EU-US Standards Harmonization Task Group Report: Testing for ITS Security

Document HTG1-2

EU-US ITS Task Force
Standards Harmonization Working Group
Harmonization Task Group 1

November 12, 2012

Publication # FHWA-JPO-13-078

European Commission

U.S. Department of Transportation

EU US ITS COOPERATION

Produced by the Implementing Arrangement between the European Commission and the U.S. Department of Transportation in the field of research on Information and Communications Technologies for transportation

U.S. Department of Transportation

Research and Innovative Technology Administration (RITA)

Notice

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-13-078		

4. Title and Subtitle	5. Report Date
EU-US Standards Harmonization Task Group Report: Testing for ITS Security (Document HTG1-2)	November 12, 2012
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Scott Cadzow, Wolfgang Hoefs, Eric Koenders, Ola Martin Lykkja, Richard Roy, Steve Sill, Siebe Turksma, William Whyte	

9. Performing Organization Name And Address	10. Work Unit No. (TRAIS)
ITS Joint Program Office, Research and Innovative Technology Administration, U.S. Department of Transportation, 1200 New Jersey Avenue, SE, Washington, DC 20590	11. Contract or Grant No.

12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
	14. Sponsoring Agency Code

15. Supplementary Notes

16. Abstract

Harmonization Task Group 1 (HTG1) was established by the EU-US International Standards Harmonization Working Group to attempt to harmonize standards (including ISO, CEN, ETSI, IEEE) on security to promote cooperative ITS interoperability. HTG1 worked in close coordination with HTG3 whose focus is on harmonization of communications protocols. In collaboration, the two HTGs developed an integrated set of technical reports including this report. This report describes a set of interoperability tests, the results of which are intended to give confidence that ITS stations interoperate cooperatively and securely. It should be read in conjunction with HTG1-1— Status of ITS Security Standards, which summarizes the analysis conducted to identify the necessary subset of available standards to provide assurance of interoperable security measures in Cooperative ITS (C-ITS).

17. Key Words	18. Distribution Statement
intelligent transport systems, mobile, standards, harmonization, cooperative, safety, interoperability, security, communications, protocol	

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
		25	

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

Table of Contents

1 References

This list of references is not intended to be a complete list of all HTG-related standards but reflects a snap-shot used by the HTG3 team. This list does not indicate any preference for an SDO.

References without a date in their titles are currently under development and may not be publicly available. For non-specific references (i.e., undated or no specific version number), the latest edition of the referenced document (including any amendments) applies.

1.1 ISO

[1] ISO 16444, Intelligent transport systems—Communications access for land mobiles (CALM)—Geo-Routing

[2] ISO 16788, Intelligent transport systems—Communications access for land mobiles (CALM)—IPv6 networking security

[3] ISO 16789, Intelligent transport systems—Communications access for land mobiles (CALM)—IPv6 optimization

[4] ISO 21210:2012, Intelligent transport systems—Communications access for land mobiles (CALM)—IPv6 Networking

[5] ISO 21215:2010, Intelligent transport systems—Communications access for land mobiles (CALM)—M5

[6] ISO 21217:2010, Intelligent transport systems—Communications access for land mobiles (CALM)—Architecture

[7] ISO 21217, Intelligent transport systems—Communications access for land mobiles (CALM)—Architecture

[8] ISO 21218:2008, Intelligent transport systems—Communications access for land mobiles (CALM)—Medium service access points

[9] DIS 21218:2012, Intelligent transport systems—Communications access for land mobiles (CALM)—Access technology support

[10] ISO 24102:2011, Intelligent transport systems—Communications access for land mobiles (CALM)—Management

[11] DIS 24102-1:2012, Intelligent transport systems—Communications access for land mobiles (CALM)—Station management—Part 1: ITS station management

[12] ISO/NP 24102-2:2012, Intelligent transport systems—Communications access for land mobiles (CALM)—Station management—Part 1: Remote management

