Feedback to Standards Development Organizations—Security

Document HTG1-3

Version: 2012-11-12

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

European Commission

U.S. Department of Transportation

EU S ITS COOPERATION

Table of Contents

1 Executive Summary

In order to achieve the goals of EU-US interoperability in ITS for the purposes defined in “Overview of Harmonization Standards” (HTG1&3-1) and examined for the security domain in HTG1-1, the present document provides guidance to the SDOs for actions to be taken that raise the assurance of interoperability of deployed equipment.

In order to support deployment of standards-compliant equipment there are additional actions that are required to be taken that have been identified in the present document as "non-SDO" actions. In those cases where the SDO is closely linked to the appropriate non-SDO authority the SDO may be asked through the present document to coordinate the non-SDO actions with those of the SDO. The actions are further classified as actions to remove discrepancies between EU and US standards (prefixed by D-) and as actions to fix incompleteness where further standardization is required before devices can be brought to market (prefixed by I-). The priority indication is considered as follows:

- High
  - Failure to address this will lead to inability to launch common equipment in multiple markets and may lead to inability of manufacturers to build equipment within a single market that will give high assurance of interoperability and interworking with similar equipment from competing manufacturers.
- Medium
  - Failure to address may delay development and operation in the market and may lead to uncertainty in performance or capability in some markets.
- Low
  - May not impact ability to build and market equipment, but some services may not be able to be launched.

The bulk of the analysis for the findings presented below is given in the accompanying document HTG1-1 [66] and the analysis is not repeated here. In some cases the actions arising from issues identified in HTG1-1 have been combined to a single action (e.g., issues related to PKI management appear multiple times in the analysis but the set of actions are only addressed once). The findings are to be seen as recommendations for action by the SDOs involved in ITS and the SDOs are therefore invited to review them and to use the document as a basis for coordinated work that implements the recommendations and passes them to the ITS industry.

Specification of mechanisms should include the following as appropriate:

- Specification of PDUs exchanged between two communicating devices.
- Specification of processing on particular devices.
- Specification of abstract interfaces (Service Access Points (SAPs) and primitives) to be used to allow entities on a particular device to access a service offered by that device.

Action	Summary of Action	Responsible Organization	Priority
HTG1-VOB-01-D-01	Harmonization of the means by which generation time is included in transmitted messages.	ETSI and SAE	High
HTG1-VOB-01-D-02	Harmonization of choice of signature scheme in Basic Safety/Cooperative Awareness messages (taking due account of performance, IPR and extensibility issues). A single global signature scheme is the intended output.	ETSI and SAE	High
HTG1-VOB-01-D-03	Harmonization of the location of signing within the stack. The aim is to ensure, as far as possible, single signature in the stack.	ETSI and SAE	High
HTG1-VOB-01-D-04	Provision of GeoNetworking risk analysis. NOTE: ETSI has already committed to extending the TVRA (ETSI TR 102 893) to address GeoNetworking and to identify measures to assure its security.	ETSI	High
HTG1-VOB-01-D-05	Message Signature Verification policy. The signature verification policy has an impact on consistency of user experience and also on performance of the ITS system.	ETSI and SAE	Low

Action	Summary of Action	Responsible Organization	Priority
HTG1-VOB-01-D-06	Harmonization of possible future changes to IEEE 1609.2. ETSI and IEEE should liaise and agree on possible changes to IEEE 1609.2. The intent is that as the common base for security mechanisms is IEEE 1609.2, all required capabilities should only be described in the IEEE document, leaving the application of the mechanisms to the ETSI/SAE harmonized standards. NOTE: This particularly addresses the draft work item at ETSI identified as DTS/ITS0050023 (ETSI TS 103 097). ETSI should not approve any divergence from 1609.2 unless IEEE 1609 also approves the changes and implements them.	ETSI and IEEE	High
HTG1-VOB-01-D-08	Certificate transfer policy. Specify a management message to allow different jurisdictions to have different certificate transfer policies and to transmit information about those policies.		Low
HTG1-VOB-01-I-01	Assure that all assertions in a single message can be signed by a single key.	ETSI and SAE	Medium

Action	Summary of Action	Responsible Organization	Priority
HTG1-VOB-02-I-01	Provision of reversible pseudonymity service. This shall include the following sub-actions: • Specification of protocol for reversible pseudonymity. ○ SDOs should solicit proposals from key stakeholders (including CAMP and C2C) and develop standards in collaboration with them. • Specification of conditions for reversible pseudonymity (considerations here include protection of privacy against insiders at the reversibility service). • Specification of certificate revocation information format for reversible pseudonyms.	ETSI and SAE, following input from stakeholders	High
HTG1-VOB-02-I-02	Pseudonym change interval and algorithm. Whilst the underlying mechanism for using pseudonymous certificates to sign messages is agreed upon, the details for pseudonym change interval and algorithm, which affects privacy, is not. Requirements for privacy need to be specified so that SDOs and system designers can ensure that standards support those requirements.	Non-SDO	High
	Define message protocols for exchange of pseudonym change policy (it may be possible to exchange such data by extension of the enrolment or authorization authority's capabilities as defined in ETSI TS 102 940).	SDO (ETSI)	Medium

Action	Summary of Action	Responsible Organization	Priority
HTG1-VOB-02-I-03	Definition of alert state. During an alert state, linkability of messages becomes critical to track the alerting event. Thus it should be possible to suspend the pseudonymity service when in this state. The definition of such states needs to be harmonized in order to harmonize the state machines.	SDO ETSI and SAE	Medium
HTG1-VOB-02-I-04	Synchronization of identifier change across stack. As any individual element of identifying data may be used to attack privacy, it is important to ensure that all identifying data transmitted by a station should be protected. The pseudonymity protection mechanism should operate in such a manner that all identifying data that can be changed is changed at the same time.	ETSI/ISO	Medium
HTG1-VOB-03-D-1	Geographic region encoding within Certificate. 1. Determine a data dictionary containing commonly used geographic regions, with their definition as a series of points and a compact identifier.	ETSI	High
	2. Specify management messages to be used to update this data dictionary from time to time as necessary.	ETSI	Low
HTG1-VOB-03-D-2	Permissions encoding and PSID value. Agree how permissions should be encoded in the ITS-AID/Message Set ID/port number approach. This should be done as part of the HTG2 message set harmonization between SAE and ETSI.	ETSI and SAE	High

Action	Summary of Action	Responsible Organization	Priority
HTG1-VOB-03-I-1	Service Specific Permissions. Specify SSP for CAM/BSM. This should be done as part of the HTG2 message set harmonization between SAE and ETSI.	ETSI and SAE	High
HTG1-IOB-02-I-1	Revocation vs. short-lived certificates. Create policy for when revocation should be used versus short-lived certificates (responsibility of governance bodies rather than SDOs).	Non-SDO	High
HTG1-IOB-02-I-2	Logging of vehicle-originating messages. Define to what extent and for what retention period RSUs and infrastructure are required and allowed to log incoming vehicle-originated messages. This is to give assurance of compliance to extant data retention regulations for both law enforcement and commercial purposes. NOTE: Legal guidance already exists though may not be sufficiently specific.	Non-SDO	Medium
HTG1-IVU-02-I-1	Encryption of messages in unicast sessions between infrastructure and ITS-S. Specify mechanisms to be used for provision of confidentiality assurance for messages of this type.	IEEE	Low
HTG1-IVU-03	Understand privacy requirements of these services.	Stakeholder organizations	Medium
	Generate standards that support these privacy requirements.	SDOs	Low

