EU-US Standards Harmonization Task Group Report: Status of ITS Security Standards

Document HTG1-1

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

November 12, 2012

Publication # FHWA-JPO-13-077

European Commission

U.S. Department of Transportation

EU★S 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-13-077		

4. Title and Subtitle	5. Report Date
EU-US Standards Harmonization Task Group Report: Status of ITS Security Standards (Document HTG1-1)	November 12, 2012
	6. Performing Organization Code

7. Author(s)	8. Performing Organization Report No.
Scott Cadzow, Wolfgang Hoefs, Frank Kargl, Richard Roy, Steve Sill, 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 which includes this report. This report summarizes the analysis conducted to identify the necessary subset of available standards to provide assurance of interoperable security measures in Cooperative ITS (C-ITS). Its two primary areas of focus are 1) cooperative ITS using the 5.9 GHz access technology based on IEEE Std 802.11 and 2) to identify areas where implementations of the protocol stack (defined in ISO Technical Committee (TC) 204, ETSI TC ITS, IEEE Working Group 1609 and SAE International) will not be interoperable, because the specification of technical features in standards from various Standards Development Organizations is different or incomplete.

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

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
		86	

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 HTG3. This list does not indicate any preference for an SDO.

References without a date point to documents which are currently under development and thus 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 14906 Road transport and traffic telematics—Electronic fee collection—Application interface definition for dedicated short-range communication

[2] ISO 15628 Road transport and traffic telematics—Dedicated short range communication (DSRC)—DSRC application layer.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[21] 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

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

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

1.2 CEN

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

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

1.3 ETSI

[26] ETSI TS 102 636-x, Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking
Part 1: Requirements (2010-03)
Part 2: Scenarios (2010-03)
Part 3: Network architecture (2010-03)
Part 4: Geographical addressing and forwarding for point-to-point and point-to-multipoint communications

- Sub-part 1: Media-Independent Functionality (2011-06)
- Sub-part 2: Media dependent functionalities for ITS-G5A media (draft)
Part 5: Transport Protocols; Sub-part 1: Basic Transport Protocol (2011-02)
Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols (2011-03)

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

[28] ETSI TS 102 637-3 V1.1.1 (2010-09), Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 3: Specifications of Decentralized Environmental Notification Basic Service

[29] ETSI ES 202 663 V1.1.0 (2010-01), 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

[30] ETSI EN 302 665 V1.1.1 (2010-09), Intelligent Transport Systems (ITS); Communications Architecture

[31] ETSI TS 102 687 V1.1.1 (2011-07): Intelligent Transport Systems (ITS); Decentralized Congestion Control Mechanisms for Intelligent Transport Systems operating in the 5 GHz range; Access layer part

[32] ETSI TS 102 724 V1.1.1 (2012-10), Intelligent Transport Systems (ITS); Harmonized Channel Specifications for Intelligent Transport Systems operating in the 5 GHz frequency band, Channel specifications 5 GHz

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

[34] ETSI TS 102 860 V1.1.1 (2011-05), Intelligent Transport Systems (ITS); Classification and management of ITS application objects

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

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

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

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

[39] ETSI EN 302 931 V1.1.1 (2011-07), Intelligent Transport Systems (ITS); Vehicular Communications; Geographical Area Definition

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

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

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

[43] ETSI TR 102 962 V1.1.1 (2012-02). Intelligent Transport Systems (ITS); Framework for Public Mobile Networks in Cooperative ITS (C-ITS)

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

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

1.4 IEEE

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

[47] 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

[48] 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

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

[50] 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

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

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

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

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

[55] 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)

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

1.5 Regulations

[57] 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)

[58] 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

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

[60] 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

[61] 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

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

[63] 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

[64] 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

[65] 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)

[66] 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)

1.7 Other references

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

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

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

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

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

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

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

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

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

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

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

[78] 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

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

[80] 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

[81] 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

[82] 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

[83] 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)

[84] 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

[85] 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

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

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

[88] EU FP7 project PRESERVE (http://www.preserve-project.eu)

[89] Safe and Intelligent Mobility Test Field Deutschland (simTD) (http://www.simtd.org/index.dhtml/135082605e7b5754029u/-/deDE/-/CS/-/#)

[90] United States Department of Transportation, Research and Innovative Technology Administration, Intelligent Transportation Systems Joint Programs Office: *Security Credential Management System Design – Security system design for cooperative vehicle to-vehicle crash avoidance applications using 5.9 GHz Dedicated Short Range Communications (DSRC) wireless communications*. Draft Report—February 29, 2012. Available on request.

[91] Car 2 Car Communications Consortium, *Public Key Infrastructure – Memo*, Internal draft version 1.20, February 2011.

[92] European Commission Joint Research Centre – Digital Tachograph. http://dtc.jrc.ec.europa.eu/index.php

[93] Internet Engineering Task Force, Network Mobility (nemo) Working Group (concluded), http://tools.ietf.org/wg/nemo/

[94] Internet Engineering Task Force, IP Routing for Wireless/Mobile Hosts (mobileip) Working Group (concluded), http://tools.ietf.org/wg/mobileip/

[95] Internet Engineering Task Force, Transport Layer Security (tls) Working Group, http://tools.ietf.org/wg/tls/

2 Glossary/Abbreviations

2.1 Abbreviations

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

Table 1: Acronyms

Acronym	Meaning	Reference
API	Application Programming Interface	[9]
BRAN	Broadband Radio Access Networks	[61]
BSMD	Bounded Secured Managed Domain	[9]
BSS	Basic Service Set	
BTP	Basic Transport Protocol	[26]
CCH	Control Channel	[24, 29]
CEN	Comité Européen de Normalisation	http://www.cen.eu
CI	Communication Interface	[11]
CIP	Communication Interface Parameter	[18]
C-ITS	Cooperative ITS	[9, 21]
CTX	Context message	
DCC	Distributed Congestion Control	[31]
DIS	Draft International Standard	ISO
DSAP	Destination SAP address	[47]
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	[18]
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	[26]
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)	[9]
ITS-AID	ITS Application Identifier	[34]
ITS-S	ITS Station	[9]
LLC	Logical Link Control	[46]
MAC	Medium Access Control	[46]
MIB	Management Information Base	[46]
OSI	Open Systems Interconnection	[22]
PDU	Protocol Data Unit	[46]
PSID	Provider Service Identifier	
SACH	Service Advertisement Channel	[24]

Acronym	Meaning	Reference
SAE	Society of Automotive Engineers	http://www.sae.org/
SAM	Service Advertisement Message	
SAP	Service Access Point	[15]
SCH	Service Channel	[24, 29]
SCHx	Service Channel number x	[29]
SDO	Standards Development Organization	general
SDU	Service Data Unit	[46]
SfCH	Safety Channel	[24]
SNAP	Sub-Network Access Protocol	[46]
SNMP	Simple Network Management Protocol	IETF, [46]
SSAP	Source SAP address	[47]
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	**[59]**
US	United States	general
VCI	Virtual Communication Interface	[11]

Acronym	Meaning	Reference
VSA	Vendor Specific Action	
WAVE	Wireless Access in Vehicular Environments	[51, 55, 56]
WG	Working Group	general
WSA	WAVE Service Advertisement	
WSMP	WAVE Short Message Protocol	
XID	eXchange IDentification IEEE Std 802.2 LLC service	[47]

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 provides an analysis to identify the necessary subset of available standards to give an assurance of interoperable security measures in Cooperative ITS (C-ITS).

The document has two particular areas of focus.

1) The technical scope is focused on cooperative ITS using the 5.9 GHz access technology based on IEEE Std 802.11 operating outside the context of a Basic Service Set (BSS),[1] where protocol stacks and applications are defined in ISO TC204, ETSI TC ITS, IEEE WG 1609 and SAE. Applications defined outside the identified working groups are out of scope.

2) The emphasis of the document is to identify areas where implementations of the protocol stack will not be interoperable, because the specification of technical features in standards from SDOs is different.

Additionally, to provide focus, the areas of comparison between the standards are motivated by particular use cases. These use cases are defined in separate document HTG1&3-1 *Overview of Harmonization Task Groups 1&3* [67].

3.2 Structure of the document

Sections 5-16 of this document present topics relevant to interoperability of equipment intended for usage in the US and the EU. There is one section for each of the use cases given in [1], and additional sections to address system-level security issues.

Each section on a specific use case begins with a table identifying the security services needed for that use case. The subsequent subsections within a section discuss interoperability issues under a number of section-specific topic headings. For each topic, interoperability is discussed in terms of:

- Technical interoperability (i.e., the ability of devices following one set of standards to correctly process datagrams created by devices following a different set of standards).
- Consistency of application behavior between implementations (i.e., the ability to ensure that two different implementations, receiving the same set of input datagrams under the same circumstances, behave identically).
- Consistency of user experience (i.e., are there any ways in which the configuration of the service may give a false impression of the security or privacy of the ITS services, such that a device may transmit similar messages in different locations but the behavior of the receiving entity may be

[1] This functionality within the 802.11 standard was previously contained in IEEE Std 802.11p.

quite different. For example, law enforcement penalties may be issued in one region and not another).

The hierarchy of interoperability requirements is such that technical interoperability is a pre-requisite for consistency of behavior between implementations which is a pre-requisite for consistency of user experience. Full interoperability is only achieved when all conditions are fulfilled.

NOTE: This hierarchy may be applied in the communications domain as well as in the security domain.

The detailed discussion of the non-interoperable issue distinguishes "Incompleteness (I)" and "Divergence (D)". Each detail is identified by a key character (I or D) and a sequential number. The concatenation of the topic identifier and the identifier for a detail of a topic will be used in the other documents from HTG1, which will identify short-term approaches to resolve interoperability issues in each area for the interoperability test (HTG1-2), or a list of options for long-term resolution of the interoperability issues in each area, to be considered by the respective SDOs (HTG1-3).

4 Vehicle-Originating Broadcast (VOB)

4.1 Communications security services: summary

The originating vehicle broadcasts information about its movements and safety-related attributes frequently to make sure that this information is available to other vehicles so that each receiving vehicle can identify potentially hazardous situations rising from the behavior of the transmitting vehicle. This most commonly involves broadcast of Cooperative Awareness or Basic Safety Messages. Communications characteristics of these applications are described in HTG1&3-1 *Overview of Harmonization Task Groups 1&3* [67].

For vehicle-originating broadcast messages in support of V2V safety applications the need for communications security services is as shown in Table 1 (the colour coding of the table shows green where a known interoperability mechanism exists).

Table 1: Security Services requirements analysis for Vehicle Originating Broadcast

Security Service	Required	Rationale	Interoperability mechanism	Known Interoperability Mechanism Exists
Confidentiality	No	Messages are broadcast for giving information to all (all informed broadcast)	n/a	No
Authenticity	Yes	Messages must be authenticated to prevent injection of false messages into the system.	Message signature	Yes
Integrity	Yes	In order to prevent manipulation of messages between transmit and receive	Message signature	Yes
Authorization and privilege classes	Yes	Requirement to specify different privilege classes, for example to distinguish emergency vehicles from general vehicles.	PSID/ITS-AID and Service Specific Permissions within certificate accompanying message signature	Yes

Security Service	Required	Rationale	Interoperability mechanism	Known Interoperability Mechanism Exists
Non-repudiation of origin	Yes	Where a received message invokes actions on the receiver it may be necessary to show that the behavior was in response to a specific transmitted message. Similarly messages may be received that indicate misbehaviour of the transmitting vehicle or its equipment that will give rise to a misbehaviour report. Non-repudiation of origin ensures that the originator of information cannot successfully deny having sent the information.	Message signature. For some services (e.g., misbehavior detection), this is required but should not impose a requirement to reveal the identity of the vehicle user.	Yes

Security Service	Required	Rationale	Interoperability mechanism	Known Interoperability Mechanism Exists
Non-repudiation of receipt	No	Non-repudiation of receipt is the corollary of non-repudiation of origin and ensures that the recipient of information cannot successfully deny receiving the information. In an unconfirmed best effort system (e.g., the 5GHz radio link), any message may be lost, and any message received may be audited, but there may be a mismatch in proof of what is transmitted and what is received. No requirement for non-repudiation of receipt has been identified and non-repudiation of receipt cannot be achieved through communications security alone	n/a	No
Anti-replay	Yes	Replay may or may not be an attack and the facility to filter out replayed messages is required.	Message signature containing verifiable time variant data (e.g., timestamp of signature generation)	Yes

Security Service	Required	Rationale	Interoperability mechanism	Known Interoperability Mechanism Exists
Plausibility verification	Yes	Plausibility verification is necessary to prevent false warnings from being raised to drivers (e.g., 1 report of sub-zero temperatures against (say) 5 reports of high temperatures within a small time/location window may suggest the sub-zero report is wrong).	IEEE P1609.2 provides some high-level plausibility check mechanisms, but applications need to define the parameters to these mechanisms. Additional, more detailed plausibility checks may also be helpful.	No
Availability		Threats to availability are significant obstacles to the correct functioning of the application.	Not defined	No
Privacy protection measures • Pseudonymity • Unlinkability	Yes	End-users have an expectation of (and a legal right to a certain level of) privacy, though the level of privacy expected and required may differ between an opt-in and a mandatory system, and by local regulations.	Short lifetime signing keys (certificates) Coordinated change of identifiers	Yes
Regulatory compliance	Yes	Data Protection and Privacy (DP&P) compliance is required. Conformance to national and regional exceptions to the DP&P regulations in support of law enforcement.	Privacy protection measures (see above) Reversible pseudonymity	Yes

For each of the interoperability mechanisms identified in the above table, the succeeding sub-clauses further identify the standards and issues regarding EU-US harmonization.

4.2 HTG1-VOB-01: Message Signature (data format / profile)

Vehicle-Originating Broadcast messages are signed. Both ETSI and SAE sign these messages using mechanisms defined in IEEE P1609.2 [16]. The technical basis for achieving interoperability is thus assured, however the issues outlined below do exist and are further explained here.

The following issues affect technical interoperability:

- **HTG1-VOB-01-D-01**: **Inclusion of generation time.**
- **HTG1-VOB-01-D-02: Choice of signature scheme.**
- **HTG1-VOB-01-D-03**: **Cross-layer issues in signing.**
- **HTG1-VOB-01-D-04: Geonetworking.**
- **HTG1-VOB-01-D-06 Modification of signed data format.**
- **HTG1-VOB-01-D-07 Inclusion of geonetworking in security scope.**

The following issues affect consistency of application behavior:

- **HTG1-VOB-01-D-05**: **Message Signature Verification policy.**
- **HTG1-VOB-01-D-08: Certificate Transfer.**

The following issues affect consistency of user experience:

HTG1-VOB-01-I-01: Ability to Assert All permissions.

Divergence:

- **HTG1-VOB-01-D-01**: **Inclusion of generation time**. The BSM from SAE J2735 includes a time value that may roll over in the lifetime of the system, so BSMs use the Generation Time field in the 1609.2 structure thus introducing two different time values in transmitted secured messages. The ETSI CAM includes a time value that was intended to not roll over and thus ETSI has elected not to use the Generation Time field in the 1609.2 structure.

NOTE: The ETSI decision regarding time and the profile of 1609.2 is also in part due to the signature being performed at the CAM level.

- **HTG1-VOB-01-D-02: Choice of signature scheme**. IEEE P1609.2 allows both ECDSA-256 and ECDSA-224, and for ECDSA it allows both implicit and explicit certificates (for ECDSA-224 only explicit certificates are allowed). SAE J2735 uses ECDSA-256 with implicit certificates. ETSI uses

ECDSA-224 with explicit certificates. Since in the unconnected context of VOB there is no means for mobile devices to negotiate the signing mechanism in advance, receivers that are not able to support verification of all mechanisms that signers may use will be unable to verify some messages.