[13] DIS 24102-3:2012, Intelligent transport systems—Communications access for land mobiles (CALM)—Station management—Part 3: Management SAPs

[14] DIS 24102-5:2012, Intelligent transport systems—Communications access for land mobiles (CALM)—Station management—Part 5: Fast service advertisement protocol (FSAP)

[15] ISO 29281:2011, Intelligent transport systems—Communications access for land mobiles (CALM)—Non-IP networking

[16] DIS 29281-1:2012, Intelligent transport systems—Communications access for land mobiles (CALM)—Non-IP networking—Part 1: Fast networking & transport layer protocol (FNTP)

[17] DIS 29281-2:2012, Intelligent transport systems—Communications access for land mobiles (CALM)—Non-IP networking—Part 2: ISO 15628 support

[18] ISO 18377, Intelligent transport systems—Communications access for land mobiles (CALM)—Conformance Requirements

[19] TR 17465-1, Intelligent transport systems—Terms, definitions and guidelines for Cooperative ITS standards documents—Part 1: Terms, definitions and outline guidance for standards documents

[20] ISO/IEC 7498-1:1994, Information technology—Open Systems Interconnection—Basic Reference Model: The Basic Model

[21] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation criteria for IT security - Part 2: Security functional requirements"

1.2 CEN

[22] CEN ISO 17419, Classification and management of ITS applications in a global context

[23] CEN ISO 17423, Intelligent Transport Systems—Cooperative Systems—Application requirements for selection of communication profiles

1.3 ETSI

[24] ETSI TS 102 636-x, Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking;
Part 1: Requirements (2010)
Part 2: Scenarios (2010)
Part 3: Network architecture (2010)
Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications

- Sub-part 1: Media-Independent Functionality (2011)
- Sub-part 2: Media dependent functionalities for ITS-G5A media (draft)
Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol (2011)
Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols (2011)

[25] ETSI EN 302 637-2, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Service

[26] ETSI TS 102 637-3 V1.1.1:2010, Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service

[27] ETSI ES 202 663 V1.1.0:2010, Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band

[28] ETSI EN 302 665 V1.1.1:2010, Intelligent Transport Systems (ITS); Communications Architecture

[29] ETSI TS 102 687 V1.1.1:2011: Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part

[30] ETSI TS 102 724, Intelligent Transport Systems (ITS); Harmonized Channel Specifications for Intelligent Transport Systems operating in the 5 GHz frequency band, Channel specifications 5 GHz

[31] ETSI TS 102 731, Intelligent Transport Systems (ITS); Security Architecture and Services

[32] ETSI TS 102 860 V1.1.1:2011, Intelligent Transport Systems (ITS); Classification and management of ITS application objects

[33] ETSI TS 102 867, Intelligent Transport Systems (ITS); 1609.2 mapping

[34] ETSI TS 102 890-2, Intelligent Transport Systems (ITS); Facilities layer function Part 2: Services announcement specification

[35] ETSI TS 102 940, Intelligent Transport Systems (ITS); Security Architecture

[36] ETSI TR 102 893, Intelligent Transport Systems (ITS); Threat Vulnerability and Risk Analysis

[37] ETSI EN 302 931 V1.1.1:2011, Intelligent Transport Systems (ITS); Vehicular Communications; Geographical Area Definition

[38] ETSI TS 102 941, Intelligent Transport Systems (ITS); Trust and Privacy

[39] ETSI TS 102 942, Intelligent Transport Systems (ITS); Access Control

[40] ETSI TS 102 943, Intelligent Transport Systems (ITS); Confidentiality Services

[41] ETSI TR 102 962 V1.1.1:2012. Intelligent Transport Systems (ITS); Framework for Public Mobile Networks in Cooperative ITS (C-ITS)

[42] Draft ETSI TS 102 965, Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration list