Action	Summary of Action	Responsible Organization	Priority
HTG1-SM-01-I-1	Key management – initialization policy/process. 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. It is essential to have advice from the PKI stakeholders on means to achieve such management (i.e., determine whether proprietary approaches to trust management are acceptable or whether a standardized approach is necessary).	Non-SDO	Medium
	• If a standardized approach is necessary, provide standards to support it, including standards that transition from proprietary approaches used in initial deployment to final, standardized approaches.	SDO	Medium
	• If standards are not necessary, determine whether there are minimum security requirements that should be enforced and (SDO) specify those.	Non-SDO	Medium
HTG1-SM-01-I-3	Definition of ITS PKI structure. Whilst the overall use of PKCs is defined in IEEE 1609.2 and its endorsement by ETSI, there is no definition of the structure of the PKI (or PKIs) that such mechanisms operate within. It is necessary to define the requirements for the PKI and to determine whether current standards meet the stated PKI requirements.	Non-SDO	High
	For individual applications, specify the actual PKI hierarchy to be used for instances of that application.	Non-SDO SDO	Medium

Action	Summary of Action	Responsible Organization	Priority
HTG1-SM-01-I-4	PKI management. Generate guidance on use of PKI. This may be jurisdiction-specific. Provide guidance on managing transitions between regions with different policies. This activity has to consider a number of actions for the management of the PKI including: • HTG1-SM-01-I-5 Specification of protocol for addition of root certificate authorities. • HTG1-SM-02-I-1 Specification of protocol for obtaining new pseudonyms when roaming. • HTG1-SM-02-I-1 Specification of protocol for updating long-term certificates.	Non-SDO	High
HTG1-SM-02-I-1	Specification of protocol for obtaining new pseudonyms when roaming.	ETSI	Medium
HTG1-SM-03-I-1	Specification of protocol for updating long-term certificates.	IEEE	High
HTG1-SM-04-I-1	Specify reversible pseudonymity protocol.	IEEE, following input from stakeholder organizations	High
HTG1-SM-04-I-2	Specification of conditions for reversible pseudonymity.	Non-SDO	
HTG1-SM-04-I-3	Protocol to notify ITS-S owner of privacy policy changes.	ETSI Non-SDO	Medium

Action	Summary of Action	Responsible Organization	Priority
HTG1-SM-05-I-1	Specification of certificate revocation distribution process. Specify how CRLs may be distributed to those ITS-S that do not have frequent data connectivity to the certificate management service.	ETSI/IEEE, following completion of appropriate research.	Medium
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).	ETSI and SAE, following completion of appropriate research.	High
HTG1-SM-07-I-2	Specification of 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).	ETSI and SAE	High
HTG1-LTCS-01	Public-key based mechanisms for LTCS.	IEEE	Low
HTG1-LTCS-02	Review EFC standards to evaluate associated privacy risks.	ISO/CEN/IEEE	High
HTG1-LTCS-03	Guidelines for privacy against eavesdropping in LTCS (specifically EFC).	Non-SDO/ISO/CEN	Medium
HTG1-LNCS-01	Public-key based mechanisms for LNCS.	IEEE	Low
HTG1-LNCS-02	Symmetric key mechanism for LNCS.	SDO	Low
HTG1-LNCS-03	Liaise with IETF as necessary.	SDO	Low
HTG1-LNCS-04	Guidelines for privacy against eavesdropping in LNCS.	Non-SDO/ISO/CEN	Medium
HTG1-MRS-01-1	Specify security and operational requirements for multi-RSU sessions.	Non-SDO/Stakeholders	Low

Action	Summary of Action	Responsible Organization	Priority
HTG1-MRS-01-2	Use of V-HIP for multi-RSU sessions.	IEEE/ETSI	Low
HTG1-MRS-01-3	Standardized interfaces for secure sessions handoff.	ETSI	Low
HTG1-Adv-01-I-01	Produce a TVRA for service advertisements. This would determine freshness requirements. Specify maximum lifetimes for acceptable service advertisements based on the TVRA. Specify verification policy for service advertisements based on the TVRA.	SDO	High
HTG1-Adv-01-I-02	Specify a generic mechanism for initiating application or facilities layer secure sessions based on information within the service advertisement.	IEEE (for 1609) ISO	Medium
HTG1-Adv-01-I-03	Specify a mechanism for initiating network layer secure sessions based on information in the service advertisement.	ETSI	Medium
HTG1-Adv-01-I-03	Specify a mechanism for initiating MAC layer secure sessions using information in a service advertisement.	ETSI	Medium
HTG1-Adv-04-I-01	Maximum lifetimes for service advertisements based on TVRA.	ETSI/ISO/IEEE	Medium
HTG1-Adv-05-I-01	Verification policy for advertisements based on TVRA.	ETSI/ISO/IEEE	High
HTG1-Adv-02	Signed advertisement format based on TVRA.	ETSI/IEEE	High
HTG1-Adv-04	Certificate attachment interval/algorithm.	IEEE/ISO	Low
HTG1-LL-01	Security requirements for lower layers.	ETSI/stakeholder organizations	Low
HTG1-LL-02	Common set of parameters for lower layer security in IP communications for ITS.	ETSI	Low

Action	Summary of Action	Responsible Organization	Priority
HTG1-LL-03	Minimum security requirements for privacy in IP communications.	Non-SDO	High
	Mechanisms to provide privacy in IP communications to required level.	ETSI/IEEE	Medium
HTG1-LL-04	Determine whether layer 2 security mechanisms are necessary.	Non-SDO/stakeholder organizations	High
	Select mechanism.	IEEE	Medium
HTG1-MA-01-1	Create syntax for statement of resources on an ITS-S.	ETSI/ISO	Medium
HTG1-MA-01-2	Create policy for which applications may use restricted resources.	Non-SDO	Medium
HTG1-MA-01-3	Create process for approval of application use of resources on installation.	Non-SDO/ETSI/ISO	Medium
HTG1-MA-01-04	Create process for 1609.2 certificate request.	SDO	Medium
HTG1-MA-01-05	Create process for other certificate request.	SDO	Medium
HTG1-MA-02-01	Determine requirements for privacy when ITS-S are running multiple applications.	Non-SDO /ETSI	Medium
HTG1-MA-02-2	Specify mechanisms for privacy protections.	ETSI/ISO	Medium
HTG1-MA-03-1	Determine whether minimum security requirements for protection against malware are necessary.	Non-SDO	Medium
HTG1-MA-03-2	Create specification against which implementations may make conformance claims for malware protection level (at a requirements level).	SDO	Medium
HTG1-MA-03-3	Determine whether specifications for mechanisms to implement malware protection should be standardized.	Non-SDO	Medium
HTG1-MA-03-4	Create specification for malware protection mechanisms if necessary.	SDO	Low