NOTE:
The use of implicit certificates is subject to IPR owned by Certicom, currently a subsidiary of Research in Motion. Certicom has provided a letter of assurance regarding IPR licensing for use of the implicit certificate mechanisms in 1609.2 that may be considered as compliant to the FRAND conditions of the primary SDOs involved in the EU-US harmonization task force. This is not a legally binding view and would need to be evaluated by a lawyer against current IPR law and the FRAND conditions set by the SDOs.

- **HTG1-VOB-01-D-03**: **Cross-layer issues in signing**.

  Background: There has not been agreement regarding where, in the ITS protocol stack, message signature processing should be applied. There is a general assumption in the wider security field that a signature is applied at the point where the "document" is considered complete. In a communications protocol stack however this completeness may be asserted at multiple points[2]. In a single-hop transaction from a monolithic (single application) device it can be argued that the "document" is completed at the network layer and that a signature at that point is correct. However if two or more applications, possibly on different processors, use the same communications media, then the "document" is completed by the application and a single signature at the network layer does not give the same degree of risk assurance as discrete signatures at the application layer. Additionally, if an application may use more than one communications medium and if security services are provided below the application/facilities layer in the protocol stack, the application's communications may end up with different security properties depending on the network stack used. (See 13.1 for further discussion.)

  For reasons of performance and overall stack integrity, the following requirements are broadly agreed upon:

  - There should only be one signature applied to a packet which should capture all relevant elements of a packet that could cause harm to ITS if modifications by an attacker would go unnoticed (i.e., prevention of manipulation attacks by message integrity proof).

[2]In the 7 layer OSI model each layer terminates with its peer and each layer is considered independent (i.e., cannot make assumptions on the behaviour of adjacent layers). Some communications models "bundle" layers taking account of the overall implementation and are considered as monolithic across those bundled layers. A true OSI model, however, cannot bundle layers and thus has to treat each layer and instantiation of each layer as independent.

- The solution needs to be suitable for multiple types of devices: Devices without facilities layer, different radio interfaces, and devices with multiple physical components, one communication router and one or more facilities/applications unit.

Current practice and potential divergence issue: ETSI signs at the facilities layer, SAE signs essentially at the application layer. If the facilities layer adds no additional fields to the datagram, the two approaches are consistent; if the facilities layer adds or modifies fields, the two approaches are inconsistent.

Some European field trials and research projects (for example [88, 89]) have implemented signing at the network layer to protect the geonetworking headers. If these implementations are propagated through to ETSI standards, those standards will be incompatible with the US approach. PRESERVE technical report 3 [88] discusses the pros and cons of different placement options in the communication stack and recommends signing at the network layer, based on the assumption that geonetworking takes place at the network layer. See [74] for further discussion.

- **HTG1-VOB-01-D-04: Geonetworking**: ETSI includes additional network headers for geo-networking. This introduces additional security considerations that do not exist in other domains not using geo-networking. For example, since the originator of a message can specify the area where a message is sent and how long the message stays alive, the ability to send a message to a particular area of a particular size and to keep it alive for a particular time must be properly authorised. This is closely related to HTG1-VOB-01-D-03 "Cross-layer issues in signing." There are also additional concerns related to privacy: see 14.3. A full TVRA for geonetworking has not been carried out.

  HTG1-VOB-01-D-05: Message Signature Verification policy: A signed message should have its signature verified; however verification is costly in time and performance (processor cycles, system memory, etc.), so if not all incoming messages need to be verified, the cost of the device can be kept down by selecting which messages to verify. However, there need to be minimum performance requirements for verification of messages to ensure that all messages are verified if they actually do require verification (for example, messages that result in an alert being raised to the driver). Additionally, since verification takes time, implementations should ensure they are able to complete the processing in a time appropriate to the application. ETSI and CAMP/SAE have different verification policies (the former recommends to verify all messages, the latter to only verify those that raise alerts).

- **HTG1-VOB-01-D-06 Modification of signed data format:** ETSI has an open work item (reference DTS 103 097) to modify the data structure of IEEE P1609.2 that may result in divergence.

- **HTG1-VOB-01-D-07 Certificate transfer:** IEEE P1609.2 allows a signed datagram to explicitly contain the signer's certificate, or to contain a reference to the certificate. Different implementations may select different policies to achieve the necessary optimization of system resources, leading to divergence of system behavior irrespective of conformance to the same base standard.

Incompleteness:

- **HTG1-VOB-01-I-01 Ability to assert all permissions**: BSM / CAM allow an ITS-S to make multiple assertions in a single message (e.g., vehicle speed and lightbar status). The general model for multiple assertions is that each assertion may be validated by a different authority and may be valid in a different set of conditions. For example, the right of an ITS-S to assert that it has a lightbar may be authorized by an emergency services authority that may apply geographical and time constraints on the validity of the assertion, whereas the right to assert speed ITS-S may be authorized by the vehicle manufacturer. It is therefore conceivable that a sender may need multiple different proofs of authorization (i.e., multiple certificates) to make all the assertions within a single message. Care must be taken to ensure that necessary assertions can be made without causing complexity or channel congestion. For example:
    - The message sets could be defined so that a single legal authority will always be able to grant authorization for all possible messages. It is not clear that this is possible for message designers to predict in advance.
    - All legal authorities could delegate their authorization privileges to a single CA, so that the CA has to check with multiple authorities before issuing a certificate but receivers can trust a single certificate. This may be the most practical.
    - Message sets could be carefully designed so that there is as little redundancy as possible between messages that one authority may authorize and messages that a different authority may authorize.

4.3 HTG1-VOB-02: Pseudonymity service

The pseudonymity service has a number of aspects.

- V2V safety messages are signed using pseudonymous certificates (i.e., the certificate and the message contents should not be directly linked to a specific user) whose time in use is short and where pseudonyms are changed frequently such that a single pseudonym is not exposed for a sufficient period to reveal true identity information.
- The pseudonymity service modifies all identifying information in the protocol stack that is exposed over an open interface (i.e., all fields that are considered mutable and exposed are modified at the same time to minimize risks to privacy through linking of data). In practice it is recognized that this may not be possible. If a vehicle is in a state where there is heightened risk to neighboring devices (known as an alert state), and if while in an alert state it changes its pseudonym, this may impact the ability of neighboring devices to maintain a consistent model of the ongoing incident (because they temporarily lose track of the vehicle). The system should be designed to as to minimize or eliminate the likelihood of pseudonym change in an alert state.

In some instances, subject to local regulation, the pseudonym service may have to be suspended or its effects made reversible. US-EU harmonization in this area will depend on the degree to which harmonization of regulation is achieved. It is expected that the SDOs will continue to work with the regulatory authorities in developing standards that achieve any such requirements in an open and flexible manner.

Additional considerations for privacy, pseudonymity and unlinkability are discussed in 14.3.

The pseudonym service uses the message signature capability of IEEE P1609.2, thus the technical root for achieving interoperability is assured; however the issues outlined below do exist.

The following issues affect technical interoperability:

- **HTG1-VOB-02-D-1**: **Reversible pseudonymity**
- **HTG1-VOB-02-D-1**: **Synchronization of identifier changes**

The following issues affect consistency of application behavior:

- **HTG1-VOB-02-D-2: Pseudonym change interval and algorithm**
- **HTG1-VOB-02-D-3: Alert state**

Divergence:

- **None**

Incompleteness:

- **HTG1-VOB-02-I-1 Reversible pseudonymity**: There is no standard or proposed standard certificate format that allows for reversible pseudonymity. Certificate formats that allow reversible pseudonymity have been proposed in research projects and used in field tests as follows:
    - The US Safety Pilot security design, based on [90], specifies a format for reversible pseudonymity, but this is not yet standardized.
    - C2C-CC specifies an approach for pseudonymity in [91]. This document is not publicly available, but has been provided to ETSI and some other organizations/projects for review and comments. C2C-CC suggests that this architecture is considered in ETSI standardization.
    - PRESERVE bases its pseudonym architecture on the basic systems that come from SeVeCom and PRECIOSA and that also influenced the C2C-CC PKI memo.
- **HTG1-VOB-02-I-2 pseudonym change interval and algorithm**: No standards or minimum security requirements exist. The rationale for changing the set of identity information in the

transmitted stack often during any ITS-S movement to minimize linkability and PII exposure is well known but there is no standardized guidance on the frequency at which this takes place. There is an impact on the implementation as this affects local storage and processing requirements.

- **HTG1-VOB-02-I-3 alert state**: See discussion of alert state in the introductory text of this section. There is no agreed definition of the alert state. If the pseudonymity service is to be suspended, the means by which the decision is made and the pseudonymity service subsequently re-instated should be defined.

- **HTG1-VOB-02-I-4 synchronization of identifier changes**: There is no standard in the IEEE 1609 series that defines a pseudonymity service; there are primitives that allow signing certificate change and MAC address change but no mechanism that enforces making these changes simultaneously. ETSI has ongoing work items [SN-SAP, SF-SAP] that start to define a pseudonymity service with simultaneous changes.

4.4 HTG1-VOB-03: Permissions encoding within signed message

Permissions are one element of Role Based Access Control within ITS (as distinct from identity based access control). Role Based Access Control is able to reinforce the privacy model offered by pseudonymity and unlinkability services. There are a large number of system security issues as each permission may be granted by a distinct authority (or chain of authorities). Permission may be linked to other elements including time and location.

The IEEE 1609.2 certificate format allows permissions to be specified by a combination of PSID and Service Specific Permissions. Service Specific Permissions (SSP) are hierarchical within the namespace of the PSID and specify permissions with more granularity than the PSID alone. For example, the SSP for a cooperative awareness device might specify the level of physical security a device provides, or whether a device is allowed to claim that it has a light bar activated.

All issues within this subsection affect technical interoperability.

Divergence:

- **HTG1-VOB-03-D-1: Geographic region encoding**: Where SSP is given within a specific geographic context the means by which IEEE P1609.2 allows geographic region encoding as circular, rectangular, polygonal, or NULL is not consistent with ETSI who have additionally allowed geographic region encoding by an identifier [35]. This identifier would not be accepted by a pure US implementation. Note however that ETSI has not yet fully specified the geographic region identifiers.

- **HTG1-VOB-03-D-2: Permissions encoding and PSID value**: IEEE P1609.2 encodes permissions as PSID. ETSI encodes permissions as either ITS-AID or port number encoded as an ITS-AID. For cooperative awareness, SAE uses PSID 0x20. ETSI intends to authorize the CAM message with a

port number encoded as an ITS-AID, but this port number has not yet been defined and it is possible that ETSI will instead use an ITS-AID. A US CAM verifier would not currently accept a certificate with a PSID other than 0x20; ETSI does not currently intend to use PSID 0x20. This is further complicated by the use of message set IDs, ITS-AIDs, and port numbers within the ISO architecture (issues covered by HTG3). There is no generally accepted approach within the ITS communications security community as to how these should be incorporated into a permissions language.

Incompleteness:

- **HTG1-VOB-03-I-1: Service Specific Permissions**: No standard has defined Service Specific Permissions for use with cooperative awareness. It is unclear exactly what permissions are actually conveyed by the CAM ITS-AID or port number, or by PSID 0x20.
- **HTG1-VOB-03-I-2: Additional properties to be encoded within certificate**: As noted in section 15, different platforms may provide different levels of physical security. It may be useful to state the physical security level explicitly in the certificate.

5 Infrastructure-Originating Broadcast (IOB)

Infrastructure-originating broadcasts are used to disseminate data that are relevant to all vehicles in the vicinity of a specific road infrastructure location where an RSU is installed, in support of safety, mobility or sustainability applications.

Communications characteristics of these applications are described in HTG1&3-1 *Overview of Harmonization Task Groups 1&3* [67].

5.1 HTG1-IOB-01: Communications security services

From a security perspective, these should be basically treated like Vehicle-Originating Broadcasts (VOB) discussed in Sec. 4 with a few differences and exceptions that will be discussed next. First, we will review the security services requirements for IOB.

Table 2: Security Services requirements analysis for Infrastructure Originating Broadcast

Security Service	Required	Rationale	Interoperability mechanism	Difference to VOB	Known Interoperability Mechanism Exists
Confidentiality	No	Messages are broadcast for giving information to all (all informed broadcast)	n/a	None	No
Authenticity	Yes	Messages must be authenticated to prevent injection of false messages into the system.	Message signature	None	Yes
Integrity	Yes	In order to prevent manipulation of messages between transmit and receive	Message signature	None	Yes
Authorization and privilege classes	Yes	Requirement to specify different privilege classes, for example to distinguish traffic signs from traffic lights.	Service Specific Permissions within message signature	None, just different permissions	Yes

Security Service	Required	Rationale	Interoperability mechanism	Difference to VOB	Known Interoperability Mechanism Exists
Non-repudiation of origin	Yes	Where a received message invokes actions on the receiver it may be necessary to show that the behavior was in response to a specific transmitted message. Similarly messages may be received that indicate misbehavior of the transmitting vehicle or its equipment that will give rise to a misbehaviour report. Non-repudiation of origin ensures that the originator of information cannot successfully deny having sent the information.	Message signature.	Can be fully implemented without giving consideration to DP&P issues.	Yes
Non-repudiation of receipt	No	Non-repudiation of receipt is the corollary of non-repudiation of origin and ensures that the recipient of information cannot successfully deny receiving the information.	Not defined In an unconfirmed best effort system (e.g., the 5GHz radio link) any message may be lost, any message received may be audited but there may be a mismatch in proof of what is transmitted and what is received.	None	No

Security Service	Required	Rationale	Interoperability mechanism	Difference to VOB	Known Interoperability Mechanism Exists
Anti-replay	Yes	Replay may or may not be an attack and the facility to filter out replayed messages is required.	Message signature containing verifiable time variant data (e.g., timestamp of signature generation)	None	Yes
Plausibility verification	Yes	Plausibility verification is necessary to prevent false warnings from being raised to drivers (e.g., 1 report of sub-zero temperatures against (say) 5 reports of high temperatures within a small time/location window may suggest the sub-zero report is wrong).	Not defined Multiple models for plausibility verification exist in the literature and in some deployed systems but are not standardized.	None	No
Availability		Threats to availability are significant obstacles to the correct functioning of the application.	Not defined	None	No
Privacy protection measures • Pseudonymity • Unlinkability	No	As infrastructure and RSUs are not expected to be linked to persons in any way, IOBs are not expected to carry personal or person-relatable data. Thus privacy protection is not an issue.	Long lifetime signing keys (certificates)	Certificates can be longer lived and can include identifiers. As infrastructure is static, there is also no need for frequent key change.	Yes

Security Service	Required	Rationale	Interoperability mechanism	Difference to VOB	Known Interoperability Mechanism Exists
Regulatory compliance	Yes	While in general, regulatory compliance is needed, DP&P do not apply. However, it should be clearly defined to what extend VOBs and VOU can be logged by infrastructure.		No DP&P compliance required (with the exception of logging)	Yes

5.2 HTG1-IOB-01: Message Signature (data format/profile)

Everything discussed in Sec. 4 fully applies here. To ease design and development of RSUs and message interoperability, IOB and VOB message signatures should be identical in structure and in the processing.

5.3 HTG1-IOB-02: Pseudonymity service

IOB messages are not expected to carry personal or person-relatable data. Thus, data protection and privacy regulations do not apply and applying the pseudonymity service would create extra and unnecessary effort. By enabling roadside infrastructure to use certificates with unique identifiers, we avoid all of the issues in I-HTG1-VOB-02-1 to -4.