[43] Online registry for ITS-AID: http://aid.its-standards.info/ITS-AID Registry/ITSaidRegistrationIndex.html

1.4 IEEE

[44] IEEE 802™:2001, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture

[45] ISO/IEC 8802-2:1998, ANSI/IEEE Std 802.2™:1998, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks— Specific requirements Part 2: Logical Link Control

[46] IEEE Std 802.3™:2000, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications

[47] Ethertype registry: http://standards.ieee.org/develop/regauth/ethertype/public.html

[48] IEEE Std 802.11™:2012, IEEE Standard for Information technology—Telecommunications and information exchange between systems - Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications

[49] IEEE P1609.0™ D3, Draft Guide for Wireless Access in Vehicular Environments (WAVE)—Architecture

[50] IEEE P1609.2™ D15, Draft Standard for Wireless Access in Vehicular Environments (WAVE)—Security Services for Applications and Management Messages

[51] IEEE Std 1609.3™:2010, IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Networking Services

[52] IEEE Std 1609.4™:2010, IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Multi-channel Operation

[53] IEEE Std 1609.11™:2010, IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Over-the-Air Electronic Payment Data Exchange Protocol for Intelligent Transport Systems (ITS)

[54] IEEE P1609.12™:D7, IEEE Standard for Wireless Access in Vehicular Environments (WAVE)—Identifier allocations

1.5 Regulations

[55] FCC 47 CFR 90 Telecommunications, Private land mobile radio services, 371 – 377: Regulations governing the licensing and use of frequencies in the 5850–5925 MHz band for dedicated short-range communications service (DSRCS)

[56] FCC 06-110 Amendment of the Commission's Rules Regarding Dedicated Short-Range Communication Services in the 5.850-5.925 GHz Band (5.9 GHz Band); Memorandum Opinion and Order to designate channels 172 and 184 for safety of life and property usage

[57] FCC 47 CFR 15 Telecommunications, Radio frequency devices

[58] ETSI EN 302 571 V1.2.1: 2008, Intelligent Transport Systems (ITS); Radio communications equipment operating in the 5 855 MHz to 5 925 MHz frequency band; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive

[59] ETSI EN 301 893 V1.7.1: 2012, Broadband Radio Access Networks (BRAN); 5 GHz high-performance RLAN; Harmonized EN covering the essential requirements of article 3.2 of the R&TTE Directive

1.6 Testing

[60] ETSI EG 202 798 V1.1.1 (2011-01), Intelligent Transport Systems (ITS); Testing; Framework for conformance and interoperability testing

[61] ETSI TS 102 985-1 V1.1.1 (2012-07), Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for ITS station management (ISO 24102);
Part 1: Protocol implementation conformance statement (PICS) proforma
Part 2: Test Suite Structure and Test Purposes (TSS&TP)
Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma

[62] ETSI TS 102 797-1 V1.1.1 (2012-08), Intelligent Transport Systems (ITS); Communications Access for Land Mobiles (CALM); Test specifications for non-IP networking (ISO 29281);
Part 1: Protocol implementation conformance statement (PICS) proforma
Part 2: Test Suite Structure and Test Purposes (TSS&TP)
Part 3: Abstract Test Suite (ATS) and partial PIXIT proforma

[63] ETSI TS 102 868 V1.1.1 (2011-03), Intelligent Transport Systems (ITS); Testing; Conformance test specification for Co-operative Awareness Messages (CAM);

Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma
Part 2: Test Suite Structure and Test Purposes (TSS&TP)
Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)

[64] ETSI TS 102 916-1 V1.1.1 (2012-05), Intelligent Transport Systems (ITS); Test specifications for the methods to ensure coexistence of Cooperative ITS G5 with RTTT DSRC;
Part 1: Protocol Implementation Conformance Statement (PICS)
Part 2: Test Suite Structure and Test Purposes (TSS&TP)
Part 3: Abstract Test Suite (ATS) and partial Protocol Implementation eXtra Information for Testing (PIXIT)