Action	Summary of Action	Responsible Organization	Priority
HTG1-PPS-01-1	Create specifications for level of platform security.	ETSI/ISO	High
HTG1-PPS-01-2	Create minimum standards for platform security for platforms running particular applications.	Non-SDO/ETSI/SAE	High
HTG1-PPS-02	Statement of platform capabilities to CA.	ETSI/IEEE	High
HTG1-PPS-03	Statement of platform capabilities to application.	ETSI/ISO	Low
HTG1-PPS-04	Minimum security and performance requirements for secure firmware upgrade.	Non-SDO	Medium
HTG1-PPS-05	Define mechanisms for remote management of stations.	IEEE/ETSI/ISO	Medium
HTG1-Fut-01-1	Define mechanisms for upgrading implementations of 1609.2 security to use new algorithms.	IEEE	Medium
HTG1-Fut-01-1	Define mechanisms for upgrading implementations of 1609.2 security to use new algorithms.	IEEE	Medium
HTG1-Fut-01-2	Guidance on appropriate hardware support.	Non-SDO	Medium
HTG1-Fut-01-3	Guidance on satisfactory replacement algorithms.	Non-SDO/ETSI	Medium
HTG1-Fut-01-1	Define mechanisms for upgrading implementations of 1609.2 security to use new algorithms.	IEEE	Medium
HTG1-Fut-02-1	Define mechanisms for upgrading implementations of non-1609.2 security to use new algorithms.	IEEE	Medium
HTG1-Fut-02-2	Guidance on appropriate hardware support for non-1609.2 security.	Non-SDO	Medium
HTG1-Fut-02-3	Guidance on satisfactory replacement algorithms for non-1609.2 security.	Non-SDO/ETSI	Medium

2 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 in their titles indicate documents that 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.

2.1 ISO

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.2 CEN

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

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

2.3 ETSI

[24] 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)

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

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

[27] ETSI 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

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

[29] 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

[30] 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

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

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

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

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

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

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

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

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

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

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

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

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

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

2.4 IEEE

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

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

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

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

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

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

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

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

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

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

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

2.5 Regulations

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

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

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

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

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

2.6 Testing

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

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

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

[63] ETSI TS 102 868 V1.1.1 (2011-03), Intelligent Transport Systems (ITS); Testing; Conformance test specification for Co-operative Awareness Messages (CAM);
Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) proforma
Part 2: Test Suite Structure and Test Purposes (TSS&TP)
Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)

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

2.7 Other references

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

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

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

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

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

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

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

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

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

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

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

[76] 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

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

[78] 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.

[79] 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.

[80] 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.

[81] 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).

[82] 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

[83] 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

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

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

3 Introduction

3.1 Scope

This document promotes the goals of, and is a product of the project methodology described in, document [65]. It is based on the interoperability topics identified and described in [66], which identifies differences among, and gaps in, ITS standards developed in ETSI, ISO/CEN and IEEE. For some of these topics, a potential for increased harmonization has been identified. This document suggests technical topics for consideration by the various SDOs toward the goal of completeness of and increasing harmonization among the relevant standards.

3.2 Structure of the document

This document has the following structure:

- Section 2 contains a list of references.
- This section (3) provides an introduction and a summary.
- Section 4 defines terminology.
- Sections 5 through to 16 list topics in interoperability between the current standards, as introduced in [66].

For each topic in sections 5 through to 16, the document identifies a high-level objective for harmonization in this area, followed by a brief discussion of the subject. The full coverage of the topic is found in [66]. Where appropriate, suggestions are offered to the appropriate SDOs, including an identification of needed coordination among SDOs, followed by an estimate of the priority (high, medium, low) of the topic. The priority is a subjective estimate of the impact that the issue has to interoperability. A high-priority issue is considered critical to harmonization; a low-priority issue is considered to have little or no impact (e.g., because it relates to an optional or little-used feature).

In some cases, this document recommends that SDOs should specify mechanisms to provide a particular security-related service. Specification of mechanisms should include the following as appropriate:

- Specification of PDUs exchanged between two communicating devices.
- Specification of processing on particular devices.
- Specification of abstract interfaces (Service Access Points (SAPs) and primitives) to be used to allow entities on a particular device to access a service offered by that device.

This document uses HTG1-1, “Security Status,” as a starting point. For each interoperability issue identified in HTG1-1, this document provides feedback in the form of next actions to be taken. Where the action can logically be taken by a particular SDO, this document identifies the appropriate SDO. This SDO identification is not intended to be dispositive but simply our best expert guess as to the SDO that is best placed to carry out the work. Additionally, because security sometimes requires regulation or policy as well as technology, this document identifies areas where policy or regulatory action can help improve security. Where this is done, the document identifies feedback to SDOs with (SDOs) and feedback to other organizations with (Non-SDO).

4 Glossary

Table 1 below lists acronyms used in documents produced by the HTG1&3 teams.

Table 1: Acronyms

Acronym	Meaning	Reference
API	Application Programming Interface	[7]
BRAN	Broadband Radio Access Networks	[59]
BSMD	Bounded Secured Managed Domain	[7]
BSS	Basic Service Set	[48]
BTP	Basic Transport Protocol	[24]
CCH	Control Channel	[22, 27, 51]
CEN	Comité Européen de Normalisation	http://www.cen.eu
CI	Communication Interface	[9]
CIP	Communication Interface Parameter	[16]
C-ITS	Cooperative ITS	[7, 19]
CTX	Context message	[14]
DCC	Distributed Congestion Control	[29]
DIS	Draft International Standard	ISO
DSAP	Destination SAP address	[45]
EDCA	Enhanced Distributed Channel Access	[48]
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/
FNTP	Fast Networking & Transport layer Protocol	[16]
From DS	Field in the IEEE Std 802.11 MAC header	[48]
FSAP	Fast Service Advertisement Protocol	[14]

Acronym	Meaning	Reference
GeoNet	Name of an EU research project	www.geonet-project.eu
GeoNetworking	Name of a protocol developed at ETSI based on the results from GeoNet	[24]
HTG	Harmonization Task Group	-
IANA	Internet Assigned Numbers Authority	http://www.iana.org
IEEE	Institute of Electrical and Electronics Engineers	http://www.ieee.org
IETF	Internet Engineering Task Force	http://www.ietf.org
IP	Internet Protocol	IETF
IPv6	Version 6 of the Internet Protocol	IETF
ISO	International Standards Organization	http://www.iso.org
ITS	Intelligent Transport Systems (CEN, ETSI, ISO) Intelligent Transportation Systems (US)	[7]
ITS-AID	ITS Application Identifier	[32]
ITS-S	ITS Station	[7]
LLC	Logical Link Control	[44]
MAC	Medium Access Control	[44]
MIB	Management Information Base	[44]
OSI	Open Systems Interconnection	[20]
PDU	Protocol Data Unit	[44]
PSID	Provider Service Identifier	[51]
SACH	Service Advertisement Channel	[22]
SAE	Society of Automotive Engineers	http://www.sae.org/
SAM	Service Advertisement Message	[14]
SAP	Service Access Point	[13]
SCH	Service Channel	[22, 51, 27]

Acronym	Meaning	Reference
SCHx	Service Channel number x	[27]
SDO	Standards Development Organization	general
SDU	Service Data Unit	[44]
SfCH	Safety Channel	[22]
SNAP	Sub-Network Access Protocol	[44]
SNMP	Simple Network Management Protocol	IETF, [44]
SSAP	Source SAP address	[45]
SSP	Service specific permissions From 802.11:2012 subscription service provider (SSP): An organization (operator) offering connection to network services, perhaps for a fee. From 1609.2 service specific permissions (SSP): A field that encodes permissions relevant to a particular certificate holder.	[50]
Std	Standard	IEEE
TDMC	Time Domain Multiple Channel switching	-
To DS	Bit field in the IEEE Std 802.11 MAC header	[48]
TS	Technical Specification	ETSI/ISO
U-NII	Unlicensed National Information Infrastructure	**[57]**
US	United States	general
VCI	Virtual Communication Interface	[9]
VSA	Vendor Specific Action	[48]
WAVE	Wireless Access in Vehicular Environments	[49, 50, 51, 52, 53, 54]
WG	Working Group	general
WSA	WAVE Service Advertisement	[51]
WSMP	WAVE Short Message Protocol	[51]

Acronym	Meaning	Reference
XID	eXchange IDentification IEEE Std 802.2 LLC service	[45]

5 Vehicle-Originating Broadcast

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

5.1.1 Objective

Identical data structures and encoding for messages with identical security requirements.