However, the following issues do exist:

Divergence:

- **None**

Incompleteness:

- **HTG1-IOB-02-I-1 Revocation vs. short-lived certificates**: to address the issue of misbehaving or malicious RSUs (e.g., due to tampering where key material is extracted from an RSU), there are two principal strategies:
  - RSU certificates are short-lived and need to be reloaded from an authority that refuses issuance in case of misbehavior of that entity. This would require an (at least sporadic) online connection from that RSU.
  - RSU certificates are long-lived and we have an efficient certificate revocation and CRL distribution to ITS-Ss in place.

- **HTG1-IOB-02-I-2 Logging of vehicle-originating messages:** it needs to be defined to what extent and for what retention period RSUs and infrastructure are required and allowed to log incoming vehicle-originating messages. To enforce extensive data logging may endanger privacy as research has shown that vehicles can be tracked through historic records even when the data has been anonymised (e.g., by use of pseudonyms). This is not necessarily an issue for SDOs but for regulators.

5.4 HTG1-IOB-03: Permissions encoding within signed message

While different permissions are required for IOB, the mechanisms for encoding in signed messages should be identical. No new issues arise.

6 Infrastructure-Vehicle Unicast (IVU)

6.1 Background

The infrastructure-vehicle unicast communication scenario involves individual transactions between a vehicle and the infrastructure. Communications characteristics of these applications are described in HTG1&3-1 *Overview of Harmonization Task Groups 1&3* [67].

From a security point of view, there are three possible models:

1) Messages from both nodes are protected using security mechanisms for broadcast.
2) The initial message from the mobile node is protected using security mechanisms for broadcast, subsequent messages are protected using security mechanisms for session.
3) All messages are protected using security mechanisms for sessions with pre-arranged keys.

This section focuses only on the second model. The first is covered in sections 4 and 5 and the third is covered in sections 8 and 9.

6.2 Security services for broadcast followed by unicast

From a security perspective, the non-broadcast nature of IVU creates some changes to security services requirements compared to VOB or IOB.

Table 3: Security Services requirements analysis for Infrastructure-Vehicle Unicast

Security Service	Required	Rationale	Interoperability mechanism	Difference to VOB/IOB	Known Interoperability Mechanism Exists
Confidentiality	Yes	Unicast may contain information that needs to remain confidential.	Not currently standardized	Confidentiality needed here, not needed in VOB/IOB	No
Authenticity	Yes	Messages must be authenticated to prevent injection of false messages into the system.	Message signature	None	Yes

Security Service	Required	Rationale	Interoperability mechanism	Difference to VOB/IOB	Known Interoperability Mechanism Exists
Integrity	Yes	In order to prevent manipulation of messages between transmit and receive, messages must be integrity protected.	Message signature	None	Yes
Authorization and privilege classes	Yes	Requirement to specify different privilege classes, for example to verify authorization for traffic light preemption.	Service Specific Permissions within message signature	None, just different permissions	Yes

Security Service	Required	Rationale	Interoperability mechanism	Difference to VOB/IOB	Known Interoperability Mechanism Exists
Non-repudiation of origin	Yes	Where a received message invokes actions on the receiver it may be necessary to show that the behavior was in response to a specific transmitted message. Similarly messages may be received that indicate misbehaviour of the transmitting vehicle or its equipment that will give rise to a misbehaviour report. Non-repudiation of origin ensures that the originator of information cannot successfully deny having sent the information.	Message signature. For some services (e.g., misbehavior detection), this is required but should not impose a requirement to reveal the identity of the vehicle user. Some other services may require full identification.	One partner (vehicle) requires privacy protection, the other (RSU) not. Depending on the specific service, full authenticati on may be needed.	Yes

Security Service	Required	Rationale	Interoperability mechanism	Difference to VOB/IOB	Known Interoperability Mechanism Exists
Non-repudiation of receipt	No	Non-repudiation of receipt is the corollary of non-repudiation of origin and ensures that the recipient of information cannot successfully deny receiving the information.	Not defined In an unconfirmed best effort system (e.g., the 5GHz radio link) any message may be lost, any message received may be audited but there may be a mismatch in proof of what is transmitted and what is received.	None	No
Anti-replay	Yes	Replay may or not be an attack and the facility to filter out replayed messages is required.	Message signature containing verifiable time variant data (e.g., timestamp of signature generation).	None	Yes

Security Service	Required	Rationale	Interoperability mechanism	Difference to VOB/IOB	Known Interoperability Mechanism Exists
Plausibility verification	Yes	Plausibility verification is necessary to prevent false warnings from being raised to drivers (e.g., one report of sub-zero temperatures against (say) five reports of high temperatures within a small time/location window may suggest the sub-zero report is wrong).	Not defined Multiple models for plausibility verification exist in the literature and in some deployed systems but are not standardized.	None	No
Availability		Threats to availability are significant obstacles to the correct functioning of the application.	Not defined	None	No

Security Service	Required	Rationale	Interoperability mechanism	Difference to VOB/IOB	Known Interoperability Mechanism Exists
Privacy protection measures • Pseudonymity • Unlinkability	Partially	End-users have an expectation of (and a legal right to a certain level of) privacy, though the level of privacy expected and required may differ between an opt-in and a mandatory system, and by local regulations. This is not relevant for the infrastructure side of the communication.	RSU side: Long lifetime signing keys (certificates) Vehicle side: Short lifetime signing keys (certificates) and pseudonymity service.	A mix of VOB and IOB	Yes
Regulatory compliance	Yes	Data Protection and Privacy (DP&P) compliance is required for the vehicle side. Conformance to exceptions to the DP&P regulations.	Privacy protection measures and reversible pseudonymity for the vehicle side.	A mix of VOB and IOB	Yes

6.3 HTG1-IVU-01: Message Signature (data format/profile)

The requirements for this case are the same as for the session cases described in sections 8 and 8.2.

6.4 HTG1-IVU-02: Encryption

Messages after the initiating message may require confidentiality services. IEEE P1609.2 provides a mechanism to support encrypted messages in response to signed broadcast messages.

Incompleteness:

- **HTG1-IVU-02-I-1 Encryption**: 1609.2 may not be appropriate for some applications.

6.5 HTG1-IVU-03: Privacy and maintenance of communications

The vehicle side of the communication will typically require privacy, the RSE side typically will not. Privacy implications are as discussed in section 8.2 and 14.3.

6.6 HTG1-IVU-04: Permissions encoding within signed message

While different permissions are required for IOB, the mechanisms for encoding in signed messages should be identical. No new issues arise.

7 Security Management for VOB and IOB

7.1 Overview

Figure 1 provides an overview of the functional entities involved in managing trusted communications in the ITS setting. These are the entities used for establishing and verifying cryptographic trust of individual messages within the operational system. Entities involved in initializing actors within the system (i.e., determining that instances of applications resident on instances of platforms are eligible for certificates) are illustrated in Figure 3. The entities in Figure 1 reflect the CAMP architecture rather than the C2C/PRESERVE architecture, but the two are very similar. The entities are as follows, listed top to bottom and left to right. Messages across all interfaces except the Misbehavior Authority/Administrative Review interface are within the scope of SDOs.

- Trust management: responsible for managing root certificates on devices. Analogous to the code signing certificates for web browsers that allow root certificates to be added and removed as part of a software update.
- Root CA: CA with a self-signed certificate that must be trusted by out-of-band means (i.e., by approval by a Trust Management entity) that issues certificates for other entities.
- Intermediate CA: A CA that does not have a self-signed certificate and that issues certificates for other entities, including CAs.
- Long-Term CA (LTCA): A CA that issues certificates to end-entities, allowing them to apply for pseudonym certificates. LTCAs may issue certificates for devices, or for instances of applications on those devices.
- Pseudonym CA (PCA): A CA that issues pseudonym certificates to end-entities.
- Request Coordination: An entity that ensures that an end-entity cannot apply for multiple sets of certificates that are valid at the same time and in the same place.
- Registration Authority (RA): The entity that initially approves certificate requests from end-entities and forwards that approval to CAs.
    - NOTE: in the C2C-CC model, the certificate request is approved by the Long-Term CA, which therefore plays two roles: LTCA and RA.
- Linkage Authority (LA): Used to support reversible pseudonymity.
- Gateway: The Internet (or other networking) connection used to provide access from end-entities to the RA. May include anonymous routing capabilities.
- Misbehavior authority: Responsible for assessing misbehavior reports and making an initial determination that a given unit should be revoked.

- Revocation CA: Issues CRLs.
- CRL store: Stores CRLs for pull access
- CRL broadcast: Distributes CRLs via push access.
- Certification Lab: coordinates with LTCA to ensure that only valid devices get long-term certificates. See Figure 3 for more details.
- Administrative Review: A process that can be used to review and potentially provide redress to decisions made by the misbehavior authority.

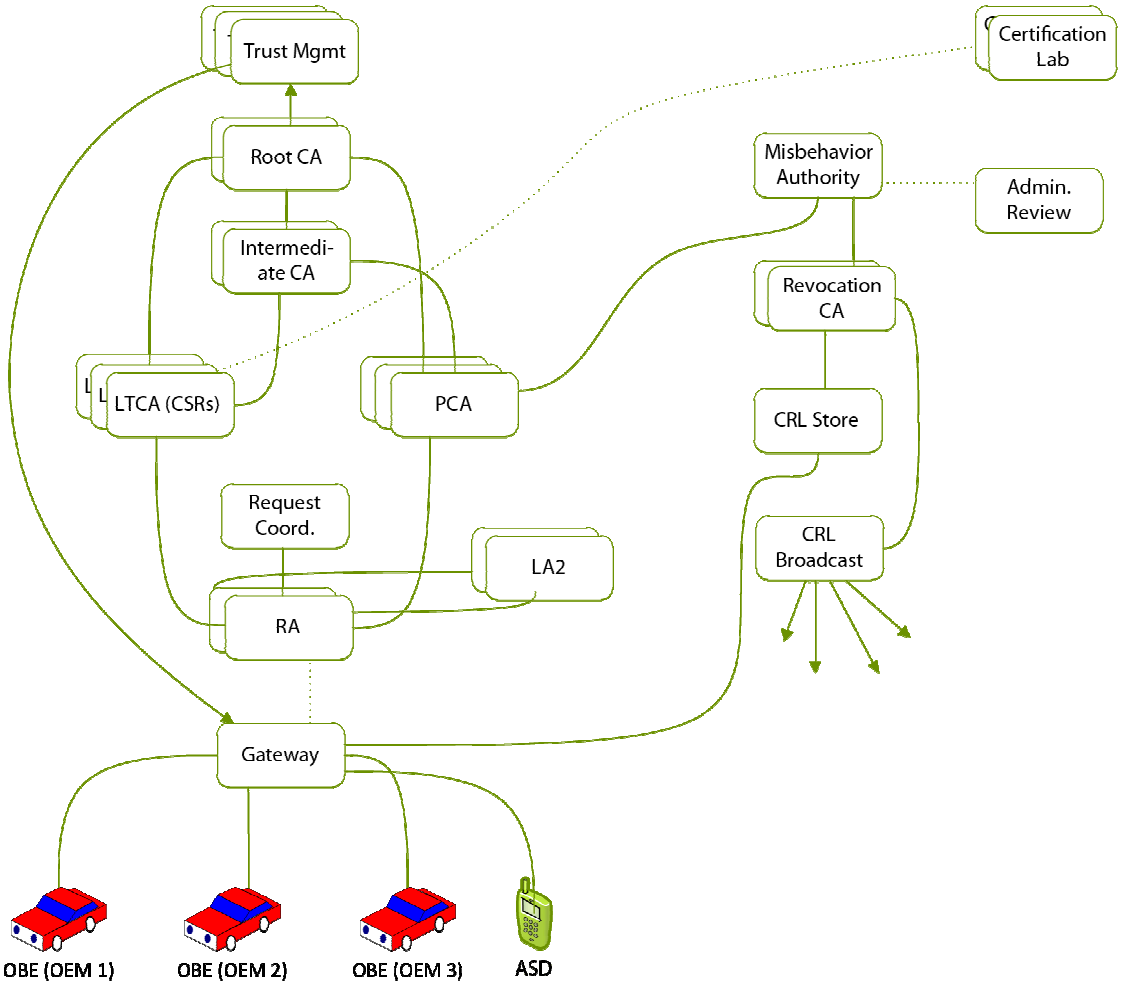


Figure 1: Functional entities for security management for VOB/IOB/IVU

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

7.2 HTG1-SM-01: Adding root certificates

In the absence of a fully defined PKI (see I-HTG1-VOB-01-3 "PKI structure"), it may be assumed that at least one root certificate exists per regulatory domain and that as a result multiple root certificates will

exist. Furthermore, it may be assumed that such domains will change over the lifetime of ITS. Thus if vehicles are to operate in a domain where they are not equipped with the necessary root certificate that is used to validate all other certificates in the domain, a process has to be established that allows the vehicle to install additional root certificates. This is managed by the "Trust Management" functional entity(ies) in Figure 1.

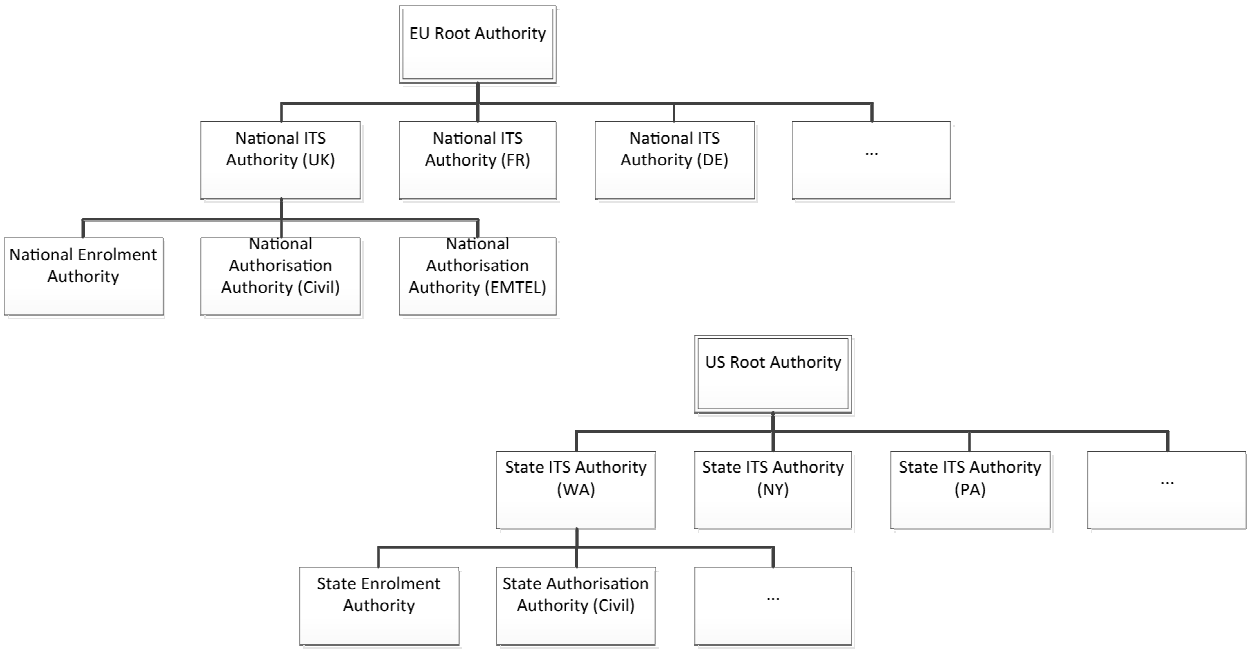


Figure 2: Example of Certificate Authority Hierarchy

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

The example of a CA hierarchy in Figure 2 illustrates some of the issues of managing PKIs for ITS. The example does not claim to be authoritative nor to be the one that will be implemented. However it illustrates the concerns:

- If a certificate is authorized/authenticated at the bottom of the tree, validation is possible at the first shared root.
    - However, if roots are unconnected (in the example this is the case of the US Root Authority and the EU Root Authority), there has to be either a new root added above them, or cross certification of the roots.
- Adding or modifying a CA at any level requires the knowledge of all dependent leaves to be updated.
- Revoking an authority requires dependent leaves to be updated.