[65] ETSI EG 202 237 V1.2.1 (2010-08), Methods for Testing and Specification (MTS); Internet Protocol Testing (IPT); Generic Approach to Interoperability Testing

1.7 Other references

[66] HTG1&3-1:2012, Overview of Harmonization Task Groups 1 & 3

[67] HTG1-1:2012, Status of ITS Security Standards

[68] HTG1-2:2012, Testing for ITS Security

[69] HTG1-3:2012, Feedback to Standards Development Organizations

[70] HTG3-1:2012, Status of ITS Communications Standards

[71] HTG3-2:2012, Testing for ITS Communications

[72] HTG3-3:2012, Feedback to Standards Development Organizations

[73] HTG1&3-3:2012, Observations on GeoNetworking

[74] IANA, Port number registry
http://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xml

[75] SAE J2735: DEDICATED SHORT RANGE COMMUNICATIONS (DSRC) MESSAGE SET DICTIONARY

[76] Certicom Letter of Assurance to IEEE: http://standards.ieee.org/about/sasb/patcom/loa-1609_2-certicom-22dec2010.pdf

[77] F. Kargl, Florian Schaub, Stefan Dietzel, Mandatory Enforcement of Privacy Policies using Trusted Computing Principles, Intelligent Information Privacy Management Symposium (Privacy 2010), AAAI, March 2010, http://vts.uni-ulm.de/doc.asp?id=7278

[78] R. Agrawal, J. Kiernan, R. Srikant, Y. Xu, Hippocratic Databases, Proceedings of the 28th VLDB Conference, Hong Kong, China, 2002

[79] European Parliament and Council. 1995. Directive 95/46/ec (Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data). Official Journal L 281, 23/11/1995 P. 0031 - 0050.

[80] European Parliament and Council. 2002. Directive 2002/58/ec (Directive on Privacy and Electronic Communications). Official Journal L 201, 31/07/2002 P. 0037 - 0047.

[81] OECD. 1999. OECD guidelines on the protection of privacy and transborder flows of personal data. http: //www.oecd.org/document/18/0,2340,en_ 2649_34255_1815186_1_1_1_1,00%.html.

[82] Bundesrepublik Deutschland. 2003. Bundesdatenschutzgesetz (BDSG). Version as published on 14. January 2003 (BGBl. I S. 66), last changed in Article 1 on 14. August 2009 (BGBl. I S. 2814).

[83] Peter Hustinx, Opinion of the European Data Protection Supervisor on the Communication from the Commission on an Action Plan for the Deployment of Intelligent Transport Systems in Europe and the accompanying proposal for a Directive of the European Parliament and of the Council laying down the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other transport modes, Official Journal of the European Union, Vol. 47(2), pp 6-15, 2010

[84] U.S. Supreme Court, 460 U.S. 276 UNITED STATES v. KNOTTS CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE EIGHTH CIRCUIT No. 81-1802. Argued December 6 1982 Decided March 2, 1983, http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=460&invol=276

[85] EU FP7 project i-SCOPE (http://www.iscopeproject.net/)

[86] EU FP7 project i-Tour (http://www.itourproject.com/web/)

2 Glossary and abbreviations

2.1 Abbreviations

Table 1 below lists acronyms used in documents produced by the HTG1 and HTG3 teams.

