ETSI TS 103 096-2 V1.4.1 (2018-08)

Intelligent Transport Systems (ITS);
Testing;
Conformance test specifications for ITS Security;
Part 2: Test Suite Structure and Test Purposes (TSS & TP)

Reference

RTS/ITS-00543

Keywords

ITS, security, testing, TSS&TP

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Intelligent Transport Systems (ITS).

The present document is part 2 of a multi-part deliverable covering Conformance test specifications for ITS Security, as identified below:

Part 1: "Protocol Implementation Conformance Statement (PICS)";

Part 2: "Test Suite Structure and Test Purposes (TSS & TP)";

Part 3: "Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)".

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document provides the Test Suite Structure and Test Purposes (TSS & TP) for Security as defined in ETSI TS 103 097 [1] in accordance with the relevant guidance given in ISO/IEC 9646-7 [i.6].

The ISO standards for the methodology of conformance testing (ISO/IEC 9646-1 [i.3] and ISO/IEC 9646-2 [i.4]) as well as the ETSI rules for conformance testing (ETSI ETS 300 406 [i.7]) are used as a basis for the test methodology.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI TS 103 097 (V1.3.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".

[2] IEEE Std 1609.2™-2016: "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages", as amended by IEEE Std 1609.2a™-2017: " IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages - Amendment 1".

[3] ETSI TS 103 096-1 (V1.4.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)".

[4] ETSI TS 102 871-1 (V1.4.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma".

[5] United Nations Statistics Division: "Composition of Macro Geographical (Continental) Regions, Geographical Sub-Regions, and Selected Economic and Other Groupings".

NOTE: Available at http://unstats.un.org/unsd/methods/m49/m49regin.htm.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI EG 202 798 (V1.1.1): "Intelligent Transport Systems (ITS); Testing; Framework for conformance and interoperability testing".

[i.2] ETSI TS 102 965 (V1.3.1): "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration".

[i.3] ISO/IEC 9646-1 (1994): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 1: General concepts".

[i.4] ISO/IEC 9646-2 (1994): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 2: Abstract Test Suite specification".

[i.5] ISO/IEC 9646-6 (1994): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 6: Protocol profile test specification".

[i.6] ISO/IEC 9646-7 (1995): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 7: Implementation Conformance Statements".

[i.7] ETSI ETS 300 406 (1995): "Methods for testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in ETSI TS 103 097 [1], ETSI TS 102 965 [i.2], ISO/IEC 9646-6 [i.5] and ISO/IEC 9646-7 [i.6] apply.

3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AA	Authorization Authority
AID	Application Identifier
AID_CAM	ITS Application Identifier for CAM
AID_DENM	Application Identifier for DENM
AID_GN	Application Identifier for general GeoNetworking messages
AT	Authorization Ticket
ATS	Abstract Test Suite
BO	Exceptional Behaviour
BV	Valid Behaviour
CA	Certificate Authority
CAM	Co-operative Awareness Messages
CAN	Controller Area Network
CERT	Certificate
COER	Cannonical Octet Encoding Rules
DE	Data Element
DEN	Decentralized Environmental Notification
DENM	Decentralized Environmental Notification Message
EA	Enrolment Authority
ECC	Elliptic Curve Cryptography
GN	GeoNetworking
ITS	Intelligent Transport Systems
ITS-S	Intelligent Transport System - Station
IUT	Implementation under Test
MSG	Message
PICS	Protocol Implementation Conformance Statement
PSID	Provider Service Identifier
RCA	Root Certificate Authority
SSP	Service Specific Permissions
TP	Test Purposes

TSS Test Suite Structure

4 Test Suite Structure (TSS)

4.1 Structure for Security tests

Table 1 shows the Security Test Suite Structure (TSS) defined for conformance testing.

Table 1: TSS for Security

Root	Group	Category
Security	ITS-S data transfer	Valid
	ITS-S - AA authorization	Valid
	ITS-S - EA enrolment	Valid
	Sending behaviour	Valid
	Receiving behaviour	Valid and Invalid
	Generic messages	Valid
	CAM testing	Valid
	DENM testing	Valid
	Certificate testing	Valid

5 Test Purposes (TP)

5.1 Introduction

5.1.1 TP definition conventions

The TP definition is built according to ETSI EG 202 798 [i.1].

5.1.2 TP Identifier naming conventions

The identifier of the TP is built according to table 2.

Table 2: TP naming convention

Identifier	TP_<root>_<tgt>_<gr>_<sgr>_<rn>_<sn>_<x>		
	<root> = root	SEC	
	<tgt> = target	ITSS	ITS-S data transfer
		AA	ITS-S - AA authorization
		EA	ITS-S - EA enrolment
	<gr> = group	SND	Sending behaviour
		RCV	Receiving behaviour
	<sgr> =sub- group	MSG	Generic messages
		CAM	CAM testing
		DENM	DENM testing
		CERT	Certificate testing
	<sn> = test purpose sequential number		01 to 99
	<x> = category	BV	Valid Behaviour tests
		BO	Invalid Behaviour Tests

5.1.3 Rules for the behaviour description

The description of the TP is built according to ETSI EG 202 798 [i.1].