As noted in I-VOB-MS-3, there are no standards for PKI management. Whilst ETSI TS 102 940 identifies certificate issuing authorities, it does not define how they fit to a PKI deployment. Existing standards and

standards bodies are not discussing this issue yet in the context of provision of documentary guidance. Consortia documents such as the C2C-CC PKI Memo include a discussion of both the initial bootstrapping of the security system and later additions of root certificates. The same is true for some project documents (e.g., the PRESERVE TR 6 PKI documentation). It specifies a process for "Lifetime and Update of Root CA certificate" which can easily be extended to add new root certificates.

Divergence:

- **None**

Incompleteness:

- **HTG1-SM-01-I-1 Key management:** There are no currently available standards for the long term management and initial distribution of certificates although data structures exist in IEEE P1609.2 and its endorsement in ETSI for protocols to adopt.
- **HTG1-SM-01-I-2 ITS-S initialization**: As noted in "D-HTG1-VOB-01-02: Choice of signature scheme," the choice of signature scheme is not agreed upon, thus the key sizes are also not agreed upon. The ITS-S uses a key-pair that has to be generated by the key owner and the public component certified by an authority in the PKI structure. There are no current standards for this phase although many of the pilot projects in both the EU and the US have arranged for initialization as part of the pilot (although not on the level that a full ITS system would require where 100s of millions of vehicles would need initialization and update).
- **HTG1-SM-01-I-3 PKI structure**: Whilst ETSI TS 102 940 identifies authorities for each of enrolment (identification) and authorization (access control), no standards currently exist for the detail of the PKI structure. Different applications or roles may naturally have different hierarchies, for example, public safety vehicles may naturally be authorized by a very local CA while end-user vehicles with high privacy requirements may naturally be authorized by a single national CA (or one of multiple national CAs, randomly chosen).
- **HTG1-SM-01-I-4 PKI management**: There are no standards for management of the overall PKI system. Thus there is no guidance on introduction of new authorities and the dissemination of root certificates, on signature and certification practices.

NOTE:
A model for PKI management in the Digital Tachograph setting [92] does exist for Europe that describes in detail such practices but translation to a generic co-operative ITS model has not been carried out.

- **HTG1-SM-01-I-5 Specification of protocol for addition of root certificate authorities:** This extends the concerns identified above for the specific functionality to allow introduction of new RCAs.

7.3 HTG1-SM-02: Obtaining new pseudonyms when roaming

As discussed in HTG1-SM-01, for addition of new root certificates similar issues arise for connection to and receiving pseudonym certificates. For maximum privacy by minimum exposure of identifying information, it is advised that all vehicles in a particular area should use the same pseudonym provider, thus requiring the same form of management as for HTG1-SM-01.

ETSI TS 102 941 and TS 102 940 define an architecture and protocol for receiving pseudonym certificates, however they do not address issues of the overall PKI structure. In some of the research and demonstration projects, however, where PKIs have been defined for the demonstration phase, there have been more detailed examinations of this topic with each of CAMP [90], PRESERVE [88], and C2C-CC [91] developing proposals.

Divergence:

- **None**

Incompleteness:

- **HTG1-SM-02-I-1 Specification of protocol for obtaining new pseudonyms when roaming:** This extends the concerns identified in I-HTG1-VOB-MS-1, I-HTG1-VOB-MS-2, I-HTG1-VOB-MS-3 and I-HTG1-VOB-MS-4 for the functionality to allow attachment to local pseudonym authorities.

7.4 HTG1-SM-03: Updating long-term certificates

Where a certificate is issued for a long life (e.g., the enrolment and identity certificates described in TS 102 940 and TS 102 941), it may be necessary to update it in the lifetime of the ITS system. Long-term certificates have certain expiration dates and vehicles would be required to contact the CA via a communication channel (online or even offline) and perform a certificate update before expiration of their old certificates.

Divergence:

- **None**

Incompleteness:

- **HTG1-SM-03-I-1 Specification of protocol for updating long term certificates:** This extends the concerns identified in I-HTG1-VOB-MS-1, I-HTG1-VOB-MS-2, I-HTG1-VOB-MS-3 and I-HTG1-VOB-MS-4 for the functionality to allow attachment to local pseudonym authorities.

7.5 HTG1-SM-04: Resolution of pseudonyms for enforcement purposes

A pseudonym is a temporary alias tied to a single identity, with the aim in ITS of frequent changes of the association of alias to identity. In some cases it may be necessary to resolve the identity associated to a

particular alias using a service of "Reversible Pseudonymity." The instantiation of a reversible pseudonymity service has to be protected from casual use to prevent privacy violations.

Divergence:

- **None**

Incompleteness:

- **HTG1-SM-04-I-1 Specification of protocol for reversible pseudonymity:** This extends the concerns identified in I-HTG1-VOB-MS-1, I-HTG1-VOB-MS-2, I-HTG1-VOB-MS-3 and I-HTG1-VOB-MS-4 for the functionality to allow reversible pseudonymity.
- **HTG1-SM-04-I-2 Specification of conditions for reversible pseudonymity:** Specify the circumstances under which authorities are legally allowed to reverse pseudonymity.
- **HTG1-SM-04-I-3 Protocol to notify ITS-S owner if privacy policy changes:** ITS-S owners may wish to be informed if privacy policy changes, to allow them to adjust their behavior appropriately.

7.6 HTG1-SM-05: Revocation and distribution of revocation lists

The concern here is how nodes will be excluded from the network. The rationale for exclusion includes malicious or misbehaving nodes, and nodes that have reached end of life (e.g., when a vehicle is destroyed its certificates should be revoked). This issue has been subject of long debates in all SDOs, consortia, and research projects with no agreement. Short-lived certs/keys are generally agreed to not be subject to in-network revocation (assumes verification of cert validity on receipt). Instead, short-term pseudonymous certificates with limited lifetime would be issued only to valid and non-revoked vehicles.

If short-term pseudonymous certificates have longer lifetime (or at least an expiration date in the more distant future), there is a consensus that in-network revocation will be needed but there is no agreement yet how this can be achieved technically in an efficient manner.

This issue is mentioned in the risk analysis and in the security architecture in ETSI but no recommendation for a solution has been made so far. It is also addressed by various reports of consortia and research projects which propose specific solutions. A number of solutions do exist but the aim is to ensure that when a single solution is specified the risk of divergence from implementation of the solution is minimized.

Divergence:

- **None**

Incompleteness:

- **HTG1-SM-05-I-1 Specification of certificate revocation information format for reversible pseudonyms:** This extends the concerns identified in the Vehicle Originating Broadcast section for each of I-HTG1-VOB-MS-1, I-HTG1-VOB-MS-2, I-HTG1-VOB-MS-3 and I-HTG1-VOB-MS-4 by noting the lack of standards for the functionality to allow for management of units through revocation of certificates.
- **HTG1-SM-05-I-1 Specification of certificate revocation distribution process:** This extends the concerns identified in I-HTG1-VOB-MS-1, I-HTG1-VOB-MS-2, I-HTG1-VOB-MS-3 and I-HTG1-VOB-MS-4 for the functionality to allow for management of units through revocation of certificates.

7.7 HTG1-SM-06: Revocation, removal, replacement of CAs

Extending from the arguments in HTG1-SM-05 it can be expected that the PKI structure will change during the lifetime of an ITS due to new CAs entering or leaving the market. The ITS needs to be able to cope with this structural change to PKIs by allowing CAs to be revoked, removed, or added to the PKI. This is mostly an issue of disseminating new or updated CA certificates to vehicles or revocation certificates that have been deployed.

Depending on the time-scale by which these changes have to be pushed to all vehicles, this is more or less challenging. The extent of this challenge also depends on the question how regularly vehicles will be able to contact backend systems (e.g., by cellular radios or via RSUs).

Divergence:

- **None**

Incompleteness:

- **HTG1-SM-06-I-1 Specification of certificate revocation process for CAs:** This extends the concerns identified in I-HTG1-VOB-MS-1, I-HTG1-VOB-MS-2, I-HTG1-VOB-MS-3 and I-HTG1-VOB-MS-4 for the functionality to allow for management of units through revocation of certificates of CAs.

7.8 HTG1-SM-07: Misbehavior reporting

The issue of misbehavior detection and reporting is described as essential to provide a solution for in the ETSI TVRA. As an observing vehicle only has access to the pseudonym of the misbehaving vehicle and as the pseudonym may change many times whilst the misbehaving vehicle is active it is not trivial to be able to report to an appropriate authority the detection and identity of a misbehaving vehicle. Thus standardized mechanisms for both detection and reporting need to be made available taking due account of the need to prevent additional attack vectors being created by malicious reporting.

There are three classes of misbehavior detection:

- Local: The ITS-S that receives a message analyses it for internal consistency and consistency with the ITS-S's knowledge of the external world, and rejects messages that are inconsistent.
- Cooperative: The ITS-S exchanges information with nearby ITS-S to determine the trustworthiness of incoming messages. This approach is somewhat vulnerable to Sybil attacks and its widespread use could make Sybil attacks more attractive. Since the ITS-S cooperate to identify and ignore bad actors, each ITS-S could be considered to be exercising local revocation authority.
- Global: Each ITS-S periodically reports back to the Misbehavior Authority with messages chosen according to appropriate criteria—for example, they may be messages that resulted in alerts being raised, and/or they may be randomly selected from received messages, and/or they may be chosen by some other means. The Misbehavior Authority has authority to request that units are revoked. If a unit is revoked, it may appear on a revocation list that is distributed to all relevant ITS-S, and/or the revocation may be notified to CAs who refuse new pseudonyms to the revoked unit.

Cooperative and Global misbehavior detection affects technical interoperability as communicating entities must use an agreed upon technique.

All three issues may affect consistency of application behavior between implementations.

The issue could affect consistency of user experience between jurisdictions if different jurisdictions (a) have different criteria for global revocation and/or (b) restrict the use of cooperative misbehavior detection by groups of ITS-S, for example, due to concerns about privately held ITS-S taking the decision to exclude another ITS-S from some part of the system.

Divergence:

- **None**

Incompleteness:

- **HTG1-SM-07-I-1 Specification of misbehavior detection algorithm:** It is essential (as identified by ETSI's TVRA) to be able to detect misbehavior using a common algorithm (i.e., such that misinterpretation of behavior does not occur).
- **HTG1-SM-07-I-2 Specification of global misbehavior reporting protocol:** Once detected it is essential to have a harmonized and standardized means of reporting misbehavior to an authorized entity and defining the process of resolving the misbehavior in the network (see revocation).
- **HTG1-SM-07-I-3 Specification of cooperative misbehavior reporting protocol:** As above, it is essential to have a harmonized and standardized means of reporting misbehavior to a

cooperative system and defining the process of resolving the misbehavior in the network (see revocation).

- **HTG1-SM-07-I-4 Criteria for revocation:** If different jurisdictions have different criteria for revocation, it will impact consistency of user experience.

7.9 HTG1-SM-08: Bootstrap

This is closely related to "I-HTG1-VOB-01-2 ITS-S initialization" but extends to all elements of ITS. During the production process of any ITS component initial key material, credentials and root certificates need to be installed. This bootstrapping process needs to happen in a secure and tamper-resistant way as otherwise all later security mechanisms risk failure. Whilst no standards for generic co-operative ITS exist there are similar processes used for digital tachographs that may be considered as the basis of the bootstrap mechanism. See sections 14.1, 15.1 for further discussion.

Divergence:

- **None**

Incompleteness:

- **HTG1-SM-08-I-1 Specification of bootstrap process:** Extends I-HTG1-VOB-MS-2.

8 Local Time-Critical Sessions

8.1 HTG1-LTCS-01: Security Considerations for Local Time-Critical Session

Local non-time critical session applications are initiated in response to service advertisements. Communications characteristics of these applications are described in HTG1&3-1 *Overview of Harmonization Task Groups 1&3* [67].

They may use application-specific security mechanisms and will probably wish not to use lower-layer security mechanisms for efficiency reasons. Standards already exist for application-level security for certain applications (e.g., tolling [1, 2, 55]). In these standards, in general, the security mechanism specification is integrated with the application specification. This document does not further discuss application-specific security mechanisms for these applications.

Privacy issues relating to the use of multiple applications on a single ITS-S are discussed in section 14.3. Privacy issues relating to response to service advertisements are discussed in more detail elsewhere in the present document.

Divergence:

- **None**

Incompleteness:

- **HTG1-LTCS-01-I-1 Extract security mechanisms from application-specific standards:** There may be value in extracting the security mechanisms from application-specific standards so that they may be used by other applications.

- **HTG1-LTCS-01-I-2 Use of lower layer security mechanisms:** See 13 for a discussion of lower layer security mechanisms. There is an outstanding action item to determine whether lower layer security mechanisms are necessary to preserve privacy; if they are necessary in general, further analysis is necessary to determine whether and how individual applications may opt out from their use.

8.2 HTG1-LTCS-02: Privacy

See section 12.7 for a general discussion of privacy issues associated with responses to advertisements.

Since time-critical sessions may not wish to use lower layer encryption methods, in order to preserve privacy, each session should use different identifiers. This is currently supported by [55].

Divergence:

- **HTG1-LTCS-02-D-1 Changing identifiers**: [55] supports the use of identifiers that change between application sessions. [1, 2] do not specify a technique to change identifiers between sessions.

Incompleteness:

- **HTG1-LTCS-02-I-1 Guidance on privacy:** There are no standardized principles to be followed by SDOs when developing LTCS applications to ensure that they preserve privacy.

9 Local Non-Time-Critical Session applications

9.1 HTG1-LNTCS-01: Security and security management

Local non-time-critical session applications are initiated in response to service advertisements. Communications characteristics of these messages are described in HTG1&3-1 *Overview of Harmonization Task Groups 1&3* [67].

These applications may use application-specific security mechanisms or lower layer security mechanisms. As noted in section 3.1, application-specific security mechanisms are out of scope for applications defined outside a specific set of SDO working groups. Lower layer security mechanisms are discussed in section 13. Privacy issues relating to the use of multiple applications on a single ITS-S are discussed in section 14.3.

9.2 HTG1-LNTCS-02: Privacy

See discussion under HTG1-LTCS-02. The same considerations apply here.

10 Multi-RSU Session applications

10.1 HTG1-MRS-01: Maintaining a secure session

10.1.1 Description

Consider an application on a mobile ITS-S that wants to communicate securely with a server to exchange a lot of data. There may not be time to complete the transaction within the communication zone of a single RSU, so the data exchange must be capable of being resumed when a new RSU is encountered. This includes re-establishing the secure session in such a way that the endpoints are authenticated and appropriate confidentiality services are established before the data exchange is resumed.

Existing standards outside the ITS world provide mechanisms for achieving this goal. Different standards focus on different areas of the stack. For example, NEMO [93] and Mobile IP [94] provide resumable sessions over IP, and the Fast Session Resume functionality in TLS [95] provides resumable sessions running via TLS (which in turn typically runs over TCP/IP).

If there is a standardized set of secure session resumption protocols that ITS-S suppliers implement, it becomes easier to deploy applications that use persistent secure sessions.

10.1.2 Interoperability summary

This issue affects technical interoperability as client and server must use the same technique.

This issue may affect consistency of application behavior between implementations as applications may wish to communicate only between stations that support secure session resumption.

The issue probably will not affect consistency of user experience between jurisdictions, as it involves the use of standardized protocols from outside the ITS world.