Table 1: Acronyms

Acronym	Meaning	Reference
API	Application Programming Interface	[7]
BRAN	Broadband Radio Access Networks	[59]
BSMD	Bounded Secured Managed Domain	[7]
BSS	Basic Service Set	
BTP	Basic Transport Protocol	[24]
CCH	Control Channel	[22, 27]
CEN	Comité Européen de Normalisation	http://www.cen.eu
CI	Communication Interface	[9]
CIP	Communication Interface Parameter	[16]
C-ITS	Cooperative ITS	[7, 19]
CTX	Context message	
DCC	Distributed Congestion Control	[29]
DIS	Draft International Standard	ISO
DSAP	Destination SAP address	[45]
EDCA	Enhanced Distributed Channel Access	
EN	European Norm	ETSI
ETSI	European Telecommunications Standards Institute	http://www.etsi.org
EU	European Union	general
FCC	Federal Communications Commission	http://www.fcc.gov/

Acronym	Meaning	Reference
FNTP	Fast Networking & Transport layer Protocol	[16]
From DS	Field in the IEEE Std 802.11 MAC header	
FSAP	Fast Service Advertisement Protocol	
GeoNet	Name of an EU research project	www.geonet-project.eu
GeoNetworking	Name of a protocol developed at ETSI based on the results from GeoNet	[24]
HTG	Harmonization Task Group	
IANA	Internet Assigned Numbers Authority	http://www.iana.org
IEEE	Institute of Electrical and Electronics Engineers	http://www.ieee.org
IETF	Internet Engineering Task Force	http://www.ietf.org
IP	Internet Protocol	IETF
IPv6	Version 6 of the Internet Protocol	IETF
ISO	International Standards Organization	http://www.iso.org
ITS	Intelligent Transport Systems (CEN, ETSI, ISO) Intelligent Transportation Systems (US)	[7]
ITS-AID	ITS Application Identifier	[32]
ITS-S	ITS Station	[7]
LLC	Logical Link Control	[44]
MAC	Medium Access Control	[44]
MIB	Management Information Base	[44]
OSI	Open Systems Interconnection	[20]
PDU	Protocol Data Unit	[44]
PSID	Provider Service Identifier	

Acronym	Meaning	Reference
SACH	Service Advertisement Channel	[22]
SAE	Society of Automotive Engineers	http://www.sae.org/
SAM	Service Advertisement Message	
SAP	Service Access Point	[13]
SCH	Service Channel	[22, 27]
SCHx	Service Channel number x	[27]
SDO	Standards Development Organization	general
SDU	Service Data Unit	[44]
SfCH	Safety Channel	[22]
SNAP	Sub-Network Access Protocol	[44]
SNMP	Simple Network Management Protocol	IETF, [44]
SSAP	Source SAP address	[45]
SSP	Service specific permissions From 802.11:2012 subscription service provider (SSP): An organization (operator) offering connection to network services, perhaps for a fee. From 1609.2 service specific permissions (SSP): A field that encodes permissions relevant to a particular certificate holder.	
Std	Standard	IEEE
TDMC	Time Domain Multiple Channel switching	
To DS	Bit field in the IEEE Std 802.11 MAC header	
TS	Technical Specification	ETSI / ISO
U-NII	Unlicensed National Information Infrastructure	**[57]**

Acronym	Meaning	Reference
US	United States	general
VCI	Virtual Communication Interface	[9]
VSA	Vendor Specific Action	
WAVE	Wireless Access in Vehicular Environments	[49, 53, 54]
WG	Working Group	general
WSA	WAVE Service Advertisement	
WSMP	WAVE Short Message Protocol	
XID	eXchange IDentification IEEE Std 802.2 LLC service	[45]

2.2 Glossary

Linkability: the ability of a system to support linking.

Linking: the act of determining that the same device caused certain specific operations.

Pseudonymity: service that enforces a pseudonym such that unauthorized users and/or subjects are unable to determine the identity of a user bound to a resource or service whilst the user can still be accountable for use.

Pseudonym: data used to replace identity revealing information.

Reversible pseudonymity: service that allows an authorized entity to determine the real identity of a user from knowledge of the pseudonym.

Service specific permissions: Permission applied to a specific service as part of the access control mechanism. Also, a specific means of encoding those permissions specified in IEEE 1609.2.

Unlinkability: the property of being unable to determine whether the same device caused certain specific operations.

