



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

PREVIEW
Standard
https://standards.iteh.ai/catalog/standards/sist/061e3f49-53e7-4379-9a23-e4e69850e66e/etsi-ts-103-096-2-v1.3.1-2017-03

Reference

RTS/ITS-00535

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>

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2017.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE™** are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights	6
Foreword.....	6
Modal verbs terminology.....	6
1 Scope	7
2 References	7
2.1 Normative references	7
2.2 Informative references.....	7
3 Definitions and abbreviations.....	8
3.1 Definitions.....	8
3.2 Abbreviations	8
4 Test Suite Structure (TSS).....	9
4.1 Structure for Security tests	9
5 Test Purposes (TP)	9
5.1 Introduction	9
5.1.1 TP definition conventions.....	9
5.1.2 TP Identifier naming conventions.....	9
5.1.3 Rules for the behaviour description	9
5.1.4 Sources of TP definitions.....	10
5.1.5 Mnemonics for PICS reference.....	10
5 ITS-S Security	10
5.1 Overview	10
5.2 Sending behaviour.....	10
5.2.1 Check the message protocol version.....	10
5.2.2 Check that AT certificate is used to sign communication messages of ITS-S.....	11
5.2.3 Check Signature ECC point type	12
5.2.4 CAM profile.....	12
5.2.4.1 Check secured CAM its_aid value	12
5.2.4.2 Check header fields	13
5.2.4.3 Check that IUT sends digest as sender info	13
5.2.4.4 Check that IUT sends cert to unknown ITS-S.....	14
5.2.4.5 Check that IUT restarts the timer when the certificate has been sent.....	15
5.2.4.6 Check that IUT sends certificate when requested	15
5.2.4.7 Check that IUT send certificate_chain when requested	16
5.2.4.8 Check generation time.....	17
5.2.4.9 Check sending certificate request to unknown station	18
5.2.4.10 Check Payload.....	18
5.2.4.11 Check presence of trailer field	18
5.2.4.12 Check signature.....	19
5.2.5 DENM profile.....	19
5.2.5.1 Check secured DENM its_aid value	19
5.2.5.2 Check header fields	20
5.2.5.3 Check that signer info is a certificate	20
5.2.5.4 Check generation time.....	21
5.2.5.5 Check generation location.....	21
5.2.5.6 Check Payload.....	24
5.2.5.7 Check trailer field presence.....	24
5.2.5.8 Check signature.....	25
5.2.6 Generic signed message profile	25
5.2.6.1 Check secured its_aid value	25
5.2.6.2 Check header field.....	26
5.2.6.3 Check that signer info is a certificate	26
5.2.6.4 Check generation time.....	27
5.2.6.5 Check generation location.....	27