5.1.2 Discussion

- **HTG1-VOB-01-D-01**: **Inclusion of generation time**. ETSI and SAE use the IEEE 1609.2 generation time field inconsistently in the BSM/CAM.
- **HTG1-VOB-01-D-02: Choice of signing algorithm**. SAE uses implicit certificates and ECDSA-256; ETSI uses explicit certificates and ECDSA-224.
- **HTG1-VOB-01-D-03**: **Cross-layer issues in signing**. ETSI currently signs at the facilities layer, SAE signs 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 fields, the two approaches are inconsistent.
- **HTG1-VOB-01-D-04: Geonetworking**: If geonetworking is built into the network stack, it introduces additional security concerns which have not been addressed in current standards (drafts), and causes a divergence between SDO approaches.
- **HTG1-VOB-01-D-05**: **Message Signature Verification policy**: Both ETSI and SAE recommend verifying messages that the receiver makes use of. However, in the ETSI model, all messages are made use of because they are used to update the local dynamic map. An ETSI ITS-S will therefore need to support greater verification throughput than an ITS-S restricted to SAE active safety applications. This is not an interoperability issue, except that an ITS-S that supports low rates of verification will not be able to implement more sophisticated uses of the LDM.
- **HTG1-VOB-01-D-06**: **Modification of signed data format**: ETSI have a WI on secure message formats that would lead to divergence from 1609.2.
- **HTG1-VOB-01-D-07**: **Certificate transfer**: If different jurisdictions have different certificate transfer policies, it would be helpful for there to be a management message specifying these policies.
- **HTG1-VOB-01-I-01**: **Ability to assert all permissions**: HTG1-1 provides three alternatives[1] for ensuring that permissions can be asserted cleanly.

5.1.3 Actions

- **HTG1-VOB-01-D-01**: **Inclusion of generation time**. As part of harmonization of CAM and BSM, ETSI WG1 and SAE should synchronize on the correct use of time. Note that if the 1609.2 generation time field is always present in a valid CAM or BSM, there is no need to include a separate generation time field within the application PDU itself, but in the situation

[1] Option (a) The message sets could be defined so that a single legal authority will always be able to grant authorization for all possible messages; (b) 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; (c) 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.

where the timestamp is used for security purposes, e.g., replay protection, the semantics of the timestamp needs to be clearly described, no matter where it is added to the packet.

- **HTG1-VOB-01-D-02: Choice of cryptographic signing mechanism**. SAE and ETSI WG1 should coordinate on whether concerns about licensing outweigh the technical advantages and implement a decision that favours a single approach (implicit or explicit certificates) and algorithm.
- **HTG1-VOB-01-D-03**: **Cross-layer issues in signing**. As part of harmonization of CAM and BSM, ETSI WG1 and SAE should coordinate with ETSI WG5 and 1609.2 to ensure a common understanding of the correct location of signing within the stack.
- **HTG1-VOB-01-D-04: Geonetworking**: ETSI needs to evaluate the use of geonetworking and its security requirements. Other SDOs should evaluate whether geonetworking should be included in their standards.
- **HTG1-VOB-01-D-05**: **Message Signature Verification policy**: SAE and ETSI ITS WG1 should liaise on signature verification policy to ensure consistency of user experience where appropriate.
- **HTG1-VOB-01-D-06**: **Modification of signed data format**: ETSI and IEEE should liaise on possible changes. ETSI should not approve any divergence from 1609.2 unless IEEE 1609 also approve the changes and implement them.
- **HTG1-VOB-01-D-07**: **Certificate transfer**: Authorities in the PKI structures (peers if distinct PKI structures are supported for different domains) should ensure that policy information related to certificate transfer can be exchanged with retention of semantic and syntactic content.
- **HTG1-VOB-01-I-01**: **Ability to assert all permissions**: (SDOs): ETSI WG1 and SAE should be advised to bear the discussion of HTG1-1 in mind when determining message contents. Both groups should review current message sets to ensure that they support single authorities. (Non-SDO): Organizations responsible for regulations governing authorization should try where possible to allow a single CA to issue certificates authorizing the full range of permissions

5.1.4 Priority

- D-01 to D-04, D-06, D-07: High
- I-01: Medium
- D-05, D-08: Low

5.2 HTG1-VOB-02: Pseudonymity service

5.2.1 Objectives

Common understanding of whether requirements for pseudonymity are the same or different in the different jurisdictions. Where requirements are the same, common mechanisms are used to achieve them. Understanding of implications of moving between jurisdictions that have different privacy policies and requirements.

5.2.2 Discussion

- **HTG1-VOB-02-I-01 Reversible pseudonymity**: There is no standard or proposed standard certificate format that allows for reversible pseudonymity. The different research projects in

Europe and the US have different approaches to privacy against the certificate service provider.

- **HTG1-VOB-02-I-02 pseudonym change interval and algorithm**: It is not understood whether the requirements for pseudonym change and numbers of pseudonyms differ between jurisdictions. Long pseudonym periods increase the ability of law enforcement to track vehicles. If there is a requirement for properly constituted authorities to be able to dictate pseudonym policy, and to change it from time to time or when vehicles travel across borders, then this needs to be agreed upon in short order so that appropriate support mechanisms can be defined. Possible considerations include:
    - Should ITS-S (owners/users) be notified if pseudonym change policy changes?
    - The C2C approach (multiple simultaneously valid certs) supports flexible change policies better than the CAMP approach. On the other hand, the CAMP approach locks in a highly privacy-preserving approach. These two benefits should be balanced.
- **HTG1-VOB-02-I-03 alert state**: 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 noting the fact that pseudonyms may be application-specific.
- **HTG1-VOB-02-I-04 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 changes and MAC address changes 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.