3 Introduction

3.1 General

This document describes a set of interoperability tests, the results of which are intended to give confidence that ITS stations interoperate co-operatively and securely. It should be read in conjunction with HTG1-1 [67].

NOTE: An ITS-S that passes all the tests identified in this document and in HTG3-2 [71] cannot be guaranteed to work in all possible ITS scenarios, but the scope of the tests selected are considered sufficient to give a high assurance of operation in practical application but cannot account for all the variables in deployment that may adversely impact operation.

Interoperability testing is the activity of proving that end-to-end functionality between (at least) two communicating systems is as required by those systems' base standards. The goal of interoperability tests is to verify that devices claiming to be able to work together and also claiming to provide the functionalities described by the mechanisms and protocols published by the standards bodies contributing to co-operative ITS are truly able to interoperate with each other. ETSI EG 202 237 [65] describes a generic approach to interoperability testing where the important factors that characterise interoperability testing are:

- The Equipment Under Test (EUT) and the Qualified Equipment (QE) together define the boundaries for testing.
- The EUT and QE come from different suppliers (or, at least, different product lines).
- Interoperability tests are performed at interfaces that offer only normal user control and observation.
- Interoperability tests are based on functionality as experienced by a user (i.e., they are not specified at the protocol level). In this context a user may be human or a software application.
- The tests are performed and observed at functional interfaces such as Man-Machine Interfaces (MMIs), protocol service interfaces and Application Programming Interfaces (APIs).

The fact that interoperability tests are performed at the end points and at functional interfaces means that interoperability test cases can only specify functional behaviour. They cannot explicitly cause or test protocol error behaviour.

The components and the steps for developing an interoperability test specification are:

1. Specify the Abstract Architecture.
2. Prepare draft Interoperable Functions Statement (IFS).
3. Specify Test Suite Structure (TSS).

4. Write Test Purposes (TP) and place them into the TSS.
5. Write Test Cases and place them into a Test Suite according to the TSS.
6. Validate Test Cases.
7. Finalize IFS.

The scope of the present document is to fully specify steps 2 through to 5 of the above list. The abstract architecture of co-operative ITS for US-EU harmonization is described in HTG1&3-1 Overview of Harmonization Task Groups 1 & 3 [66].

For the purposes of security interoperability testing, the IFS shall be the PICS defined for the application of IEEE 1609.2 to secure message transfer and management of certificates defined in ETSI TS 103 097-1.

NOTE: The set of test specifications for ETSI's mapping of IEEE 1609.2 are in the ETSI work programme as a priority set of items due for completion in Q1-2013 (references [8,9,10,11]).

The *interoperability verification* uses two communication nodes EUT-A and EUT-B. An elementary stimulus evokes certain behaviour in EUT-A involving communication to EUT-B with a possible response from EUT-B. Only 'legal' stimuli are used and sample data is communicated, while communication is not interfered with. Details are described for each of the basic function tests. Figure 1 shows a typical test setup for an interoperability test.

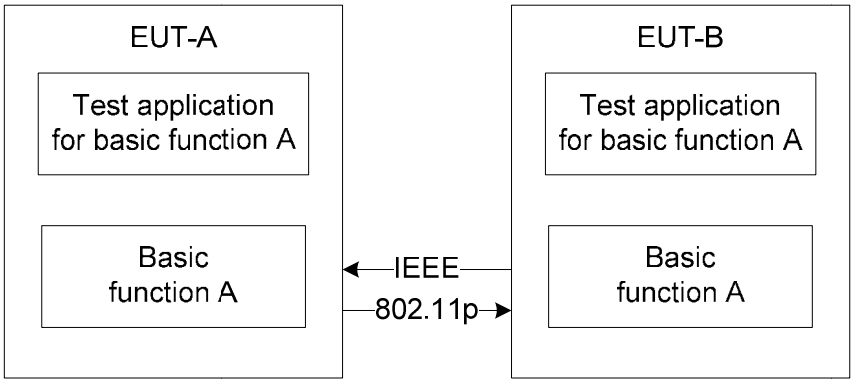

Figure 1: Interoperability test

Source: EU-U.S. ITS Task Force, November 2012.