10.1.3 Existing standards

No specific ITS standards.

10.1.4 Interoperability issues

No standards yet, so no issues.

10.1.5 Notes

The VIIC Proof of Concept project used a variation of HIP (Host Identity Protocol) to support multi-RSU secure sessions.

For further discussion of IP-layer solutions, see HTG1-LL-02: Layer 3 security mechanisms: interoperability and HTG1-LL-03: Layer 3 networking (IP): privacy.

10.2 HTG1-MRS-02: Privacy

10.2.1 Description

See HTG1-MRS-01: Maintaining a secure session for background discussion.

An application that resumes a session with a remote server must present that server with a session ID to allow session resumption. If the same ID is presented multiple times in plain text, it may be obtained by an eavesdropper. This may allow tracking. Additionally, the design of the session ID may leak information about the user and/or the type of service being used, which may count as PII depending on the amount and type of information leaked. (For example, consider a cookie which includes the user's email address).

To protect against linking or PII leakage, the session ID should be either encrypted or dynamic so that it changes every time the session is resumed.

Note:

- Unencrypted but dynamic session IDs may be repeated even though dynamic, to cover the case where a requested resumption of the session does not take place and the server is in a state that the application would otherwise consider stale.
- To protect against PII leakage, the session ID should be either encrypted or carefully designed to avoid leakage of information (this would imply a global format for session IDs so that the format of the ID did not leak information about the server).

10.2.2 Existing standards

No specific ITS standards.

10.2.3 Notes

The VIIC Proof of Concept project used a variation of HIP (Host Identity Protocol) to support multi-RSU secure sessions.

Elsewhere in this document:

- HTG1-LL-02: Layer 3 security mechanisms: interoperability discusses Layer 3 encryption, which may be used to encrypt application-layer session IDs.
- HTG1-LL-03: Layer 3 networking (IP): privacy discusses dynamic session identifiers for IP
- HTG1-LL-04: Layer 2 security mechanisms: interoperability discusses Layer 2 encryption, which may be used to encrypt session IDs at any higher layer.

ITS-S may potentially allow a user to opt out of requiring this type of privacy in order to obtain other benefits (for example faster/more reliable connections).

11 Multi-RSU Session applications: Security Management

11.1 HTG1-MRS-SM: Secure initialization

11.1.1 Description

An implementation of secure session resumption may need to have security information, such as keys, initialized. Consistency in key initialization will help developers and users.

11.1.2 Interoperability summary

This issue does not affect technical interoperability so long as different key initialization methods lead to correct keys being established.

This issue may affect consistency of application behavior between implementations as applications may support different key initialization mechanisms.

The issue may affect consistency of user experience between jurisdictions, as they may have regulations about the security of cryptography that may be used.

11.1.3 Existing standards

None known

11.1.4 Interoperability issues

None

11.1.5 Notes

None

12 Advertisements

12.1 Overview

See [71] for background material on service advertisements and discussion of non-security topics in interoperability.

12.2 HTG1-Adv-02: Communications security services

12.2.1 Description

The security requirements for service advertisements have not been analysed in depth in the research literature. IEEE P1609.2 and IEEE Std 1609.3 provide and motivate security services for WAVE Service Advertisements (WSAs). ISO 24102-5 specifies the CALM Fast Service Announcement Protocol (FSAP), but without specifying security services or providing a motivation for their omission. To proceed with harmonization it is necessary to determine exactly what the requirements are.

IEEE P1609.2 summarizes the security requirements as follows:

> A higher layer entity that registers for a provider service should request that its WSAs are signed if:
>
> - The deployer considers there is a risk to the privacy of responders, i.e., if a service is sufficiently rarely used that the fact that a given User responds to the service can be used to distinguish or track the user.
>
> - The deployer considers that an unauthenticated service could cause a force-multiplied denial of service attack, i.e., that the service is sufficiently widely used that, if it is advertised in an area of dense network traffic, so many WAVE devices will respond as to cause significant channel congestion.

A higher layer entity that registers for a user service should require valid signed WSAs if the deployer considers there is a risk to the privacy of responders. Conversely, a higher layer entity that registers for a provider or user service may choose not to require signed WSAs if there is no requirement for authentication or if the privacy of the user service is not compromised by responding to the WSA.

ISO has not provided any analysis and is expected in due course to endorse and extend the TVRA from ETSI [38]. The IEEE 1609 group's analysis that it is acceptable to have some secured and some unsecured fields in a WSA should be examined by the SDOs prior to endorsement (this has been addressed in part by the ETSI endorsement of IEEE P1609.2 described in TS 102 941).

IEEE 1609.2 and 3 do not provide a means to initiate a secure application-layer session using specific fields in the WSA, although individual advertised services may include secure session information in their PSCs.

Neither the WAVE Routing Advertisement in IEEE Std 1609.3 nor the security format in IEEE P1609.2 address IPSec. The IPSec session must be established using mechanisms in band to the IP connection. See section 13 for further discussion.

No standard specifies a security mechanism for initiating secure sessions at the MAC layer. MAC layer encryption may be a desired property to protect privacy, particularly in multi-application environments. See section 13 for further discussion.

Divergence:

- **HTG1-Adv-01-D-1 Secured advertisements only specified in IEEE**: Only IEEE specifies security for service advertisements.

Incompleteness:

- **HTG1-Adv-01-I-01**: The ISO standards (e.g., ISO 24102-5) do not specify security requirements for FSAP.
- **HTG1-Adv-01-I-02**: No standard specifies a generic mechanism for initiating application or facilities layer secure sessions.
- **HTG1-Adv-01-I-03**: No standard specifies a mechanism for initiating network layer secure sessions. See section 13 for further discussion.
- **HTG1-Adv-01-I-03**: No standard specifies a mechanism for initiating MAC layer secure sessions. See section 13 for further discussion.

For interoperability, both the EU and US sides should agree on both the security requirements and the mechanisms that satisfy those requirements. In particular as both parties share a common adoption of IEEE P1609.2 that supports both secure and unsecure elements in a single WSA, the selection of such a mechanism should be reviewed carefully in a full risk analysis approach to ensure the selection is fully informed.

12.3 HTG1-Adv-02: Signed datagram format

For interoperability, signed service advertisements should use the same format.

Existing standards (IEEE (1609.2, 1609.3)) specify a format for signed service advertisements that has not been formally adopted by other SDOs for co-operative ITS.

12.3.1 Interoperability issues

Incompleteness:

- **HTG1-Adv-02-I-01**: The ISO standards do not specify secure datagram formats for FSAP.

Even unsecured IEEE 1609 WSAs are incompatible with ISO FSAP, as the 1609.3 WSAs are wrapped in a 16092Dot2Data structure of type unsecured.

12.4 HTG1-Adv-03: Certificate Format

For interoperability, signed service advertisements should use a standardized format for their certificates.

Incompleteness:

- **I-01**: The ISO standards do not specify secure datagram formats for FSAP.

- **I-02**: The IEEE standards allow the use of Service Specific Permissions (SSP), but no SDO has yet defined SSPs for use within FSAP.

Divergence:

- **D-01**: IEEE 1609.2 uses PSID for encoding permissions. ISO would presumably use ITS-AID.

If security requirements can be harmonized, it should be straightforward to harmonize pseudonym format.

12.5 HTG1-Adv-05: Freshness requirements

Service advertisements often contain information that does not change frequently. Requiring every service advertisement to contain a fresh signature may impact performance for sender and receiver.[3] However, a long lifetime on a service advertisement allows an attacker to replay it until it expires, even if the valid advertiser has changed the services it wishes to advertise. Security standards may wish to specify an upper limit on the lifetime of a signed WSA.

Divergence:

- None

Incompleteness:

- **I-01**: The ISO standards do not specify signing intervals (or any signing) for FSAP. IEEE 1609.2 does not provide an upper bound on WSA lifetime but recommends that it be "on the order of minutes rather than seconds or hours."

12.6 HTG1-Adv-06: Performance requirements and verification policy

IEEE P1609.2 allows a receiver of a WSA not to verify it if no registered user service has requested signed advertisements.

Whilst for technical interoperability the verification of a signature does not have any impact there may be an impact on user expectation. There may however be an interoperability issue when viewed from system and user perspectives since choosing not to verify may allow the introduction of false content by an attacker relying on the non-verification that would filter false messages. Similarly a device set to bypass verification may appear to be more responsive than one that strictly enforces verification.

Incompleteness:

- **I-01**: Since ISO does not specify verification policy, it is incomplete.

[3] Less likely for the receiver, who can choose not to verify service advertisements that do not contain fresh information. See 12.5 for further discussion.

12.7 HTG1-Adv-07: Privacy

As discussed in section 12.2, privacy of units may be compromised by the observable fact that they respond to an advertisement. To protect privacy in this case, it may be useful for other units in the neighborhood to generate dummy responses (in a way that does not cause harmful congestion). If such an approach is deemed to be feasible there should be an algorithm for creating a dummy response that fools an eavesdropper but not the service provider.

Note that an alternative response to this concern is to take the approach that responses to service advertisements are “opt-in” and as such a responder can be deemed to consent to the necessary privacy-revealing processing and thus to accept the risks to privacy. While this argument carries some weight regarding information revealed by the responder to the service provider, it is not clear that the responder has the level of understanding to accept that they may reveal information to eavesdroppers via signaling data (in privacy processing, consent should be informed, and it is not clear if the end user has sufficient knowledge to make an informed decision regarding consent).

The appropriate approach should be derived as the result of a risk analysis.

Divergence:

- **None**

Incompleteness:

- **HTG1-Adv-07-I-1 Privacy requirements:** There is no specification of privacy requirements relating to responses to WSAs.
- **HTG1-Adv-07-I-2 Dummy responses:** There is no specification of whether dummy responses should be created, and if so how.
- **HTG1-Adv-07-I-3 Lower layer security**: See discussion in section 13.

13 Lower Layer

13.1 HTG1-LL-01: Statement of application communications security requirements

In the ISO CALM ITS-S architecture (also adopted in large part by ETSI), an application may request that the ITS-S provides a communications channel with certain properties. The CALM standards do not currently provide a means for applications to make statements about the required security properties of a communications channel although such profiles are being discussed and may be standardized in ISO or ETSI in due course, and standards are planned that will specify SAPs for this purpose. If there were a standardized means of specifying application requirements for channel security, this might simplify the task of developers who want to develop secure medium-neutral ITS applications and reduce the risk that

security was compromised due to a misunderstanding of the properties of a particular supplier's implementation of a particular network stack.

This issue does not affect technical interoperability but may affect consistency of application behavior between implementations.

Not all ITS-S need follow the ETSI/CALM ITS-S architecture.

Incompleteness:

- **HTG1-LL-01-I-1 Statement of application communications security requirements:** No standard specifies how applications may state communications security requirements.

13.2 HTG1-LL-02: Layer 3 security mechanisms: interoperability

IPSec is highly parameterizable. Existing ITS standards do not provide means to set up parameters for IPSec sessions. There is no support for other layer 3 security mechanisms.

This issue may affect technical interoperability as there is no adopted standard way to ensure that a given ITS-S can communicate securely using IPSec with a given endpoint even though the IETF has created the Internet Key Exchange protocols for this purpose. However, ITS-Ss may support standardized (IKE), proprietary or manual configuration.

This issue affects consistency of application behavior between implementations because different ITS-S may require different methods to configure IPSec, increasing the risk that some ITS-S do not support particular flavors required by particular applications or endpoints.

The issue probably does not affect consistency of user experience between jurisdictions.

Incompleteness:

- **HTG1-LL-02-I-1 Layer 3 security mechanisms:** No standard specifies layer 3 security mechanisms in an ITS context.

13.3 HTG1-LL-03: Layer 3 networking (IP): privacy

If an ITS-S uses the same source IP address multiple times (e.g., to communicate with a server with which it has an IPSec Security Association (SA) associated with that particular source address), the reuse of the source IP address acts as a static identifier that can be used to track the ITS-S.

This can be avoided by one of the following mechanisms:

- Change the identifiers used to initiate the IP session, as is done by, for example, the Host Identity Protocol (HIP).
- Encrypt below layer 3.

Neither of these mechanisms are yet standardized for use in ITS. Additionally, there is no explicit regulatory guidance as to the level of privacy that must be provided against an attack based on occasional reuse of network identifiers.

This issue affects technical interoperability, if this privacy protection is to be provided, as station network stacks must support the chosen privacy protection method.

Incompleteness:

- **HTG1-LL-03-I-1 Layer 3 privacy mechanisms:** No standard specifies layer 3 privacy mechanisms in an ITS context.

13.4 HTG1-LL-04: Layer 2 security mechanisms: interoperability

Layer 2 security mechanisms allow two or more nodes in a single-hop communications relationship to protect those communications, for example, from eavesdropping (by encryption) or modification (by integrity/authentication). These mechanisms might be useful to prevent leakage of PII from application or network identifiers that are not encrypted at higher layers. See HTG1-MA-02: Privacy for further discussion. The sections of IEEE Std 802.11 previously known as 802.11i define security mechanisms. However, 802.11p (IEEE Std 802.11 operating outside the context of a BSS) does not support layer 2 security mechanisms.

Even if these mechanisms are not applied in all cases, applications may wish to require that layer 2 encryption is applied in order to operate. See HTG1-LL-01: Statement of application communications security requirements for further discussion.

Layer 2 encryption may need to be compatible with one MAC chipset listening on multiple MAC addresses simultaneously. See 14.3 for further discussion.

This issue affects technical interoperability if layer 2 security mechanisms are supported, as communicating ITS-Ss must implement layer 2 security consistently.

This issue may affect consistency of application behavior between implementations as applications may wish to communicate only between stations that support layer 2 security. (See HTG1-LL-01: Statement of application communications security requirements.)

The issue may affect consistency of user experience between jurisdictions. Local authorities may wish to enforce privacy by use of layer 2 security, or to enforce that layer 2 security is not used to support law enforcement activities.

Incompleteness:

- **HTG1-LL-03-I-1 Layer 2 security mechanisms:** No standard specifies layer 2 security mechanisms in an ITS context.

14 Multiple applications and application management

14.1 Introduction: application and device initialization

An ITS-S may run multiple applications. Each application will have its own security requirements. However, the combination of applications may introduce additional threats to the communications security, such as:

- Privacy – the combination of applications that an ITS-S runs may act as an identifier
- Availability – one application may consume resources needed by another application

This section discusses the standardization of security mechanisms that may be used to mitigate these emergent risks. Figure 3 shows an overall process flow for application and device initialization. As with Figure 1, it identifies all of the functional entities separately for completeness. In practice, specific use cases (especially for single-application devices) may be able to use fewer entities or merge some of the entities of Figure 3 into a single entity. See Annex C for a further discussion, both of Figure 3 and of alternate, simpler architectures.