5.2.3 Actions

- **HTG1-VOB-02-I-01 Reversible pseudonymity**: Relevant stakeholders should determine the appropriate level of privacy against the certificate service provider (i.e., the ability available for (a) an individual insider or (b) the service provider as a whole to discover PII about a customer), where possible favouring privacy by design. This affects certificate management data structures and protocols. Once the research projects are in synch on requirements, they should propose a common set of possible solutions to SDOs that satisfy these requirements and from which a consistent and interoperable solution should be derived.
- **HTG1-VOB-02-I-02 pseudonym change interval and algorithm**: (Non-SDO) Agree whether there is a need for authorities to transmit and modify pseudonym change policy. (SDOs) Define message protocols for this. Ensure that the pseudonym issuance mechanisms support the required range of pseudonym change policies.
- **HTG1-VOB-02-I-03 alert state**: SDOs should produce a pseudonymity service that respects the ability of individual applications to note an alert state. As discussed in section 14 this has a direct impact on privacy for shared resources if there is no synchronization between the applications.
- **HTG1-VOB-02-I-04 synchronization of identifier changes**: ETSI should continue to develop standards that support synchronization of identifier changes, and other SDOs should use the ETSI results.

5.2.4 Priority

- 01, 02: high. These are issues that need to be resolved before there is a significant deployed base of personal ITS-S.
- 03, 04: medium, assuming that privacy for multi-application devices is not a high priority for initial deployment. If this assumption is wrong, the priority of these items is high.

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

5.3.1 Objective

There is a consistent set of rules and standards governing permissions encoding within signed messages.

5.3.2 Discussion

See HTG1-1.

5.3.3 Actions

- **HTG1-VOB-03-D-1: Geographic region encoding**:
  - 1. Determine a data dictionary containing commonly used geographic regions, with their definition as a series of points and a compact identifier.
  - 2. Specify management messages to be used to update this data dictionary from time to time as necessary.
    The natural SDO for this action is ETSI.
- **HTG1-VOB-03-D-2: Permissions encoding and PSID value**: Agree how permissions should be encoded in the ITS-AID/Message Set ID/port number approach. This should be done as part of the HTG2 message set harmonization between SAE and ETSI WG1.
- **HTG1-VOB-03-I-1: Service Specific Permissions**: Specify SSP for CAM/BSM. This should be done as part of the HTG2 message set harmonization between SAE and ETSI WG1.

5.3.4 Priority

- D-1.1: High
- D-1.2: Low (dictionary can be updated by firmware update and other methods)
- D-2: High
- I-1: High

6 Infrastructure originating broadcast

6.1 HTG1-IOB-02: Pseudonymity service

6.1.1 Objective

Establish harmonized policy for pseudonymity service, where necessary.

6.1.2 Discussion

See HTG1-1.

6.1.3 Actions

- **HTG1-IOB-02-I-1 Revocation vs. short-lived certificates**: (Non-SDO) Create policy for when revocation should be used vs. short-lived certificates (responsibility of governance bodies rather than SDOs).
- **HTG1-IOB-02-I-2 Logging of vehicle-originating messages**: (Non-SDO) Define to what extent and retention period RSUs and infrastructure are required and allowed to log incoming vehicle-originated messages. (responsibility of governance bodies rather than SDOs; legal guidance already exists though may not be sufficiently specific).

6.1.4 Priority

- **HTG1-IOB-02-I-1.1**: High
- **HTG1-IOB-02-I-1.2**: Medium
- **HTG1-IOB-02-I-2**: Medium

7 Infrastructure-vehicle unicast

7.1 HTG1-IVU-02: Encryption

7.1.1 Objective

Specify limited but complete set of encryption services to be used by IVU applications as necessary.

7.1.2 Discussion

See HTG1-1 for background. For encryption services to be effective, communicating parties must agree on an encryption key. This may be public-key or symmetric cryptography and may be generated by one party or agreed upon using a key agreement protocol. 1609.2 defines only public-key cryptography. The CAMP extensions provide an extension of 1609.2 techniques to symmetric cryptography, but they have been designed specifically for security management and may not be suitable for general use. The stakeholders of these applications have not been aggressive in making SDOs aware of the encryption requirements and as such, standardization in this area is far from mature.

7.1.3 Actions

- **HTG1-IVU-02-I-1 Encryption**: Specify a limited set of shared mechanisms that may be used for confidentiality for messages of this type.

7.1.4 Priority

To be determined by application stakeholders. In the absence of strong championing of this use case, priority is low.

7.2 HTG1-IVU-03: Pseudonymity Service

7.2.1 Objective

Understand privacy requirements of this service, for example, if RSU intends to send unicast response to an OBU that has since changed its identifiers.

7.2.2 Discussion

See HTG1-1 and Objective section above.

7.2.3 Actions

(Non-SDO) Application stakeholders should provide use cases to SDOs (particularly ETSI ITS WG1 and SAE) to allow analysis of privacy requirements.

7.2.4 Priority

To be determined by application stakeholders. In the absence of strong championing of this use case, priority is low.

8 Security Management for IOB and VOB

8.1 HTG1-SM-01: Adding root certificates

8.1.1 Objective

Specify protocols to be used by the Trust Management functional entity(ies) to update root certificates.

8.1.2 Discussion

See HTG1-1 for background. It is possible that manufacturers of devices may develop a, or deploy an existing, proprietary means of adding root certificates during initial rollouts. This may inhibit the development of a harmonized solution to updating root certs.

8.1.3 Actions

- **HTG1-SM-01-I-1 Key management:**
    1. (Non-SDO) Determine whether proprietary or non-harmonized approaches to trust management are acceptable or whether a standardized approach is necessary.
    2. (SDO) If a standardized approach is necessary, provide standards to support it, including standards that transition from proprietary approaches used in initial deployment to final, standardized approaches.
    3. (Non-SDO) If standards are not necessary, determine whether there are minimum performance requirements that should be enforced (e.g., time to distribute a new root cert and depend on its deployment), and (SDO) specify those.
- **HTG1-SM-01-I-2 ITS-S initialization**: See sections 14.1 and 15.
- **HTG1-SM-01-I-3 PKI structure**:
    1. (Non-SDO) Determine whether current standards meet a reasonable range of PKI requirements
    2. (SDO and Non-SDO) For individual applications, specify the actual PKI hierarchy to be used for instances of that application.
- **HTG1-SM-01-I-4 PKI management**: Generate guidance on operation of PKI. This may be jurisdiction-specific. Provide guidance on managing transitions between regions with different policies (see below).
- **HTG1-SM-01-I-5 Specification of protocol for addition of root certificate authorities:** See HTG1-SM-01-I-1 above.

8.1.4 Priority

- **HTG1-SM-01-I-1 Key management:**
    1. Medium
    2. Medium
    3. Medium
- **HTG1-SM-01-I-3 PKI structure**:
    1. High
    2. High, but not an SDO responsibility; more a responsibility of system architects for specific systems.

- **HTG1-SM-01-I-4 PKI management**: Not an SDO responsibility, more a responsibility of system architects for specific systems. Jurisdiction specific. High, but can perhaps survive a somewhat ad hoc approach during initial deployment.

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

8.2.1 Objective

Devices that roam between jurisdictions can be trusted in those new jurisdictions. See HTG1&3-1, section E for more details on border crossing scenarios and issues.

8.2.2 Discussion

The priority of this can be somewhat reduced by ensuring harmonization of security mechanisms within regions with many land borders (e.g., within the EU).

8.2.3 Actions

HTG1-SM-02-I-1 Specification of protocol for obtaining new pseudonyms when roaming: (Non-SDO) Determine responsibility of pseudonym provider/authentication authority for specific areas. (SDO) protocol needs to be specified. ETSI is a natural SDO for this task.

8.2.4 Priority

Medium.

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

8.3.1 Objective

Specify protocol for updating long-term certificates.