The *formal compliance* test seeks to cover full functionality, boundary data and 'illegal' stimuli and data. The test setup involves a Test System that can provide all possible stimuli and responses to the EUT. A full analysis of stimuli, responses and data must be done and transcribed into a formal compliance test-set. The current set of documents does not specify or describe formal compliance tests.

3.1.1 Communication scenarios

HTG1&3-1, Overview of Harmonization Task Groups 1 & 3 [66] describes six communication scenarios that are representative of the communication needs within the scope of the HTG. The following table

has as rows the communication scenarios and as columns the associated basic communication functions.

One scenario generally uses more than one basic function with its associated test.

Table 1: Communication scenarios covered by test functions

Communication Scenario	CAM/BSM Broadcast	Service advertisement without application session	Application session (non-IP)	Service advertisement with application session	IPv6 Router Advertisement	Application session (IPv6)	Border Crossing – new regulatory domain
1. Vehicle-Originating Broadcast	Yes	Yes					Yes
2. Infrastructure-Originating Broadcast	Yes	Yes					Yes
3. Infrastructure – Vehicle Unicast			Yes	Yes			
4. Local time-critical session		Yes	Yes	Yes			
5. Local non-time-critical session		Yes		Yes	Yes	Yes	
6. Multi-RSU session		Yes				Yes	

Test descriptions for the communication scenarios are outside of the scope of this document, but can be simple combinations of the basic function tests.

3.1.2 Complete application scenarios

Many real-life applications need no more than the presented communication scenarios. More complex applications, however, combine different scenarios in the course of a 'cooperative transaction', potentially using many basic communication and security functions in a complex chain.

Test descriptions for mature safety application scenarios are outside of the scope of this document. However, one example will be given on the level of a complex application with safety aspects.

3.2 Disclosure of test results

Tests are executed to improve the products of all participants. Uncontrolled disclosure of test results might harm the business of the companies involved. Therefore it is advised that all partners (companies) in the test sign an NDA and lodge it with the organizer, the purpose of which is to ensure that each partner may only disclose their own results without revealing any results from any other explicitly or implicitly identified partner. The organizer may publish information about the overall results of the test only provided it is with the consent of all partners and if anonymity with regard to specific results is afforded to all of the partners.

4 Interoperability tests

4.1 Structure of this section

As previously noted interoperability testing is the activity of proving that end-to-end functionality between (at least) two communicating systems as required by those systems' base standards and, for the present document, the agreed functionality for EU-US harmonization.

The entry for each testable topic has the following structure:

- The name of the test including a general description (test purpose).
- A detailed test description.
- An outline of how the test will be carried out. This is currently not a full or formal specification.

At the end of the section, a table shows how the test cases here cover the use cases and the interoperability topics in the status document.

4.2 Test Descriptions

The test session will be executed between devices from different vendors. One device shall be initially selected as a Qualified Equipment (QE). Each device can play different roles (sender, receiver) during the test sessions. The information about the test configuration and the roles required are indicated in the test descriptions below.

For each test the following test actions are considered during the test execution:

- **S:** a **stimulus action** corresponds to an event that enforces a EUT to proceed with a specific protocol action, like for instance sending a message (*stimulus in TPLan terminology, introduced by keyword "when"*).
- **V:** a **verify action** consists of verifying that the EUT behaves according to the expected behavior (for instance the EUT behavior shows that it receives the expected message) (*response in TPLan terminology, introduced by keyword "then"*).
- **M:** a **configure action** corresponds to an action to modify the EUT configuration (*precondition in TPLan terminology, introduced by keyword "with"*).
- **C:** a **check action** ensures the receipt of protocol messages on reference points, with valid content (*response in TPLan terminology, introduced by keyword "then"*).