5.2.6.6	Check payload.....	30
5.2.6.7	Check signature.....	31
5.2.7	Profiles for certificates.....	31
5.2.7.1	Check that certificate version is 2	31
5.2.7.2	Check the certificate chain consistence.....	32
5.2.7.3	Check rectangular region validity restriction	33
5.2.7.4	Check polygonal region validity restriction	34
5.2.7.5	Check identified region validity restriction.....	36
5.2.7.6	Check region validity restrictions in the chain	38
5.2.7.7	Check time validity restriction in the chain.....	40
5.2.7.8	Check ECC point type of the certificate signature	41
5.2.7.9	Check ECC point type of the certificate verification key.....	42
5.2.7.10	Verify certificates signatures.....	43
5.2.7.11	Check certificate assurance level in the chain.....	44
5.2.7.12	AA certificate profile	44
5.2.7.12.1	Check AA certificate subject type	44
5.2.7.12.2	Check AA certificate subject name	45
5.2.7.12.3	Check that signer info of AA certificate is a digest	45
5.2.7.12.4	Check that AA cert is signed by Root cert.....	46
5.2.7.12.5	Check AA certificate subject attributes presence and order	46
5.2.7.12.6	Check ITS-AID list of AA certificate.....	47
5.2.7.12.7	Check AA certificate validity restriction presence and order.....	47
5.2.7.12.8	Check the AA certificate time_start_and_end validity restriction.....	48
5.2.7.13	AT certificate profile.....	49
5.2.7.13.1	Check AT certificate subject type.....	49
5.2.7.13.2	Check AT certificate subject name.....	49
5.2.7.13.3	Check that signer info of AT certificate is a digest	50
5.2.7.13.4	Check AT certificate subject attributes presence and order.....	50
5.2.7.13.5	Check presence of time_start_and_end validity restriction	51
5.2.7.13.6	Check ITS-AID-SSP	52
5.2.7.13.7	Check that AT certificate is signed by AA cert.....	53
5.2.7.13.8	Check validity restriction presence and order.....	53
5.3	Receiver behaviour.....	54
5.3.1	Overview	54
5.3.2	CAM Profile	54
5.3.2.1	Check that IUT accepts well-formed Secured CAM.....	54
5.3.2.2	Check the message protocol version	57
5.3.2.3	Check header fields.....	57
5.3.2.4	Check signer info	64
5.3.2.5	Check generation time.....	66
5.3.2.6	Check its_aid.....	67
5.3.2.7	Check payload.....	68
5.3.2.8	Check presence of trailer field	70
5.3.2.9	Check signature.....	71
5.3.2.10	Check signing certificate type.....	72
5.3.2.11	Check certificate validity	74
5.3.3	DENM Profile.....	78
5.3.3.1	Check that IUT accepts well-formed Secured DENM	78
5.3.3.2	Check the message protocol version	83
5.3.3.3	Check header fields.....	83
5.3.3.4	Check signer info	91
5.3.3.5	Check generation time.....	93
5.3.3.6	Check its_aid.....	94
5.3.3.7	Check generation location.....	95
5.3.3.8	Check Payload.....	97
5.3.3.9	Check presence of trailer field	98
5.3.3.10	Check signature.....	99
5.3.3.11	Check signing certificate type.....	100
5.3.3.12	Check certificate validity	102
5.3.4	Generic Signed Message Profile.....	106
5.3.4.1	Check that IUT accepts well-formed GN Beacon message	106
5.3.4.2	Check the message protocol version	111

5.3.4.3	Check header fields	111
5.3.4.4	Check signer info	118
5.3.4.5	Check generation time.....	120
5.3.4.6	Check its_aid.....	121
5.3.4.7	Check generation location.....	121
5.3.4.8	Check Payload.....	123
5.3.4.9	Check presence of trailer field	125
5.3.4.10	Check signature.....	126
5.3.4.11	Check signing certificate type.....	127
5.3.4.12	Check certificate validity	129
5.3.5	Profiles for certificates.....	132
5.3.5.1	Check that certificate version is 2	132
5.3.5.2	Check that enrolment certificate is not used for sign other certificates.....	134
5.3.5.3	Check that authorization ticket certificate is not used for sign other certificates	136
5.3.5.4	Check that AA certificate signed with other AA certificate is not accepted	137
5.3.5.5	Check the certificate signature	137
5.3.5.6	Check circular region of subordinate certificate	138
5.3.5.7	Check rectangular region of subordinate certificate.....	145
5.3.5.8	Check polygonal region of subordinate certificate.....	151
5.3.5.9	Check identified region of subordinate certificate	158
5.3.5.10	Check time validity restrictions.....	168
5.3.5.10.1	Check time validity restriction presence.....	168
5.3.5.10.2	Check AT certificate time validity restriction presence	169
5.3.5.11	Check time validity restriction conforming to the issuing certificate.....	171
5.3.5.12	Check AID-SSP subject attribute presence and value.....	173
5.3.5.13	Check AID-SSP subject attribute value conforming to the issuing certificate.....	175
5.3.5.14	Check the authorization ticket certificate signer info.....	176
5.3.5.15	Check the authorization authority certificate signer info	178
5.3.5.16	Check the subject_name of the AT certificate	179
5.3.5.17	Check certificate assurance level presence and values.....	180
5.3.5.18	Check certificate verification key presence.....	182
5.3.5.19	Check invalid region type in validity restriction of certificates	182
Annex A (informative):	Bibliography.....	183
History		184

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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.