8.3.2 Discussion

1609.2 specifies a protocol for requesting new long-term certificates but not for demonstrating that a requesting ITS-S or application is still trustworthy.

If devices never renew long-term certificates (i.e., long-term certificates are *extremely* long term), no protocol is necessary. However, see discussion of future-proofing and potential cryptographic algorithm failures.

8.3.3 Actions

HTG1-SM-03-I-1 Specification of protocol for updating long-term certificates: protocol needs to be specified.

8.3.4 Priority

High: must be supported by devices when first deployed.

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

8.4.1 Objective

Specify mechanisms to support resolution of pseudonyms and conditions that must obtain to allow resolution.

8.4.2 Discussion

Both CAMP and C2C have put forward proposals in this area.

8.4.3 Actions

- **HTG1-SM-04-I-1 Specification of protocol for reversible pseudonymity:** SDOs should agree on a protocol, derived from those proposed by CAMP and C2C. This agreement should be reached in collaboration with CAMP and C2C as well as other stakeholders.
- **HTG1-SM-04-I-2 Specification of conditions for reversible pseudonymity**: (Non-SDO) Whilst this is jurisdiction-specific, technical protections may need to be harmonized to enable roaming operation between jurisdictions.
- **HTG1-SM-04-I-3 Protocol to notify ITS-S owner if privacy policy changes**: (Non-SDO) determine if this is necessary; (SDO) Specify this.

8.4.4 Priority

- **HTG1-SM-04-I-1 Specification of protocol for reversible pseudonymity:** High: must be known to CAs before initial deployment.
- **HTG1-SM-04-I-2 Specification of conditions for reversible pseudonymity:** High: Authorities must know the legal framework within which they are operating.
- **HTG1-SM-04-I-3 Protocol to notify ITS-S owner if privacy policy changes:** Medium: full understanding of requirements of this protocol will likely take time to emerge.

8.5 HTG1-SM-05: Revocation and distribution of revocation lists.

8.5.1 Objective

Specify CRL formats that support revocation of pseudonyms, when one vehicle owns multiple pseudonyms. Specify mechanisms for distribution of revocation lists.

8.5.2 Discussion

CAMP has put forward proposals for revocation list. C2C proposes to avoid over-the-air revocation lists. Neither has proposed a fully fleshed-out model for distribution. Theoretical/research discussions have included epidemic distribution/fountain codes, etc.

8.5.3 Actions

- **HTG1-SM-05-I-1 Specification of certificate revocation information format for reversible pseudonyms:** As described. Requires completion of HTG1-SM-04-I-1 Specification of protocol for reversible pseudonymity.
- **HTG1-SM-05-I-1 Specification of certificate revocation distribution process:** Specify how CRLs may be distributed, especially to those ITS-S that do not have frequent data connectivity to the certificate management service.

8.5.4 Priority

- **HTG1-SM-05-I-1 Specification of certificate revocation information format for reversible pseudonyms:** High
- **HTG1-SM-05-I-1 Specification of certificate revocation distribution process:** Medium: if initial deployment devices do not support all CRL distribution mechanisms, it is unlikely to cause a showstopper-level threat to the system.

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

See HTG1-SM-01 for full discussion.

8.7 HTG1-SM-07: Misbehavior reporting

8.7.1 Objective

Specify misbehavior report formats, misbehavior detection algorithms, and revocation process.

8.7.2 Discussion

Still the subject of active research; not very mature at all in the standards area.

8.7.3 Actions

- **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). This should be addressed by the SDOs in close collaboration with industry to ensure the minimum set of standards is provided.
- **HTG1-SM-07-I-2 Specification of 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).

8.7.4 Priority

High.

8.8 HTG1-SM-08: Bootstrap

See sections 13 and 14 for discussion.

9 Local Time-Critical Sessions

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

9.1.1 Objective

Applications based on local time-critical sessions use security mechanisms from a small and well-understood set.

9.1.2 Discussion

The natural example of a local time-critical session is tolling/Electronic Fee Collection (EFC), but it is outside the scope of this HTG to propose security mechanisms for EFC. EFC security mechanisms are currently the only standardized security mechanisms specifically designed for local time-critical sessions. These mechanisms are based on symmetric cryptography and require a high level of physical and system security on the infrastructure node. These mechanisms may be suitable for reuse by other applications that fit the same model (i.e., their deployers are willing to provide that high level of security on infrastructure nodes)

SDOs may also want to consider developing a set of security mechanisms based on public-key cryptography for local time-critical sessions, as these may allow more flexible deployment models. Developers of applications that fit this model should be encouraged to provide requirements to SDOs, or to develop solutions and then use those solutions as a basis for standardization.

As discussed in HTG1-Adv-01, secure sessions could potentially be established more efficiently if they use information from service advertisements to initiate the cryptographic handshake. Note however that applications should not be required to have their sessions be initiated via service advertisements in order to obtain communications security.

9.1.3 Actions

1. SDOs may consider developing a public key-based security mechanism suitable for these applications. This has been a “future work item” within IEEE 1609.2 for some time.
2. EFC standards should be reviewed to ensure that they do not maintain identifiers between sessions as noted in HTG1-1, section 9.9.
3. An appropriate SDO should develop guidelines for privacy against eavesdropping in EFC, for use by future standards. This seems a natural task for ISO/CEN.

9.1.4 Priority

1. Low
2. High
3. Medium

9.2 HTG1-LTCS-02: Privacy

9.2.1 Objective

Determine requirements for privacy attacks based on responses to service advertisements; if standardization is necessary, provide it.

9.2.2 Discussion

See HTG1-1.

9.2.3 Actions

See HTG1-1.

9.2.4 Priority

Medium.

10 Local Non-Time-Critical Session applications

10.1 HTG1-LNTCS-01: Security and security management

10.1.1 Objective

Applications based on local time-critical sessions use security mechanisms from a small and well-understood set.

10.1.2 Discussion

The natural example of a local non-time-critical session application is probe data collection. No security mechanisms are currently standardized for probe data collection or other local non-time-critical session applications. It is conceivable that there could be both symmetric and public-key mechanisms. SDOs should seek input from application stakeholders to determine requirements. Appropriate security mechanisms could include mechanisms already standardized on the Internet, potentially modified if necessary to include 1609.2 certificates.

As discussed in HTG1-Adv-01, secure sessions could potentially be established more efficiently if they use information from service advertisements to initiate the cryptographic handshake. Note however that applications should not be required to have their sessions be initiated via service advertisements in order to obtain communications security.

10.1.3 Actions

1. SDOs may consider developing a public key-based security mechanism suitable for these applications. This has been a future work item within IEEE 1609.2 for some time.
2. SDOs may consider developing a symmetric cryptography-based security mechanism suitable for these applications.
3. If existing internet mechanisms are to be modified for use in the ITS settings, ITS SDOs should liaise with the IETF.
4. An appropriate SDO should develop guidelines for privacy against eavesdropping in LNTCS applications, for use by future standards.

10.1.4 Priority

1. Low
2. Low
3. Low (cannot be higher priority than 1 and 2)
4. Medium

11 Multi-RSU Session: applications and security management

11.1.1 Objective

Provide a standardized mechanism to support secure, privacy-preserving session handoff between RSEs acting as access points.