ETSI TS 103 097 [1] does not use the finite state machine concept. As a consequence, the test purposes use a generic "Initial State" that corresponds to a state where the IUT is ready for starting the test execution. Furthermore, the IUT shall be left in this "Initial State", when the test is completed.

Being in the "Initial State" refers to the starting point of the initial device configuration. There are no pending actions, no instantiated buffers or variables, which could disturb the execution of a test.

5.1.4 Sources of TP definitions

All TPs have been specified according to ETSI TS 103 097 [1] and IEEE Std 1609.2™[2].

5.1.5 Mnemonics for PICS reference

To avoid an update of all TPs when the PICS document is changed, table 3 introduces mnemonics name and the correspondence with the real PICS item number. The 'PICS item' as defined in IEEE Std 1609.2 [2], ETSI TS 103 096-1 [3] and ETSI TS 102 871-1 [4] shall be used to determine the test applicability.

Table 3: Mnemonics for PICS reference

	Mnemonic	PICS item
1	PICS_GN_SECURITY	A.2/1 [4]
2	PICS_SEC_CERTIFICATE_SELECTION	A.8/1 [3]
3	PICS_SEC_CIRCULAR_REGION	S1.2.2.5.1.1 [2]
4	PICS_SEC_RECTANGULAR_REGION	S1.2.2.5.1.2 [2]
5	PICS_SEC_POLYGONAL_REGION	S1.2.2.5.1.3 [2]
6	PICS_SEC_IDENTIFIED_REGION	S1.2.2.5.1.4 [2]
7	PICS_SEC_ITS_AID_OTHER	A.7/1 [3]
8	PICS_SEC_SHA256	S1.2.2.1.1 [2]
9	PICS_SEC_SHA384	S1.2.2.1.2 [2]
10	PICS_SEC_BRAINPOOL_P256R1	S1.2.2.4.1.2 [2]
11	PICS_SEC_BRAINPOOL_P384R1	S1.2.2.4.2 [2]

6 ITS-S Security

6.1 Overview

Void.

6.2 Sending behaviour

6.2.1 Check the message protocol version

TP Id	TP_SEC_ITSS_SND_MSG_01_BV
Summary	Check that the IUT sends a secured message containing protocol version set to 3
Reference	ETSI TS 103 097 [1], clause 5.1 IEEE Std 1609.2 [2], clause 6.3.2
PICS Selection	PICS_GN_SECURITY
Expected behaviour	
with the IUT being in the 'authorized' state ensure that when the IUT is requested to send a secured message then the IUT sends a EtsiTs103097Data containing protocolVersion indicating value '3'	

6.2.2 CAM profile

6.2.2.1 Check that secured CAM is signed

TP Id	TP_SEC_ITSS_SND_CAM_01_BV
Summary	Check that IUT sends the secured CAM using SignedData container
Reference	ETSI TS 103 097 [1], clause 7.1.1
PICS Selection	PICS_GN_SECURITY
Expected behaviour	
with the IUT is authorized with AT certificate (CERT_IUT_A_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing content containing signedData	

6.2.2.2 Check secured CAM AID value

TP Id	TP_SEC_ITSS_SND_CAM_02_BV
Summary	Check that IUT sends the secured CAM containing the HeaderInfo field psid set to 'AID_CAM'
Reference	ETSI TS 103 097 [1], clause 7.1.1
PICS Selection	PICS_GN_SECURITY
Expected behaviour	
with the IUT is authorized with AT certificate (CERT_IUT_A_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing content containing signedData containing tbsData containing headerInfo containing psid indicating 'AID_CAM'	

6.2.2.3 Check header fields

TP Id	TP_SEC_ITSS_SND_CAM_03_BV
Summary	Check that IUT sends the secured CAM with the HeaderInfo containing generationTime and does not contain expiryTime, generationLocation, encryptionKey, p2pcdLearningRequest, missingCrlIdentifier
Reference	ETSI TS 103 097 [1], clauses 5.2, 7.1.1
PICS Selection	PICS_GN_SECURITY
Expected behaviour	
with the IUT is authorized with AT certificate (CERT_IUT_A_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing content containing signedData containing tbsData containing headerInfo containing generationTime and not containing expiryTime and not containing generationLocation, and not containing encryptionKey and not containing p2pcdLearningRequest and not containing missingCrlIdentifier	

6.2.2.4 Check signer information

TP Id	TP_SEC_ITSS_SND_CAM_04_BV
Summary	Check that IUT sends the secured CAM containing signer containing either certificate or digest Check that signing certificate has permissions to sign CAM messages
Reference	ETSI TS 103 097 [1], clauses 5.2, 7.1.1 IEEE Std 1609.2 [2], clause 6.3.4
PICS Selection	PICS_GN_SECURITY
Expected behaviour	
with the IUT is authorized with AT certificate (CERT_IUT_A_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing content containing signedData containing signer containing digest or containing certificate containing toBeSigned containing appPermissions containing the item of type PsidSsp containing psid indicating AID_CAM	