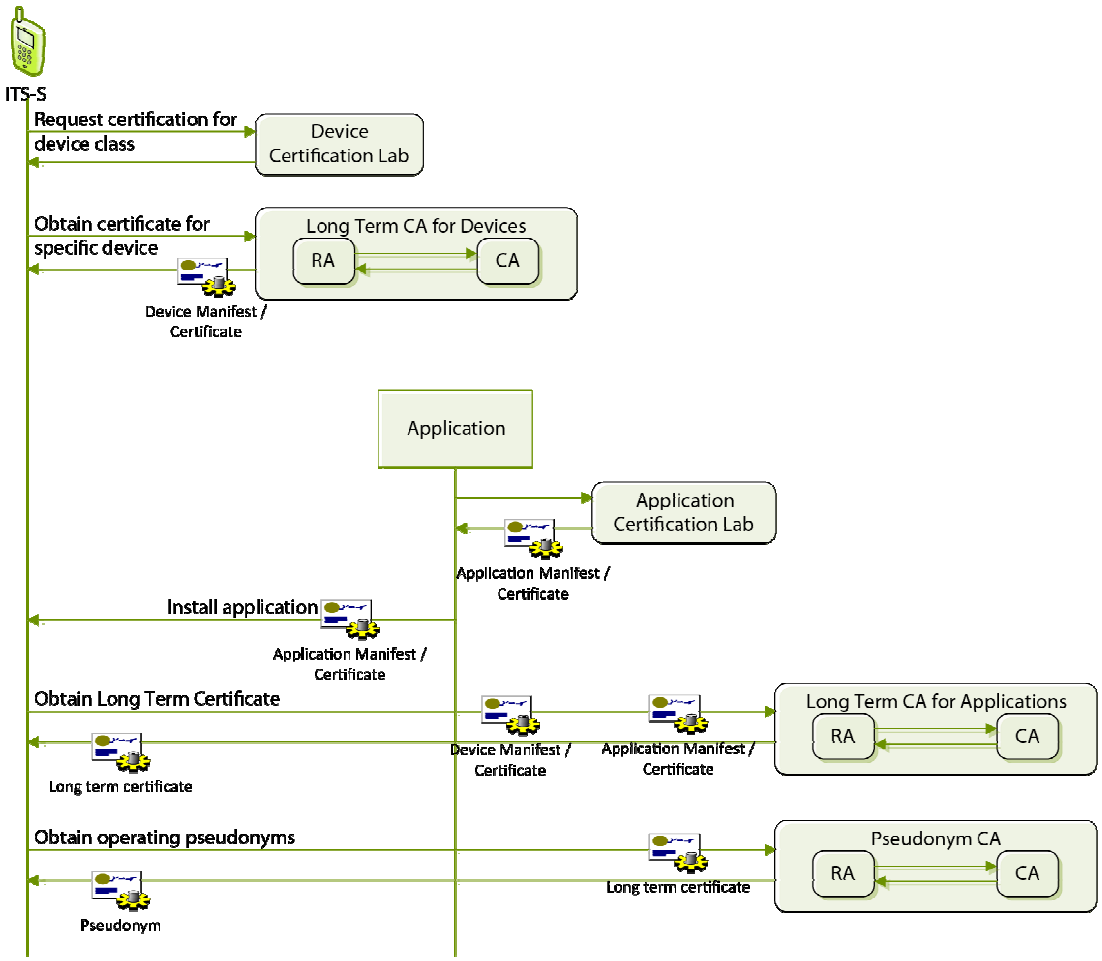


Figure 3: Initialization and approval of applications on multi-application ITS-S

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

14.2 HTG1-MA-01: Statement and approval of application use of resources

ITS applications use resources on the platform (for example CPU time, GPS information, cryptographic keys) and shared resources (for example the safety channel). Applications should only be permitted to use those resources if it can be established that they will use those resources correctly. For example, the system authorities may want to ensure that a commercial advertising application should not be able to send on the safety channel, or that malware should not have access to the CAM/BSM signing keys. An application may need to demonstrate correctness to multiple different parties, including:

- A certification lab that validates that the application behaves correctly.
- The ITS-S on which the application is installed.
- The CA or other security management entity that issues certs for use by the application.

In the first two cases, the correctness may be demonstrated by implementation-specific means. In the third case, it may prove useful to provide standard specifications for data structures by which an application can demonstrate to the CA that it is requesting access only to appropriate resources, used appropriately. The statements that use these structures should be made in conjunction with a statement of platform capabilities.

No specification for a statement of application resource requirements currently exists.

This issue does not affect technical interoperability.

This issue affects consistency of application behavior between implementations as this statement of requirements allows the CA only to issue certificates for applications that will behave correctly.

The issue affects consistency of user experience between jurisdictions, as it increases assurance that received data is correct.

Incompleteness:

- **HTG1-MA-01-I-1 Statement and approval of application use of resources:** No standard specifies statement and approval of application use of resources in an ITS context.

14.3 HTG1-MA-02: Privacy

If an ITS-S is transmitting application datagrams from multiple applications with the same network identifiers (such as the MAC address), and if the application related to each datagram can be determined (perhaps because an identifier such as an application ID or network address is in an unencrypted header), then an eavesdropper can tell that the applications are being run on the same ITS-S. The eavesdropper may also be able to tell that the applications are being run on the same ITS-S if the applications use the geonetworking stack, as the location of the sending ITS-S may only change by a small amount between sending messages from different applications.

If the eavesdropper knows the identity of the sender (perhaps because they're legitimately participating in one of the applications), this is a leak of personal information; even if the eavesdropper does not know the identity of the sender, the combination of applications could be unique to the station and allow the eavesdropper to track the vehicle.

We refer to this risk as PII leakage through Use of Multiple Applications (PUMA).

Potential countermeasures to this risk are listed below, along with potential issues with their implementation.

- Use a different set of network identifiers for each application (in other words, each application runs on its own virtual machine down through the MAC level).
    - Issue: to support different addresses for different applications on the same channel, a device would have to receive on multiple MAC addresses simultaneously. This is theoretically possible with 802.11, but it is not clear that there is commercial support for it.

- Encrypt all identifiers other than those necessary to complete the first hop (i.e., all identifiers except the destination MAC address for communications over 5.9 GHz).
    - This would require layer 2 encryption, which is not currently supported by IEEE 802.11-2012 operating outside the context of a BSS.

- Ensure that identifiers change between one use of an application and the next and do not leak information about which application the identifiers refer to.

Additionally, the level of privacy against PUMA may be subject to policy:

- Regulatory (regional or domain) policy, which might set a minimum level of privacy that requires protection against PUMA.
- ITS-S local policy, under which a user might require a minimum level of protection against PUMA that exceeds the regulatory policy.

This issue may affect technical interoperability; if layer 2 encryption is the appropriate way to handle this concern, then devices that support this level of privacy must support layer 2 encryption in a consistent way.

This issue affects consistency of application behavior between implementations as an application may wish to modify its behavior based on whether the platform provides protection against PUMA.

The issue affects consistency of user experience between jurisdictions, as privacy requirements may vary from one jurisdiction to another.

Finally, note that if one application has the ability to restrict pseudonym change in an alert state, it may impact the ability of other applications to operate with proper privacy protection if the two applications share pseudonyms or pseudonym service state. This can be mitigated by allowing different applications

to have distinct states within the pseudonym service, corresponding to different identifiers at all levels of the network stack for which this is achievable without impacting quality of service.

Incompleteness:

- **HTG1-MA-02-I-1 Privacy when using multiple applications:** No standard specifies privacy mechanisms for use of multiple applications in an ITS context.

14.4 HTG1-MA-03: Protection against malware

The model in this document assumes that software is carefully evaluated before it is allowed to run on an ITS-S (the evaluation is carried out by the Certification Lab functional element shown in Figure 1 and Figure 3 and discussed in Annex C). However, it is possible that malware may be carefully designed so as to behave innocuously during evaluation and maliciously under certain circumstances in deployment. In this case there may need to be mechanisms for removal of those applications from the system, including:

- Platform-level removal of malware using anti-virus or similar mechanisms.
- Some form of revocation list instructing recipients not to trust messages with certain characteristics.

This issue affects technical interoperability if application revocation lists are to be used.

This issue affects consistency of application behavior between implementations if platform-level removal of malware is used as different platforms may have different standards for application removal.

15 Physical and platform security

15.1 HTG1-PPS-01: Minimum security requirements for platform security

As previously stated, ITS applications use resources on the platform (for example, CPU time, GPS information, cryptographic keys) and shared resources (for example the safety channel). Applications should only be permitted to use those resources if it can be established that they will use those resources correctly. For example, the system authorities may want to ensure that a commercial advertising application should not be able to send on the safety channel, or that malware should not have access to the CAM/BSM signing keys. In order to ensure that the applications behave correctly, the platform also need to behave correctly. This may include providing security mechanisms such as enforcing trustworthiness of code, ensuring application separation, requiring code signing on installation, hardware protection of keying material, or the use of Trusted Platform Module (TPM) or similar technology to disable certain functionality if the platform is not in a known good state.

There are currently no minimum standards for the platform security mechanisms that an ITS-S must provide to ensure correct application behavior. It seems advisable to establish some such standards, or run the risk that easily-compromised devices will be manufactured, allowing attackers to easily create

and send false data. These minimum standards must be harmonized as otherwise a low-security device which is valid in one domain could be brought to and operate in a higher-security domain (assuming that all other standards are harmonized).

This could be implemented in the form of defining a number of assurance levels, from a minimum assurance level that requires no or minimal extra security mechanisms in a platform to a very high-level assurance level that requires a completely trusted platform that may require continuous platform integrity checking, trusted computing components, etc.

It would then be either up to the central authorities (e.g., the CA) to determine the minimum assurance level that is required to issue specific certificates and authorizations. For example, a police car that wants to acquire a certificate that allows control traffic lights may require a higher minimal level of assurance compared to ordinary passenger cars.

In addition to evaluating the assurance levels at the CA level when issuing certificates, vehicles may also send their assurance level in messages (as part of certificates) and let receiving vehicles take the decision to what extend to trust the message and its sender. This might be appropriate if vehicles react differently to the same message. A vehicle that just signals a warning to the driver may accept messages originating from vehicles with a lower assurance level compared to vehicles that trigger automatic reactions like automatic braking. The latter will likely require a higher assurance level to be in place.

This issue does not affect technical interoperability except in the second alternative. Here, assurance levels need to be agreed upon and integrated into certificates.

This issue affects consistency of application behavior between implementations as a less-secure ITS-S may behave differently from a more secure ITS-S.

15.2 HTG1-PPS-02: Statement of platform capabilities to CA

As previously discussed different platforms will have different resources and capabilities. A CA may need a clear statement of the capabilities of the platform in order to decide to issue certificates for applications on that platform. This may include information such as what level of physical/hardware key protection is provided or what assurance mechanisms are in place to ensure invalid applications do not have access to scarce public resources. No specification for a statement of platform capabilities to a CA currently exists. Such a statement of capabilities should be standardized.

This issue does not affect technical interoperability.

This issue affects consistency of application behavior between implementations as this statement of capabilities allows the CA only to issue certificates for applications on platforms that will behave correctly.

The issue affects consistency of user experience between jurisdictions, as it increases assurance that received data is correct.

15.3 HTG1-PPS-03: Platform authentication to application on install

Applications may need a clear statement of the capabilities of the platform in order to activate or deactivate features, or to ensure that they are being installed on a valid platform. Existing mobile operating systems provide these statements: iOS implicitly (by providing OS version number and device type) and Android explicitly (by providing a list of resources to applications on install). The HTG considers it appropriate to use proprietary mechanisms to state platform capabilities to applications, although a "master list" of resources that might be present on an ITS-S might be a useful resource to platform-, language-, or manufacturer-specific SDOs developing these proprietary mechanisms.

This issue does not affect technical interoperability.

This issue affects consistency of application behavior between implementations as it provides assurance to applications that they will operate correctly.

The issue does not affect consistency of user experience between jurisdictions.

15.4 HTG1-PPS-04: Minimum security requirements for secure firmware upgrade

An ITS-S supplier may wish to upgrade the firmware on their ITS-Ss.

Security mechanisms can be used to provide assurance to the firmware upgrade process. For example, there may be enforcement mechanisms to ensure that firmware has been produced by an approved supplier, or that it is newer than the currently installed firmware (to prevent rollback attacks to an older, less-secure version).

Suppliers may also wish to define different upgrade methods: for example, over a wired interface only, or over a wireless interface with appropriate protections.

Although these firmware upgrade mechanisms can be implementation-specific, the upgrade mechanism must be approved in order to demonstrate that it does not compromise the minimum security requirements for platform security previously discussed.

This issue does not affect technical interoperability.

This issue affects consistency of application behavior between implementations as a less-secure ITS-S may behave differently from a more secure ITS-S.

The issue affects consistency of user experience between jurisdictions, as minimum security requirements increase assurance that received data is correct.

15.5 HTG1-PPS-05: Station Management

A station owner may wish to manage it remotely. This is particularly the case with infrastructure nodes such as RSEs, though it may also be of use for commercial vehicle management. There are no standards

currently defined for security remote station management. For remote management, it may be the case that the unit being managed has no network access other than through the managing unit, and there may be multiple managing units each of which may potentially be compromised. For example, consider a weather and road conditions sensor on a bridge that is physically hard to access and can be managed by any vehicle from a fleet of maintenance vehicles.

Since RSEs of this type will typically be procured by highway agencies or similar bodies from multiple vendors and at different times, it is extremely valuable to have a standard for security for management, as this will allow the procuring agency to ensure consistent behavior.

Working items to address this are currently illustrated in ISO TC204 WG16 (ISO 24102-2) and IEEE (IEEE 1609.6).

This issue affects technical interoperability.

This issue affects consistency of application behavior between implementations as a less-secure ITS-S may behave differently from a more secure ITS-S.

The issue does not significantly affect consistency of user experience between jurisdictions.

16 Future extensibility

This is related to the issue HTG3-GE-06: Releases identified in HTG3-1:2012.

16.1 HTG1-Fut-01: Crypto algorithm agility (applications using 1609.2)

Advances in cryptanalysis or in general purpose computing may lead to currently specified cryptographic algorithms no longer offering an acceptable level of security. Note that there are known algorithms for breaking ECDSA rapidly on quantum computers of sufficient size. No such computers currently exist, but quantum computing is an area of active research and it is highly conceivable that such computers will be developed within the lifetime of the first vehicles deployed with inbuilt ITS-S.

- The protocols should support migration to new cryptographic algorithms as appropriate. This is discussed further in this section.
- If a new cryptographic algorithm is introduced, older implementations may need to be updated to support that algorithm.

This issue affects technical interoperability: different implementations must identify and support algorithms in a consistent way, but for PKI systems where the algorithm is identified in the public key certificate, the algorithm identity is exchanged between relying parties. Where a new algorithm is added to 1609.2 by revising the standard the primary impact will be to require a change to the version number of the 1609.2 data structures and for applications to act on this version number when implementing processing.

16.2 HTG1-Fut-02: Crypto algorithm agility (applications not using 1609.2)

As above, advances in cryptanalysis or in general purpose computing may lead to a situation where currently specified cryptographic algorithms no longer offer an acceptable level of security.

- The protocols should support migration to new cryptographic algorithms as appropriate. This is discussed further in this section.
- If a new cryptographic algorithm is introduced, older implementations may need to be updated to support that algorithm.

This issue affects technical interoperability: different implementations must identify and support algorithms in a consistent way. This is less problematic for PKI systems where the algorithm is identified in the certificate, but for other systems, (e.g., symmetric key systems) alternative means of exchanging algorithm identity information between relying parties are required. The impact is that non-ITS-specific security protocols may or may not support crypto algorithm agility. Implementers and designers of ITS applications that use non-ITS-specific protocols should ensure that they choose protocols that support algorithm agility, track the development of those protocols to note whether recommendations for crypto algorithms change, and support software/firmware upgrade mechanisms to ensure that a given application always uses a cryptographic mechanism that gives an appropriate level of security.

16.3 HTG1-Fut-03: Ability to support new formats (applications using 1609.2)

IEEE P1609.2 may be updated or superseded.

- Applications and protocols should support migration to a future version of IEEE P1609.2 as appropriate.
- If a new version of 1609.2 is introduced, older implementations may need to be updated to support that version.

This issue affects technical interoperability: different implementations must identify and support 1609.2 versions in a consistent way. Currently the 1609.2 version number can be used to identify new versions of 1609.2. If 1609.2 is superseded, such that the 1609.2 version number is no longer used, current applications do not support a means to migrate to a different security mechanism (for example, the definition of BSM requires that 1609.2 is used). This could be addressed by an application-specific or global security mechanism identifier.

