ETSI TS 103 096-2 V1.2.1 (2015-09)

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

Reference

RTS/ITS-00529

Keywords

ITS, testing, TSS&TP, security

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
http://portal.etsi.org/tb/status/status.asp

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

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 (http://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 ETSI TS 103 097 [1] in accordance with the relevant guidance given in ISO/IEC 9646-7 [7].

The ISO standard for the methodology of conformance testing (ISO/IEC 9646-1 [4] and ISO/IEC 9646-2 [5]) as well as the ETSI rules for conformance testing (ETSI ETS 300 406 [8]) 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 reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://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 (V1.2.1): "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/IEC 9646-1 (1994): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 1: General concepts".

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

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

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

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

[9] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes".

[10] 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 reference 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".

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], ISO/IEC 9646-6 [6] and ISO/IEC 9646-7 [7] apply.

3.2 Abbreviations

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

AA	Authorization Authority
AID	Application Identifier
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 are 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 Table/Item of ETSI TS 103 096-1 [2] if not stated otherwise.

Table 3: Mnemonics for PICS reference

	Mnemonic	PICS item
1	PICS_GN_SECURITY	A.32/12 ETSI ETSI TS 102 871-1 [3]
2	PICS_CERTIFICATE_SELECTION	A.3/1
3	PICS_USE_CIRCULAR_REGION	A.4/2
4	PICS_USE_RECTANGULAR_REGION	A.4/3
5	PICS_USE_POLYGONAL_REGION	A.4/4
6	PICS_USE_IDENTIFIED_REGION	A.4/5
7	PICS_ITS_AID_OTHER_PROFILE	A.6/1
8	PICS_USE_ISO31661_REGION_DICTIONARY	A.5/1
9	PICS_USE_UN_STATS_REGION_DICTIONARY	A.5/2

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 5.2
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 SecuredMessage
  } then {
    the IUT sends a SecuredMessage
      containing protocol_version
        indicating value '2'
  }
}
```

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	

```
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'
}
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'
          containing digest
            referencing the certificate
              containing subject_info.subject_type
                indicating 'authorization_ticket'
        }
      }
  }
}
```

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	

```
with {
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate in the next CAM
}
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'
          containing certificate
            containing subject_info.subject_type
              indicating 'authorization_ticket'
        }
      }
  }
}
```

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	

```
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
    }
  }
}
```

5.2.4 CAM profile

5.2.4.1 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	

```
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 [n].type
        indicating value < header_fields [n+1].type
      and containing header_fields ['generation_time']
      and containing header_fields['its_aid']
        indicating 'AID_CAM'
      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']
    }
  }
}
```

5.2.4.2 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	

```
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'
    contains header_fields['generation_time']
      indicating TIME_LAST
  }
ensure that {
  when {
    the IUT sends one of the next SecuredMessage
      containing header_fields['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate
        }
      }
      containing header_fields['its_aid']
        indicating 'AID_CAM'
  } then {
    this message
      contains header_fields['generation_time']
        indicating TIME (TIME >= TIME_LAST + 1sec)
  }
}
```

TP Id	TP_SEC_ITSS_SND_CAM_05_02_BV
Summary	Check that the secured CAM contains the signer_info field of 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
PICS Selection	PICS_GN_SECURITY
Expected behaviour	

```
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'
    at TIME_1
}
ensure that {
  when {
    the IUT is requested to send next CAM right after 1 second after the TIME_1
  } then {
    the IUT sends a SecuredMessage {
      containing header_fields['its_aid']
        indicating 'AID_CAM'
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate
        }
      }
    }
  }
}
```