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 specification 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 standard 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 (V1.2.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".
- [2] ETSI TS 103 096-1 (V1.3.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)".
- [3] ETSI TS 102 871-1 (V1.3.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma".
- [4] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes".
- [5] United Nations, Statistics Division (1996): "Standard Country or Area Codes for Statistical Use (Rev. 3), Series M: Miscellaneous Statistical Papers, No. 49", New York: United Nations.

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
CAM	Co-operative Awareness Messages
CAN	Controller Area Network
CERT	Certificate
DE	Data Element
DENM	Decentralized Environmental Notification Message
EA	Enrolment Authority
ECC	Elliptic Curve Cryptography
GN	GeoNetworking
ITS	Intelligent Transportation Systems
ITS-S	Intelligent Transport System - Station
IUT	Implementation under Test
MSG	Message
PICS	Protocol Implementation Conformance Statement
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
	<rn> = requirement sequential number		01 to 99
	<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 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].

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' column refers to tables and items of ETSI TS 103 096-1 [2] if not stated otherwise. The 'PICS item' as defined in ETSI TS 103 096-1 [2] and ETSI TS 102 871-1 [3] shall be used to determine the test applicability.

Table 3: Mnemonics for PICS reference

	Mnemonic	PICS item
1	PICS_GN_SECURITY	A.2/1 ETSI TS 102 871-1 [3]
2	PICS_CERTIFICATE_SELECTION	A.2/1
3	PICS_USE_CIRCULAR_REGION	A.3/2
4	PICS_USE_RECTANGULAR_REGION	A.3/3
5	PICS_USE_POLYGONAL_REGION	A.3/4
6	PICS_USE_IDENTIFIED_REGION	A.3/5
7	PICS_ITS_AID_OTHER_PROFILE	A.5/1
8	PICS_USE_ISO31661_REGION_DICTIONARY	A.4/1
9	PICS_USE_UN_STATS_REGION_DICTIONARY	A.4/2

5 ITS-S Security

5.1 Overview

Void.

5.2 Sending behaviour

5.2.1 Check the message protocol version

TP Id	TP_SEC_ITSS_SND_MSG_01_01_BV
Summary	Check that ITS-S sends a SecuredMessage containing protocol version set to 2
Reference	ETSI TS 103 097 [1], clause 5.1
PICS Selection	PICS_GN_SECURITY
Expected behaviour	
<p>with the IUT being in the 'authorized' state ensure that when the IUT is requested to send a SecuredMessage then the IUT sends a SecuredMessage containing protocol_version indicating value '2'</p>	

5.2.2 Check that AT certificate is used to sign communication messages of ITS-S

TP Id	TP_SEC_ITSS_SND_MSG_04_01_BV
Summary	Check that when IUT sends the message signed with the digest, then this digest points to the AT certificate
Reference	ETSI TS 103 097 [1], clause 6.3
PICS Selection	PICS_GN_SECURITY
Expected behaviour	
<p>with the IUT being in the 'authorized' state and the IUT is configured to send more than one CAM per second and the IUT having sent last CAM containing header_fields['signer_info'].signer.type indicating 'certificate'</p> <p>ensure that when the IUT is requested to send next CAM then the IUT sends a SecuredMessage containing header_fields ['signer_info'] containing signer containing type indicating 'certificate_digest_with_sha256' and containing digest referencing the certificate containing subject_info.subject_type indicating 'authorization_ticket'</p>	