16.4 HTG1-Fut-04: Ability to support new formats (applications not using 1609.2)

All security mechanisms may be updated or superseded.

- Applications and protocols should support migration to new security mechanisms as appropriate.

- Older implementations may need to be updated to support that version.

This issue affects technical interoperability: different implementations must identify and support security mechanisms in a consistent way. In particular, non-ITS-specific security protocols may or may not be clearly upgradeable. Implementers and designers of ITS applications that use non-ITS-specific protocols should ensure that they choose protocols that are upgradeable, track the development of those protocols to note whether upgrades are necessary, and support software/firmware upgrade mechanisms to ensure that a given application always uses a protocol that gives an appropriate level of security.

Annex A Overview of security and privacy model for cooperative ITS

The core co-operative ITS model revolves around the transmission of vehicle status messages for receipt and processing locally to each receiver. There is no over-the-air response to the status messages and an assumption that no communications sessions are established. The transmitter asserts the status of the entire content of the CAM or BSM (and of DENM for events) for verification by each receiver.

The generic model of assertion statements is given below:

Assertion **A** was issued at time **t** by issuer **R** regarding subject **S** provided conditions **C** are valid.

This statement is what the receiving (and relying) entity is provided with, and the security model requires that each of **t**, **R**, **S** and **C** are validated to ensure that any action dependent on **A** is provably allowed. In ITS validation of the issuer identity (**R**) is achieved by authentication using IEEE 1609.2 digital signature, where the subject (**S**), the data being asserted (**A**) and the conditions (**C**) are set by the ITS-S. In ITS the subject (**S**) is normally the ITS-S.

For efficiency at the air interface, the transmitter (i.e., R, the entity making the assertion) is expected to validate that conditions related to the assertion are valid before issuing the assertion to the relying party.

Whilst it can be argued that privacy is distinct from communications security (ComSec), the majority of ITS standards and development organizations have addressed privacy protection by the application of a number of security mechanisms. With regard to privacy it should be noted that vehicles are large items that can be tracked by existing systems (both manual and automatic). Both vehicles and their drivers are licensed and their rights are strictly regulated, with enforcement of regulation by both manual and automatic means. It is not possible for protection of radio signaling, with a view to transmissions not containing Personal Identifiable Information (PII), to afford privacy to vehicles in such a way that their behavior is not visible. The efforts of privacy protection in ITS have therefore been focused on ITS not being a net contributor to privacy loss, and to give assurance to ITS users that the system has made every effort in design to conform to the requirements set by Data Protection and Privacy legislation. It is expected that current legislation requiring visible vehicle registration identity and for driver managed regulation compliance will remain in force irrespective of the capabilities of ITS.

NOTE: In a widely connected ITS system, data that may be initially envisioned to be carried only by the 5.9GHz point-to-point radio system may in practice be carried by additional radio media, or be submitted to additional processing in a networked node. The effect of such broadening of scope in deployed systems will have an impact on privacy and in particular on maintenance of explicit and informed consent. Whilst not in the scope of the EU-US Harmonization effort (which has its focus on the 5GHz point-to-point radio systems), the recognition that ITS is just one element of both Smart Cities and Smart Society initiatives and that data from ITS will be integrated to them is important. Thus data that may be considered as "privacy protected" in the limited context of 5GHz co-operative ITS, may have that protection challenged in wider systems where correlation of the ITS data with other behavioural data may serve to identify an individual or a community of individuals. There is significant work in this area being carried out in research and in EU FP7 projects i-SCOPE and i-Tour that are addressing this problem and developing distributed life-time consent models that should be considered in the wider ITS context in due course.

The detail of local legislation, and regional interpretations of privacy, are not covered by the present document. In both, privacy and security standardization is an essential but insufficient element in deployment. Whilst the work of the HTG is primarily considering gaps in standardization, it has to be recognized that for full interoperability, many issues relating to policy, organization, and configuration will also have to be addressed. However in identifying the ability of harmonized ITS standards to meet the requirements of both the EU and the US, due attention has been given in this document to ensure that standards in support of privacy are analyzed and any missing or conflicting elements to achieve interoperability highlighted. Privacy legislation in general follows the principles established by the Universal Declaration of Human Rights for the right to privacy, although the regulation has in most cases not anticipated the level of data flows that arise from modern telecommunications. As a result, in spite of following a common set of principles, different jurisdictions may have different privacy policies with regard to:

- Linkability of information for law enforcement.
- Requirements for a minimum level of privacy.
- Legality of certain law enforcement actions (e.g., automatically issuing speeding tickets).
- Enforcement of restrictions on movement (e.g., barring a particular person from entering or leaving the country).

As shown in Figure 4, privacy sits at the centre of a complex mesh of rights, standards, and technologies.

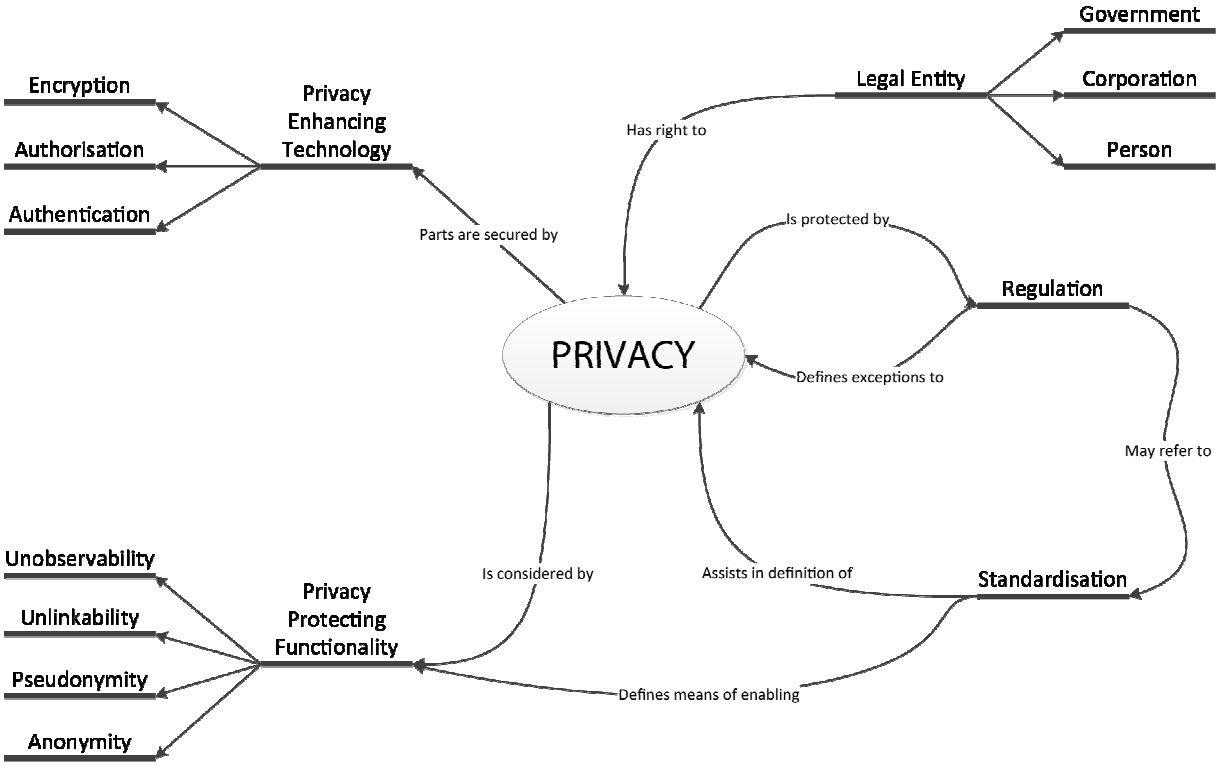


Figure 4: Mindmap of privacy in its wider context

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

Stakeholders in ITS, both in the U.S. and in Europe, have been reluctant to clearly express their privacy requirements. In some instances, this is clearly where a conflict of responsibility applies: An OEM, or a driver, or a road operator, is not a law enforcement entity and thus may not be willing to commit to support requirements that may imply such as role (e.g., whilst it is reasonable for a law-abiding citizen or corporation to expect that violators of the law should be identified and brought to justice, this is generally not considered to be equivalent to asking that citizens act as law enforcement agents in reversing an alias to a true identity). Similarly there may be different regulatory treatments of self-assertion of violations; therefore if an ITS-S acting on behalf of a driver asserts that the driver is (say) breaking the speed limit, is this treated in the same way as independent detection by a law enforcement agent of the same violation? It should be noted that many of these issues are not specific to ITS and whilst harmonization of technical standardization required to support a broad spectrum of privacy requirements is actively being conducted there may be variations in the deployment resulting from the fractured regulatory environments.

Insofar as existing standards are concerned IEEE P1609.2 acknowledges the need for privacy but does not provide detailed specifications for either a privacy architecture or anonymous certificates. In ETSI TS 102 940 and ETSI TS 102 941, whilst a high-level architecture for privacy protection that provides separation of authorities for identification and access control is defined, it does not provide protocol for

some aspects of credential management (e.g., revocation of certificates, initialization of certificates[4]). Some of the work in consortia (e.g., C2C-CC or CAMP) and research projects (e.g., PRESERVE, VSC-3) is more advanced as the context for deployment is clearer, thus allowing full technical specification of a pseudonym solution.

[4] An architecture does not define protocols but provides support of them. In this case ETSI TS 102 940 provides an architectural framework for authorities to manage certificates. A detailed protocol is only described in ETSI TS 102 941 for simple provision of pseudonymous authorisation certificates.

Annex B Overview of trust model in ITS

The security model required in co-operative ITS is to allow trust in the source of data between parties who have no pre-defined relationship. For many C-ITS applications, the means to achieve this is through asymmetric cryptographic signature of message contents, where the public key is exchanged in a message-associated certificate.

The model for certificate trust is conceptually simple: Party A (Alice) certifies that they trust a claim of Party B (Bob) and signs a certificate that proves this and identifies the context for which that trust is given. Bob can then exchange this trust certificate with his correspondents (Eve), and if Eve also trusts Alice, they may choose to trust the claim of Bob without having to know anything about Bob other than what has been certified by Alice. The content of the certificate includes the public key belonging to Bob.

The relationship of Alice to Bob—and Eve to a large extent—determines the level of trust afforded by Eve to any communication from Bob. If all of Alice, Bob and Eve are peers, the scalability of the trust model is low; whereas when Bob and Eve are peers, but Alice is a higher level authority acknowledged as such by each of Bob and Eve, the potential for the scheme to scale is increased.

When generating an asymmetric key pair the role of the public key certificate is multifold:

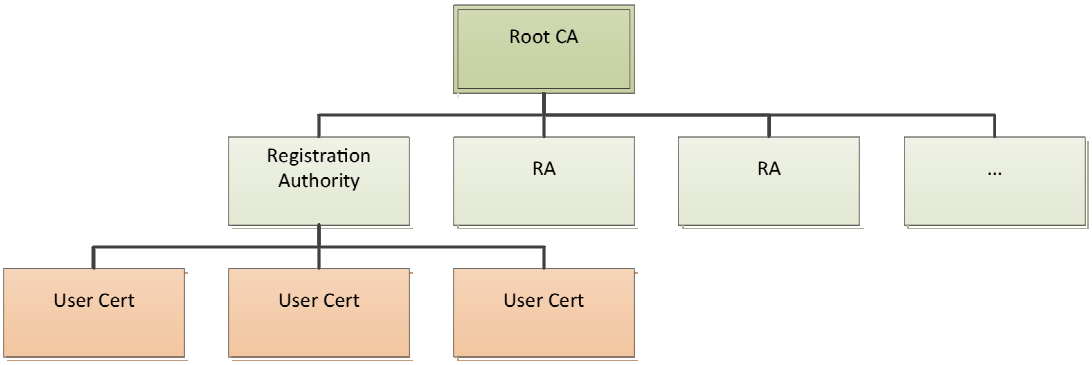
- It verifies that the authority (Alice) has proven the relationship of the public key to the private key.
- It identifies the operations with which the key pair is allowed to be associated.[5]
- It identifies the context in which operations are allowed.
- It may identify the holder of the key pair (key pair association to a person).
- It may identify a specific role (key pair association is to the role).

Each PKC therefore gives qualified claims regarding the use of the key pair.

Annex B.1 CA and PKI hierarchies

The root Certificate Authority is the one that all lower layers in the hierarchy must trust. For ITS, involving many millions of vehicles and many hundreds of distinct roles, it is also reasonable to have as few layers in the hierarchy as possible whilst allowing a reasonable management load to be carried.

[5] For example encryption, integrity, digital signature.



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

The number of levels in the PKI and also the number of entities in each layer need to be carefully managed. As each leaf acts as the authority for the leaves below, it has to have a manageable processing load taking account of how many certificates it can issue in a particular time period. It is important that due care is taken in the process prior to issue of a certificate, as the issuer is acting as a trusted third party on behalf of the requesting entity.

Annex B.2 Alternative models to PKI for key management

The rule of operation in asymmetric cryptography is that you can freely share the public key, and there are many means to achieve this, including publishing on a public web site, using a keyserver, distributing with message content (email), and X.500/LDAP directories. Sharing the public key does not damage the security of the system as there is no non-trivial means of identifying the private key from knowledge of the public key.

Whilst formally a PKI is the most structured it is also the most complex in terms of management. For small projects the web of trust model may be sufficient. Simply, ITS is not a small undertaking and justification for anything other than a true PKI is difficult to make.

Annex B.3 Overview of ITS requirements

The existing ITS standards do not define the structure of the PKI. The implication of this is that for harmonisation every application, manufacturer, road authority could establish themselves as a root authority without clear guidance given on a structure and how they should seek to place themselves within it. Taking account of the model proposed in ETSI (Figure 1) and the reference points they introduced, the security authority and registration authority are responsible for assuring that the ITS applications deployed on a station are properly certified and this may be a very simple PKI.

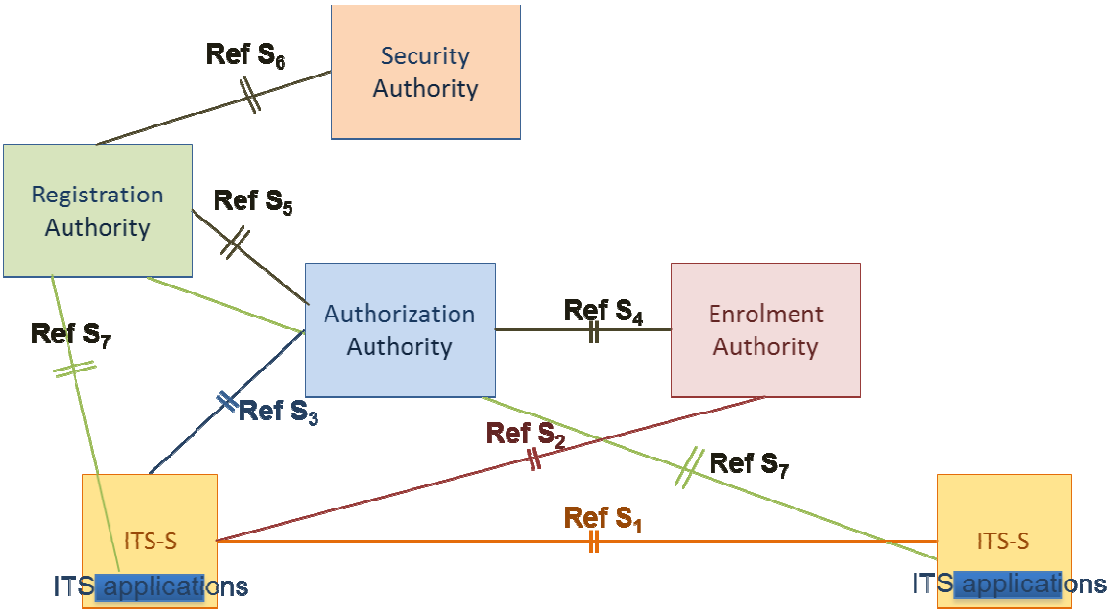


Figure 5: Authorities defined in ETSI for security processes

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

In summary the roles of the authorities with respect to the user of the ITS-S are as follows:

- Enrolment authority—knows the true identity (the canonical identity) of the ITS-S
- Authorisation authority—has a transitional relationship to the ITS-S identified only be a pseudonym that is attested by the enrolment authority (i.e., the enrolment authority acts as an identity server for the ITS-S)

There are a number of assumptions that can be stated for ITS applications:

- ITS applications are generated (developed) by various suppliers.
- ITS security authorities have means to verify/validate the correctness and authenticity of ITS applications.
- ITS security authorities issue ITS application certificates.
- ITS application certificates are granted only to verified/validated ITS applications.
- ITS application certificates contains the following information:
    - Permissions.
    - Security needs/requirements of the ITS application.
- ITS applications register at ITS registration authorities using ITS application certificate.