It is recommended by ETSI's Making Better Standards website to use TPLan to specify test purposes. The structure of a TPLan statement is given below.

```
with { <<preconditions>> }
 ensure that {
  when { <<stimuli>> }
  then { <<response>> }
```

4.3 Test Tools

For interoperability testing the observation is from the "production" equipment treated through its external interfaces only. Whilst additional information may be available for analysis by the use of specialized tools, the goal of interoperability testing is not to debug applications but to verify that the EUT performs as expected (as written in the Test Purpose) against a QE.

The HTG1 tests described below are concerned only with the security functions associated to the use of IEEE 1609.2 certificates and the processing of messages.

The following test purposes are described:

- Signature processing for co-operative awareness
    - **Signature processing for message transmission**. The ITS stations in both the QE and the EUT are configured to sign a standard ITS Co-operative awareness message (CAM) on transmission and to validate the signature on receipt.
    - **Signature processing for message receipt – positive**. This application will send out service advertisements (FSAP/WSA) with a predefined ITS-AID plus optional port number/PSID, optional data body part and optional service channel information.
    - **Signature processing for message receipt – negative Service advertisement listener** (potential service user). This application will listen for service advertisements at a known ITS-AID/PSID. Each received advertisement is logged with sender address information (if applicable) and content (the advertised service and its parameters).
- **Security management**. This application interacts with the SCMS to obtain up-to-date security management information.

4.4 Configuration for security testing

The interoperability tests cover positive tests (EUTs correctly accepting valid messages) and negative tests (EUTs correctly rejecting messages that are invalid or that cannot be confirmed to be valid).

4.5 Secure Credential Management System (SCMS) for test environment

The interoperability tests require access to an SCMS. The SCMS may be established for the test only (i.e., to prevent interference with active key spaces). The SCMS must be capable of maintaining at least two distinct root certificates, along with the CA hierarchies that flow from each root cert.

5 Interoperability Test Cases

5.1 Confirmation of maintenance of operation with security applied

In the first case the interoperability, test cases described in HTG3-2 Testing for ITS Communications will be re-tested with the security processing enabled. The pass/fail criteria shall be the same as described in HTG3-2.

- CAM/BSM Broadcast
    - This test verifies that CAM/BSM messages can be sent to other systems via all available protocol stacks.
- Service advertisement without application session
    - This test verifies that WSA messages/SAMs can be sent and received via all available non-IP protocol stacks.
- Application session (non-IP)
    - This test verifies that application unicast messages can be exchanged between two systems via all available protocol stacks.
- Service advertisement with application session
    - This test verifies that WSA messages/SAMs can be sent and received, and that a session with the advertised service can be established.
- IPv6 Router Advertisement
    - This test verifies the IEEE 1609 IPv6 WSA Router Advertisement.
- Application session (IPv6)
    - This test verifies the use of TCP/IPv6 for application-to-application communication.
- Border Crossing – new regulatory domain
    - This test is used to verify that the communication parameters (channel, bandwidth) are changed correctly when crossing a border.

5.2 Confirmation of message rejection with invalid security credentials applied

In this case, the interoperability test cases described in HTG3-2 will be re-tested with the security processing enabled but with the credentials invalid. In this case, all of the tests should fail. The following specific cases of credentials shall be applied:

- Message verification failure – no shared root certificate
- Message verification failure – certificate revoked
- Message verification failure – certificate valid only in the future (wrt EUT)

5.3 Validation of security management messages (PKI interoperability tests)

Not applicable at the present time pending delivery of protocol.

6 Example scenario for an on-street demonstration

Extends the example given in HTG3-2 with security processing enabled. Pass/fail criteria as for HTG3-2.

U.S. Department of Transportation
ITS Joint Program Office-HOIT
1200 Ney Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487
www.its.dot.gov

FHWA-JPO-13-078

U.S. Department of Transportation