11.1.2 Discussion

As discussed in HTG1-1, a secure session handoff mechanism will provide unlinkability between encounters with access points as well as providing communications security services for data within the session.

NEMO and HIP are candidate solutions, as is V-HIP, the HIP variant that was developed for use in VIIC PoC. It is not clear how important session handoff over 5.9 GHz will be in deployment, as ITS-S that require this facility may have other data connections that are better suited to large data exchanges.

Note that if ITS-S have multiple communication media, there must be an unambiguous way to ensure that applications get the security services that they expect from the medium being used. See 13.1 for further discussion.

11.1.3 Actions

1. Fully specify security and operational requirements.
2. Consider using V-HIP as a basis for secure session handoff. This work naturally belongs either in the IPv6 work done within ETSI or within 1609.2 where WG members have experience with V-HIP.
3. Standardize interfaces for initialization of secure session handoff.

11.1.4 Priority

Low.

12 Advertisements

12.1 HTG1-Adv-01: Communications security services and freshness requirements

12.1.1 Objective

Ensure that the communications security requirements for service advertisements are well understood.

12.1.2 Discussion

1609.2 provides security mechanisms for service advertisements but little analysis outside an informative Annex. [36] does not address security requirements. These should be reviewed and finalized.

A mechanism for initiating secure sessions based on service advertisements could potentially be used by local time-critical unicast or local non-time-critical unicast applications to reduce the number of exchanges needed for session establishment and should be considered. Note however that applications should not be required to have their sessions be initiated via service advertisement in order to obtain communications security.

HTG1-1 suggests that MAC layer secure sessions could be initiated using information from service advertisements.

12.1.3 Actions

1. **HTG1-Adv-01-I-01**: Produce a TVRA for service advertisements. This would determine freshness requirements. This work would naturally be done within ETSI as an extension to [36].
2. **HTG1-Adv-01-I-02**: Specify a generic mechanism for initiating application or facilities layer secure sessions based on information within the service advertisement. This work would naturally be done within ISO or IEEE and seems most suited to 1609 as 1609.3 specifies secure service advertisements and 1609.2 has an outstanding future work item to investigate this.
3. **HTG1-Adv-01-I-03**: Specify a mechanism for initiating network layer secure sessions based on information in the service advertisement. See 13.2 for further discussion.
4. **HTG1-Adv-01-I-03**: Specify a mechanism for initiating MAC layer secure sessions using information in a service advertisement. See 13.4 for further discussion.

12.1.4 Priority

1. High
2. Medium
3. See 13.2.
4. See 13.4.

12.2 HTG1-Adv-02: Signed datagram and certificate format

12.2.1 Objective

Harmonized specification of signed service advertisement.

12.2.2 Discussion

There is no divergence, so once requirements are established it should be straightforward to specify a format (or maintain the existing one defined via 1609.3 and 1609.2, if appropriate).

12.2.3 Actions

Specify format once requirements are established.

12.2.4 Priority

High.

12.3 HTG1-Adv-04: Pseudonym attachment interval/algorithm

12.3.1 Objective

Each domain (e.g., geographic region, ITS-S variant, ITS service variant) may have a pseudonym attachment algorithm appropriate to its channel capacity.

12.3.2 Discussion

Does not affect interoperability, but may affect congestion.

12.3.3 Actions

Propose pseudonym attachment algorithm(s) suitable for channel capacity of different ITS domains.

12.3.4 Priority

Low.

12.4 HTG1-Adv-05: Freshness requirements

HTG1-Adv-05-I-01: Specify maximum lifetimes for acceptable service advertisements based on the TVRA.

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

HTG1-Adv-06-I-01: Specify verification policy for service advertisements based on the TVRA.

13 Lower Layer

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

13.1.1 Objective

Standard interfaces within ITS-S that allow applications to specify the security services they need from the stack, so that any appropriate communications stack may be used.

13.1.2 Discussion

This is helpful to implementers, but not required for deployment.

13.1.3 Actions

Define primitives to specify security services. Probably an ETSI/ISO task.

13.1.4 Priority

Low.

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

13.2.1 Objective

Determine a common or restricted set of parameters for lower layer security in ITS communications

13.2.2 Discussion

Lower layer security, referring to security mechanisms applied to the link and physical layers of the OSI stack and in the context of ITS may be taken to mean the OSI network and transport layers too, will sometimes be to support communications with existing systems by applications that happen to be resident on the ITS stations. As such it may not be possible to restrict the parameters use, though it may be possible to give guidance as to parameters that new systems should use.

13.2.3 Actions

Determine a common or restricted set of parameters for lower layer security in ITS communications. Probably an ETSI task.

13.2.4 Priority

Low.

13.3 HTG1-LL-03: Networking layer (IP): privacy

13.3.1 Objective

Define mechanisms for changing IP address unlinkably. Determine whether there are minimum security requirements for IP address change for privacy such that an ITS-S must support that minimum security in order to claim conformance.

13.3.2 Discussion

See HTG1-1.

13.3.3 Actions

See objective. Minimum security requirements are the responsibility of governance bodies. The relevant governance bodies should be made aware of the need for minimum security requirements in this area. The mechanisms should be defined by a single standards body, with ETSI the natural candidate.

13.3.4 Priority

- Define mechanisms: Medium
- Determine minimum security requirements: High.

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

13.4.1 Objective

Determine whether Layer 2 security mechanisms need to be supported. If so, specify them.

13.4.2 Discussion

802.11 TGai has very active discussion of fast session setup and would be a natural place for a solution to come out of. However, it does not seem likely to produce a standard soon. ITS would need to select one of the candidates currently in TGai and bet on it, leading probably to inconsistencies with 802.11 and increased manufacturing expense. Also, as discussed in HTG1-1, the solution would need to be compatible with one MAC chipset listening on multiple MAC addresses simultaneously.

Note that this need not be implemented immediately or on all devices so long as applications can be informed of whether or not it is available so that applications that require it can be installed only on devices that support it.

13.4.3 Actions

See objective. IEEE probably the natural SDO for this as 802.11 is owned by IEEE.

13.4.4 Priority

- Determine whether necessary: High
- If necessary, select technique: Medium

14 Multiple applications and application management

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

14.1.1 Objective

- Create syntax for statement of resources available on an ITS-S that an application may wish to use.
- Create policy for which applications may use scarce resources such as (in its current form) the safety channel.
- Create process by which claims by an application may be validated when it is installed on a platform.
- Create process by which an instance of an application on an instance of a platform may demonstrate to a 1609.2 CA that it is entitled to use specific certificates.
- Create process by which an instance of an application on an instance of a platform may demonstrate to a different authority that it is entitled to use specific certificates.

14.1.2 Discussion

It will be necessary to make rapid progress in these areas to support the vision of mobile ITS-Ss that are general multi-purpose computing platforms like smartphones, that may be in vehicles or handheld, and that may have applications installed and uninstalled at the user's discretion. It is not necessary to make progress in this area if ITS-Ss are to be mainly directly installed in vehicles and with application installation controlled by the OEM. The opinion of the HTG is that system designers should plan for the first, more open case. This is particularly true in the US where the FCC licensing regulation permits effectively any vendor to market an OBE (including a portable device).

14.1.3 Actions

See objectives.

14.1.4 Priority

All medium.