Annex C Deployment models

Annex C.1 Introduction

The aim of the HTG has been to be comprehensive in identifying standards that must be developed or harmonized to allow harmonized deployment, and this has led to us identifying a large number of actions. However, individual deployers may well not need to implement all of the standards. This section discusses different deployment models for devices and applications that interact with the PKI. The aim is to illustrate that, although the system has many different identified components to allow for flexibility, in practice early deployments or deployments of simple devices can be quite simple.

Annex C.2 Multiple-application model

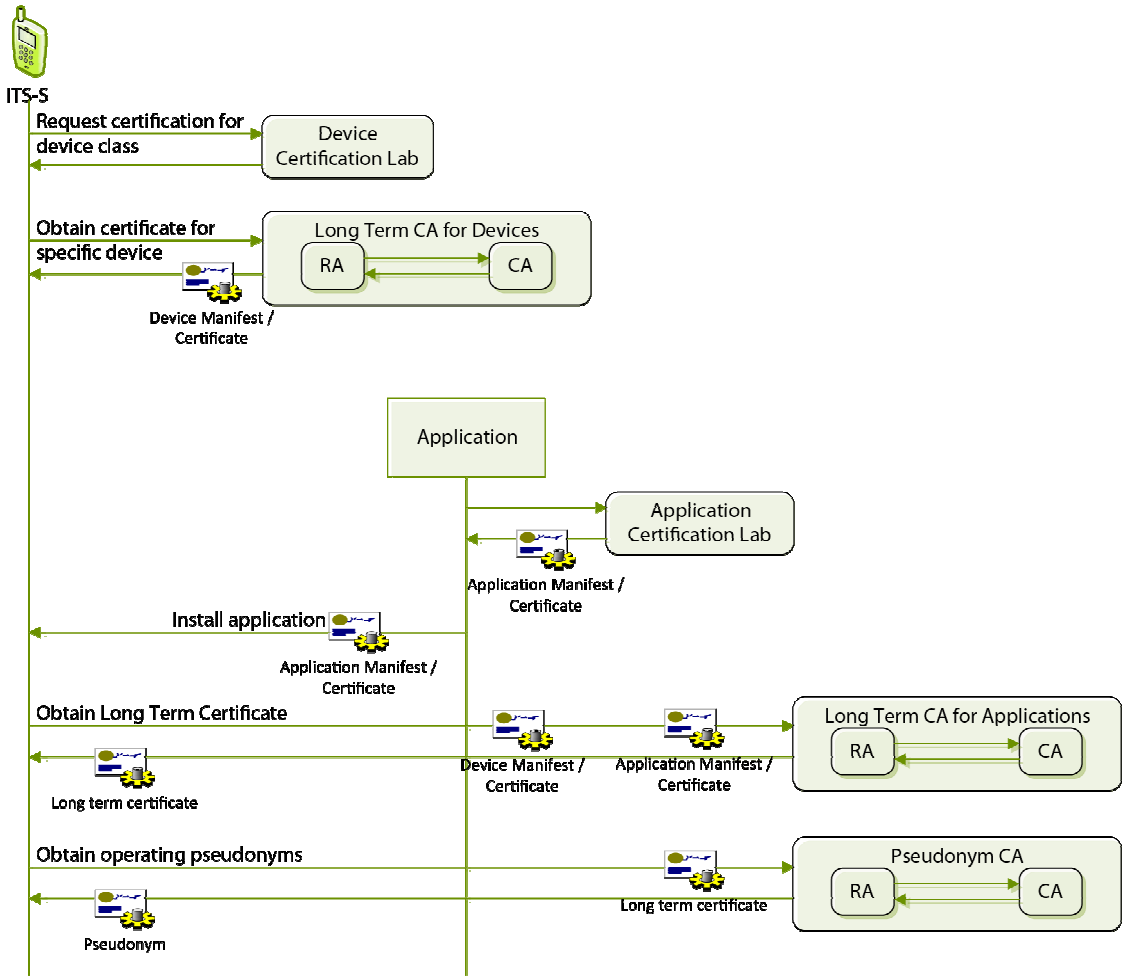


Figure 6: Full-featured application authorization model

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

Figure 6 shows a model for obtaining pseudonym certificates when a device may host multiple applications which may be installed at different times. In this model:

1) A sample or samples of the device are tested by the certification lab. The certification lab produces a report identifying the conformance properties of devices of that time.

2) For each individual device, the manufacturer obtains a device certificate. This provides, either directly or by reference (to, for example, the certification lab report), a statement of the permissions that applications on the device may be granted. The RA for devices approves the request and the CA for devices issues the certificate.

3) The application developer develops an application that requires permissions (for example, it sends on the safety channel, or it makes assertions about vehicle location that will influence others' driving decisions). The application is reviewed by an application certification lab to verify that it operates correctly. The application certification lab attests that the application is valid in this model by signing the application itself along with a statement of the permissions that the application requires and has been granted. This statement of permissions can be considered an application certificate, and the certification lab in this case acts as an RA and a CA for applications.

    - NOTE 1: The CA and RA for applications may be separate from the certification lab; they are omitted from this diagram for simplicity.

    - NOTE 2: The application developer may also have a certificate which they use to demonstrate to the certification lab that the application is correct. Highly trusted application developers may be able, in some models, to use this certificate directly to sign the application for installation.

4) The owner or operator of the device installs the application. During this process the application authenticates itself to the device and presents its certificate. The user may also manually approve the application's requests for permissions.

5) The application requests a long-term certificate. In order to obtain the long-term certificate the application instance must trustably assert to the CA that it is an instance of a trusted application, running on a trusted device. In this model the assertion is made by signing with the device certificate (to show trustworthy OS operations) a request that includes the application certificate (to specify the exact permissions requested).[6] The RA for long-term application certificates approves the request, and the CA for long-term application certificates issues the certificate.

[6] The use of the application cert isn't vital here: the LTCA may be informed of the permissions that the application is requesting by any appropriate means.

6) The application uses the long-term certificate to sign a pseudonym request. The RA for pseudonyms approves the request and the CA for pseudonyms issues the certificates.[7]

This description does not include a specification of how the device bootstraps its trust in the CAs; this can be accomplished by standard PKI means (out-of-band installation of root certificates + management messages to add other CAs as necessary).

Annex C.3 Single-application device

Figure 7 shows a model for obtaining pseudonym certificates for a single application device. This might be, for example, an active safety device running on a built-in OBE. In this model:

1) The device OEM is accredited by a certification lab to produce trustworthy devices and applications.

2) Over a secure connection from the OEM to the long-term CA, the application requests a long-term certificate. The CA for long-term application certificates issues the certificate. In this model, the OEM effectively acts as the RA because it is trusted to make the assertion that the device and application are trustworthy, i.e. to approve the request. This is shown by including the RA for long-term certificates inside the dotted box labeled "OEM" in Figure 7.

3) The application uses the long-term certificate to sign a pseudonym request. The RA for pseudonyms approves the request and the CA for pseudonyms issues the certificates.

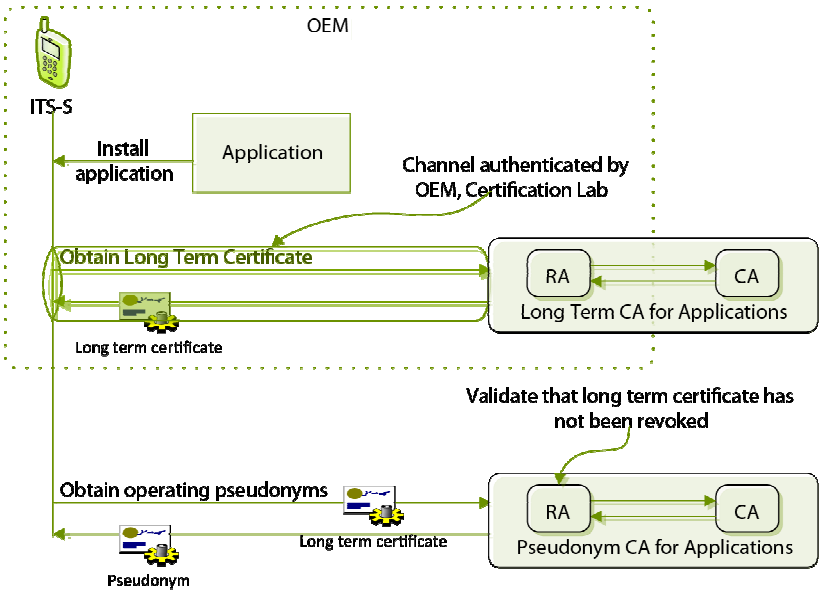


Figure 7: Certificate Request for single application device (example flow)

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

[7] In the C2C-CC PKI memo, the logical role of the RA for pseudonyms is played by the long-term CA. The description in this document is intended to identify the logical roles without making any assumption about whether the organizations that fulfill those roles are distinct.

Annex C.4 Public safety vehicle

The case of issuing certificates to public safety vehicles, such as police vehicles, has some interesting characteristics.

Public safety vehicles may not always want to make it known that they are public safety vehicles.

Public safety vehicles may not always be authorized to act as public safety vehicles (think volunteer fire department, or school buses pressed into service as evacuation vehicles during a flood).

Public safety vehicles may have built-in OBEs or use aftermarket devices.

Public safety vehicles are typically more powerful than private vehicles, so their authorizations must be policed more actively than the authorizations of private vehicles.

Given all these considerations, it is hard to show a single model for public safety vehicles. Figure 8 shows a possible model for public safety vehicles with built-in OBEs. The flow is very similar to the flow for single-application devices. The major difference between the two cases is in the behavior of the RA. For the single-application device, the RA approves the pseudonym issuance so long as the device has not been revoked. The public safety vehicle may be in a third state in addition to "approved" and "revoked." it may be not revoked, but not approved at this time. (An example would be the case of the volunteer police officer who is not on duty this week). The RA in this case has to interact with a permitting authority outside the scope of the PKI in order to track these real-world dynamic permissions.

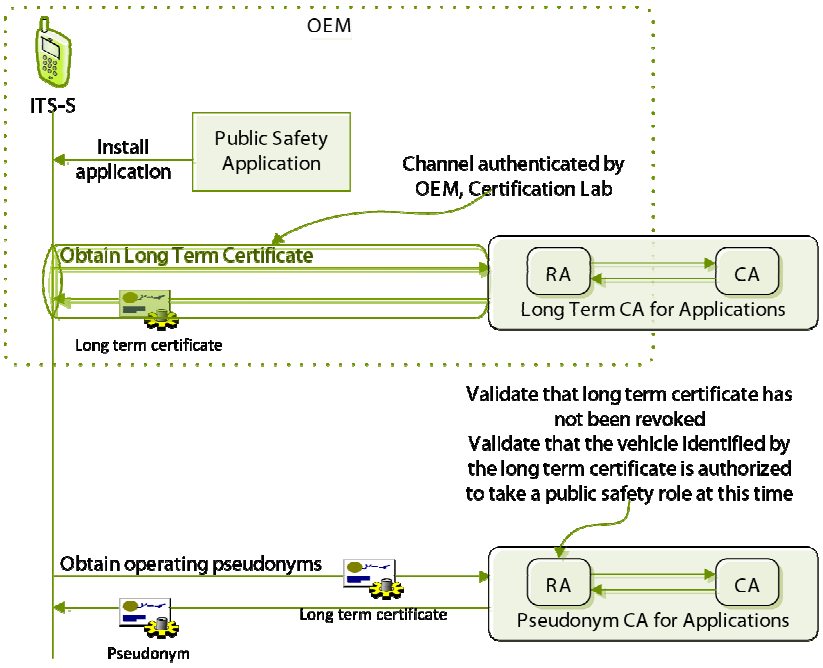


Figure 8: Certificate Request for public safety vehicle with built-in OBE

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

Annex C.5 Separation of authorities to enable identity protection

In the wider scheme the aim of separating authorisation and enrolment is to allow pseudonymous invocation of applications and transfers of data between ITS-Ss. The PKI to support this can be simple as in Figure 9.

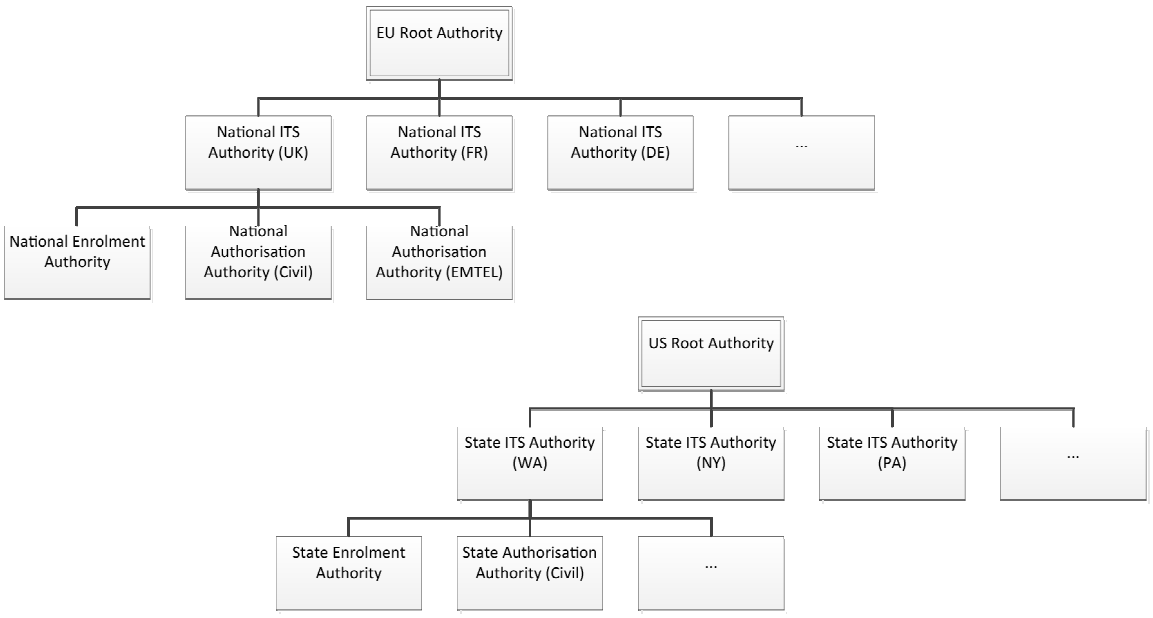


Figure 9: PKI structures with regional root and national authorities

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

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

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

FHWA-JPO-13-077

U.S. Department of Transportation