TP Id	TP_SEC_ITSS_SND_MSG_04_02_BV
Summary	Check that IUT uses the AT certificate to sign messages
Reference	ETSI TS 103 097 [1], clause 6.3
PICS Selection	PICS_GN_SECURITY
Expected behaviour	
<p>with the IUT being in the 'authorized' state the IUT being requested to include certificate in the next CAM</p> <p>ensure that when the IUT is requested to send a next CAM then the IUT sends a SecuredMessage containing header_fields ['signer_info'] containing signer containing type indicating 'certificate' and containing certificate containing subject_info.subject_type indicating 'authorization_ticket'</p>	

5.2.3 Check Signature ECC point type

TP Id	TP_SEC_ITSS_SND_MSG_05_01_BV
Summary	Check that the SecuredMessage signature contains the ECC point of type set to either compressed_lsb_y_0, compressed_lsb_y_1 or x_coordinate_only
Reference	ETSI TS 103 097 [1], clause 4.2.9
PICS Selection	PICS_GN_SECURITY
Expected behaviour	
<p>with the IUT being in the 'authorized' state ensure that when the IUT is requested to send a CAM then the IUT sends a SecuredMessage containing header_fields ['its_aid'] containing its_aid indicating 'AID_CAM' and containing trailer_fields['signature'] containing signature.ecdsa_signature containing R.type indicating 'compressed_lsb_y_0' or indicating 'compressed_lsb_y_1' or indicating 'x_coordinate_only'</p>	

5.2.4 CAM profile

5.2.4.1 Check secured CAM its_aid value

TP Id	TP_SEC_ITSS_SND_CAM_01_01_BV
Summary	Check that the sent Secured CAM contains a HeaderField its_aid that is set to 'AID_CAM'
Reference	ETSI TS 103 097 [1], clauses 5.4 and 7.1
PICS Selection	PICS_GN_SECURITY
Expected behaviour	
<p>with the IUT being in the 'authorized' state ensure that when the IUT is requested to send CAM then the IUT sends a SecuredMessage containing header_fields ['its_aid'] containing its_aid indicating 'AID_CAM'</p>	

5.2.4.2 Check header fields

TP Id	TP_SEC_ITSS_SND_CAM_02_01_BV
Summary	Check that the secured CAM contains exactly one element of these header fields: signer_info, generation_time, its_aid; Check that the header fields are in the ascending order according to the numbering of the enumeration except of the signer_info, which is encoded first; Check that generation_time_standard_deviation, expiration, encryption_parameters, recipient_info are not used
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
Expected behaviour	
<p>with the IUT being in the 'authorized' state ensure that when the IUT is requested to send a CAM then the IUT sends a SecuredMessage containing header_fields[0] containing type indicating 'signer_info' and containing header_fields [1..N] indicating header_fields [n].type < header_fields [n+1].type and containing header_fields ['generation_time'] and containing header_fields ['its_aid'] and not containing header_fields ['generation_time_standard_deviation'] and not containing header_fields ['expiration'] and not containing header_fields ['encryption_parameters'] and not containing header_fields ['recipient_info']</p>	

5.2.4.3 Check that IUT sends digest as sender info

TP Id	TP_SEC_ITSS_SND_CAM_05_01_BV
Summary	Check that the secured CAM contains the signer_info field of certificate when over the time of one second no other SecuredMessage contained a signer_info of type certificate
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
Expected behaviour	
<p>with the IUT being in the 'authorized' state and the IUT is configured to send more than one CAM per second and the IUT having sent a CAM containing header_fields['signer_info'].signer.type indicating 'certificate' and contains header_fields['generation_time'] indicating TIME_LAST ensure that when the IUT is sending CAM containing header_fields['signer_info'] containing signer containing type indicating 'certificate' then this message is containing header_fields['generation_time'] indicating TIME (TIME >= TIME_LAST + 1sec)</p>	