14.2 HTG1-MA-02: Privacy

14.2.1 Objective

- Determine requirement to support privacy when running multiple applications:
  - Against eavesdroppers.
  - Against opt-in service providers.
- If requirement is determined to exist, determine technical mechanism to support privacy, for example multiple "virtual" network stacks or link-level encryption.
- Generate standards specifying these mechanisms.

14.2.2 Discussion

Privacy when running multiple applications may not be a requirement for initial deployment, particularly in an opt-in system, for a number of reasons: (a) in initial deployment, there may not be many applications beyond basic safety applications, so there is low risk that they will be used and will reveal PII; (b) early adopters may be considered to be more technically savvy and to have made a

conscious decision to trade off privacy and functionality; (c) early adopters may choose not to install privacy-revealing applications. This is therefore not a high-priority action item, but it is important for it to be on the agenda for SDOs.

14.2.3 Actions

See objective.

14.2.4 Priority

- Determine requirement: Medium
- Determine and standardize mechanisms: Medium if required.

14.3 HTG1-MA-03: Malware

14.3.1 Objective

- **HTG1-MA-03-1** Determine whether minimum security requirements for protection against malware are necessary. (Non-SDO) Medium
- **HTG1-MA-03-2** Create specification against which implementations may make conformance claims for malware protection level (at a requirements level). (SDO) Medium
- **HTG1-MA-03-3** Determine whether specifications for mechanisms to implement malware protection should be standardized. (Non-SDO) Medium
- **HTG1-MA-03-4** Create specification for malware protection mechanisms if necessary. (SDO) Low

14.3.2 Discussion

See [66].

14.3.3 Actions

See objective.

14.3.4 Priority

- **HTG1-MA-03-1** Determine whether minimum security requirements for protection against malware are necessary: Medium
- **HTG1-MA-03-2** Create specification against which implementations may make conformance claims for malware protection level (at a requirements level): Medium
- **HTG1-MA-03-3** Determine whether specifications for mechanisms to implement malware protection should be standardized: Medium
- **HTG1-MA-03-4** Create specification for malware protection mechanisms if necessary: Low

15 Physical and platform security

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

15.1.1 Objective

In line with HTG1-MA-01, create definitions of assurance levels for security of platforms that will have access to the safety channel and other scarce resources.

15.1.2 Discussion

As stated under HTG-MA-01, it will be necessary to make rapid progress in these areas to support the widest possible range of devices acting as mobile ITS-Ss. The opinion of the HTG is that system designers should actively work to support this vision.

15.1.3 Actions

See objectives.

15.1.4 Priority

High.

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

15.2.1 Objective

In line with HTG1-MA-01, create syntax and protocol and establish requirements for the mechanisms (e.g., , hardware enforcement or procedures) to allow ITS-S to make statements of platform capabilities to the CA, so that it can issue certificates for particular applications only to platforms that give assurance that the application will behave correctly.

15.2.2 Discussion

As stated under HTG-MA-01, it will be necessary to make rapid progress in these areas to support the widest possible range of devices acting as mobile ITS-Ss. The opinion of the HTG is that system designers should actively work to support this vision.

15.2.3 Actions

See objectives.

15.2.4 Priority

High.

15.3 HTG1-PPS-03: Statement of platform capabilities to application

15.3.1 Objective

Create master list of ITS-S platform resources that can be used by proprietary SDOs to allow devices that act as ITS-S to state their capabilities to applications.

15.3.2 Discussion

Although proprietary SDOs and vendors can produce their own statements of platform capabilities, a master list of resources created by ITS experts would increase the chance of the list of capabilities being complete and correct.

15.3.3 Actions
See objectives.

15.3.4 Priority
Low.

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

15.4.1 Objective
As part of defining minimum security and performance requirements for platform security, define minimum standards for secure firmware upgrade, to ensure that devices that start life in a secure configuration will always remain in a secure configuration. Minimum standards should include guidance as to procedures to be used if any cryptographic material used in firmware upgrade is compromised.

15.4.2 Discussion
This is more important for multi-application aftermarket-type ITS-S, which may receive firmware upgrades over the air, than for inbuilt OBEs which may only allow firmware changes through wired interfaces (and for which unauthorized firmware changes may void the warranty for the entire vehicle).

This may be jurisdiction-specific and may not be within the scope of an existing standards body.

15.4.3 Actions
See objectives.

15.4.4 Priority
Medium.

15.5 HTG1-PPS-05: Station management

15.5.1 Objective
Define security mechanisms for station management that are suitable for a range of cases, including the case where 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:

15.5.2 Discussion
Work items to address this are currently underway in ISO TC204 WG16 (ISO 24102-2) and IEEE (IEEE 1609.6).

15.5.3 Actions
See objectives.

15.5.4 Priority
Medium.

16 Future extensibility

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

16.1.1 Objective

- Define mechanisms by which implementations of 1609.2 security may be upgraded if existing cryptographic algorithms are broken.
- Given that within the 30-year lifetime of an initial vehicle, there is a good chance that quantum computers will be invented and break ECDSA, provide guidance as to how cryptographic/security hardware should be deployed to allow for migration to a subsequent system.

16.1.2 Discussion

Migration to a new cryptographic algorithm may be accomplished by similar means to secure firmware upgrade so long as cryptography is done in software/firmware rather than hardware. If security hardware is to be used, one needs to define a strategy for upgrading hardware.

Most likely new algorithms (e.g., NTRU—full disclosure, William Whyte works for the company that owns the patents covering NTRU—or other lattice—based crypto algorithms, or code-based algorithms such as McEliece) are faster than elliptic curve but have larger (in some cases much larger) public keys and ciphertexts. This suggests that it will not be necessary to have hardware support for their operations, but raises the question that channel capacity limitations will make it difficult to deploy these algorithms at all.

There are fewer acceptable quantum computing proof signature algorithms than encryption algorithms. Stakeholders in ITS should be urging NIST in the US and ECRYPT in the EU to encourage research into quantum computing proof signature algorithms. Additionally, the research should attempt to find ways to minimize channel use, perhaps by use of techniques such as TESLA.

16.1.3 Actions

- Guidance on algorithm migration via secure firmware upgrade: see discussion of secure firmware upgrade.
- Guidance on appropriate hardware support given the likelihood of a need to migrate: could perhaps come from an expert group such as ECRYPT or NIST (or potentially SAGE within ETSI).
- Research into satisfactory replacement algorithms: all stakeholders should be encouraging this, and encouraging the relevant bodies to produce regular reports on the state of the art in post-quantum computing.
- Research into hardware upgradeability (e.g., using reconfigurable hardware).
- Standardizing replacement algorithms: 1609.2 should take the lead on this when there is consensus in the appropriate technical field that suitable candidates exist.

16.1.4 Priority

- Guidance on algorithm migration via secure firmware upgrade: Medium
- Guidance on appropriate hardware support given the likelihood of a need to migrate: Medium

- Research into satisfactory replacement algorithms: High priority to encourage this as results might take some time to become usable.

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

Issues are the same as in HTG1-Fut-01, except that bodies other than 1609.2 will naturally take the lead in standardizing solutions.

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

New 1609.2 formats can be supported via secure firmware upgrade. See secure firmware upgrade for further discussion.

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

New formats for standards other than 1609.2 can be supported via secure firmware upgrade. See secure firmware upgrade for further discussion.