> type. A WAVE certificate contains one or two keys for either encryption, verification or both functions.</td>
</tr>
<tr>
<td><strong>Provider Service ID (PSID)</strong></td>
<td>A signed number that identifies a service provided by an application and announced in the WAVE Service Announcement (WSA) PSID.</td>
</tr>
<tr>
<td><strong>Certificate Requests</strong></td>
<td>Device provisioning with certificates use either ‘push’ or ‘pull’ model. ‘Pull Model’ is supported with a CSR message type in 1609.2.</td>
</tr>
<tr>
<td><strong>Certificate Revocation Lists</strong></td>
<td>1609.2 defines a CRL type. The ‘Security Manager’ annex describes the CRL functionality on a 1609 device (i.e. OBE).</td>
</tr>
<tr>
<td><strong>Anonymity</strong></td>
<td>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.</td>
</tr>
</tbody>
</table>
1609.2 Security Subsystem Diagram
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

Availability

Integrity
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

<table>
<thead>
<tr>
<th>Safety message</th>
<th>Cryptographic material</th>
</tr>
</thead>
<tbody>
<tr>
<td>≈ 100 bytes</td>
<td>≈ 140 bytes</td>
</tr>
<tr>
<td>{Position, speed, acceleration, direction, time, safety events}</td>
<td>{Signer’s digital signature, Signer’s public key PK, CA’s certificate of PK}</td>
</tr>
</tbody>
</table>
WAVE Architecture Integration – Component Services (1609.2/1609.3)

- ITS Service Provisioning
- Network Services
- Configuration Management
- Protocol Enhancements
- WAVE Service Provisioning (WSA)
- Identity Management
- Public Key Infrastructure
- WAVE Monitoring
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)

- 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
The Identity Repository (LDAP) creates and manages the assignment of RSE attributes for certificates (including PSIDs).
ITS Service Provisioning – 2 of 2
ITS Identity Management (PSID Creation) – 1 of 2

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

Certificate Based Authorization

Classes of certificates identified by the 'subject_type'
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
The ITS Automotive Networking Landscape

**Communication Platform**

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

Include four basic components:
- 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?)

**ITS Services and Applications**

- Safety Services
- Commercial Services
- Convenient/Comfort Services

**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, CSI, Intellidrive)

  - **Architecture Components**
    - Identity Management
    - Secure Communication
    - Tamper Proof Devices
    - Anonymous & Pseudonymous
    - Messaging
    - Secure Applications
    - Privacy

- **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, EGIES, IBE)

**Security Testing Methods**

**ITS Implementations**

- C2C-CC, CVIS, SAFESPOT, COOPERS, SeVeCom
- Intellidrive/VII, VSC
- Japan ITS/MLIT ITS (ETC, AHS, VICS)
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!
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.
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.