TP Id	TP_SEC_ITSS_SND_CAM_05_BV
Summary	Check that IUT calculate the digest of certificate using proper hash algorithm Check that IUT canonicalize certificates before hash calculation
Reference	ETSI TS 103 097 [1], clauses 5.2, 7.1.1 IEEE Std 1609.2 [2], clause 6.3.4
PICS Selection	PICS_GN_SECURITY AND ***X_PICS***

Expected behaviour

```
with
    the IUT is authorized with AT certificate (X_CERTIFICATE)
    and the IUT is configured to send more than one CAM per second
    and the IUT having sent a secured CAM
        containing signer
            containing certificate
                indicating X_CERTIFICATE
                    containing verifyKeyIndicator
                        containing verificationKey
                            containing X_KEY
ensure that
    when
        the IUT is requested to send a subsequent secured CAM
            containing signer
                containing digest
    then
        the IUT sends a message of type EtsiTs103097Data
            containing content
                containing signedData
                    containing signer
                        containing digest
                            indicating last 8 bytes of the Hash value calculated using X_HASH algorithm
```

Permutation table

XX	*X_CERTIFICATE*	*X_KEY*	*X_HASH*	*X_PICS*
A	CERT_IUT_A_AT	ecdsaNistP256	SHA-256	
AN	CERT_IUT_A_N_AT	ecdsaNistP256 (uncompressed)	SHA-256	
B	CERT_IUT_A_B_AT	ecdsaBrainpoolP256r1	SHA-256	PICS_SEC_BRAINPOOL_P256R1
BN	CERT_IUT_A_B_N_AT	ecdsaBrainpoolP256r1 (uncompressed)	SHA-256	PICS_SEC_BRAINPOOL_P256R1
C	CERT_IUT_A_B3_AT	ecdsaBrainpoolP384r1	SHA-384	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1
CN	CERT_IUT_A_B3_N_AT	ecdsaBrainpoolP384r1 (uncompressed)	SHA-384	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1

TP Id	TP_SEC_ITSS_SND_CAM_06_BV
Summary	Check that IUT sends the secured CAM containing the signing certificate when over the time of one second no other secured CAM contained the certificate was sent
Reference	ETSI TS 103 097 [1], clause 7.1.1
PICS Selection	PICS_GN_SECURITY

Expected behaviour

```
with
    the IUT is authorized with AT certificate (CERT_IUT_A_AT)
    and the IUT is configured to send more than one CAM per second
    and the IUT having sent a secured CAM
        containing generationTime
            indicating TIME_LAST
ensure that
    when
        the IUT is sending secured CAM as a message of type EtsiTs103097Data
            containing signer
                containing certificate
    then
        this message is
            containing headerInfo
                containing generationTime
                    indicating TIME (TIME >= TIME_LAST + 1 sec)
```

TP Id	TP_SEC_ITSS_SND_CAM_07_BV
Summary	Check that IUT sends the secured CAM containing the signing certificate when the timeout of one second has been expired after the previous CAM containing the certificate
Reference	ETSI TS 103 097 [1], clause 7.1.1
PICS Selection	PICS_GN_SECURITY
Expected behaviour	
with the IUT is authorized with AT certificate (CERT_IUT_A_AT) and the IUT is configured to send more than one CAM per second and the IUT having sent a secured CAM containing signer containing certificate and containing generationTime indicating TIME_LAST ensure that when the IUT is sending a secured CAM as a message of type EtsiTs103097Data containing generationTime indicating TIME >= TIME_LAST + 1 sec then this message is containing certificate	

6.2.2.5 Check that IUT sends certificate to unknown ITS-S

TP Id	TP_SEC_ITSS_SND_CAM_08_BV
Summary	Check that IUT sends the secured CAM containing the signing certificate when the IUT received a CAM from an unknown ITS-S
Reference	ETSI TS 103 097 [1], clause 7.1.1
PICS Selection	PICS_GN_SECURITY
Expected behaviour	
with the IUT is authorized with AT certificate (CERT_IUT_A_AT) and the IUT is configured to send more than one CAM per second and the IUT having already sent secured CAM containing certificate at TIME_1 and the IUT having received a message of type EtsiTs103097Data containing signedData containing signer containing digest indicating HashedId8 value referencing an unknown certificate (CERT_TS_B_AT) at TIME_2 (TIME_1 < TIME_2 < TIME_1+1 sec) ensure that when the IUT is requested to send secured CAM at TIME_3 (TIME_1 < TIME_2 < TIME_3 < TIME_1 + 1 sec) then the IUT sends a message of type EtsiTs103097Data containing signedData containing signer containing certificate	