



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

PREVIEW
iTechStandards.com
https://standards.iteh.ai/catalog/standards-test/a14bb3dd-7cb9-453b-9583-17cb8681061e/etsi-103-096-2-v1.2.1-2015-09

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/CommitteeSupportStaff.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 2015.

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..... | 8 |
| 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 |
| 5.2 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 header fields..... | 12 |
| 5.2.4.2 Check that IUT sends digest as sender info | 13 |
| 5.2.4.3 Check that IUT sends cert to unknown ITS-S..... | 14 |
| 5.2.4.4 Check that IUT restarts the timer when the certificate has been sent..... | 15 |
| 5.2.4.5 Check that IUT sends certificate when requested | 16 |
| 5.2.4.6 Check that IUT send certificate_chain when requested | 17 |
| 5.2.4.7 Check generation time..... | 18 |
| 5.2.4.8 Check secured CAM its_aid value | 18 |
| 5.2.4.9 Check sending certificate request to unknown station | 19 |
| 5.2.4.10 Check Payload..... | 19 |
| 5.2.4.11 Check presence of trailer field | 19 |
| 5.2.4.12 Check signature..... | 20 |
| 5.2.5 DENM profile..... | 21 |
| 5.2.5.1 Check header fields..... | 21 |
| 5.2.5.2 Check that signer info is a certificate | 21 |
| 5.2.5.3 Check generation time..... | 22 |
| 5.2.5.4 Check generation location..... | 22 |
| 5.2.5.5 Check secured DENM its_aid value | 27 |
| 5.2.5.6 Check Payload..... | 27 |
| 5.2.5.7 Check trailer field presence..... | 27 |
| 5.2.5.8 Check signature..... | 28 |
| 5.2.6 Generic signed message profile | 29 |
| 5.2.6.1 Check header field..... | 29 |
| 5.2.6.2 Check that signer info is a certificate | 29 |
| 5.2.6.3 Check generation time..... | 30 |
| 5.2.6.4 Check generation location..... | 30 |
| 5.2.6.5 Check payload..... | 34 |
| 5.2.6.6 Check signature..... | 34 |
| 5.2.7 Profiles for certificates..... | 35 |
| 5.2.7.1 Check that certificate version is 2 | 35 |

| | | |
|------------|---|-----|
| 5.2.7.2 | Check the certificate chain | 36 |
| 5.2.7.3 | Geographical regions | 36 |
| 5.2.7.3.1 | Check Rectangular regions | 36 |
| 5.2.7.3.2 | Check Polygonal Region | 38 |
| 5.2.7.3.3 | Check Identified Region | 40 |
| 5.2.7.4 | Check ECC point type of the certificate signature | 44 |
| 5.2.7.5 | Check ECC point type of the certificate verification key | 44 |
| 5.2.7.6 | Check the certificate signature | 45 |
| 5.2.7.7 | AA certificate profile | 46 |
| 5.2.7.7.1 | Check the subject type | 46 |
| 5.2.7.7.2 | Check AA certificate subject name | 46 |
| 5.2.7.7.3 | Check that signer info is a digest | 47 |
| 5.2.7.7.4 | Check subject attributes presence and order | 47 |
| 5.2.7.7.5 | Check the time_start_and_end presence | 48 |
| 5.2.7.7.6 | Check verification key validity | 48 |
| 5.2.7.7.7 | Check ITS-AID | 48 |
| 5.2.7.7.8 | Check that AA cert is signed by Root cert | 49 |
| 5.2.7.7.9 | Check validity restriction presence and order | 49 |
| 5.2.7.8 | AT certificate profile | 49 |
| 5.2.7.8.1 | Check subject type | 49 |
| 5.2.7.8.2 | Check that signer info is a digest | 50 |
| 5.2.7.8.3 | Check subject name | 50 |
| 5.2.7.8.4 | Check the presence and the order of subject attributes | 51 |
| 5.2.7.8.5 | Check presence of time_start_and_end validity restriction | 52 |
| 5.2.7.8.6 | Check verification key validity | 52 |
| 5.2.7.8.7 | Check ITS-AID-SSP | 53 |
| 5.2.7.8.8 | Check that AT certificate is signed by AA cert | 54 |
| 5.2.7.8.9 | Check assurance level | 55 |
| 5.2.7.8.10 | Check validity restriction presence and order | 55 |
| 5.3 | Receiver Behaviour | 55 |
| 5.3.1 | Overview | 55 |
| 5.3.2 | CAM Profile | 56 |
| 5.3.2.1 | Check that IUT accepts well-formed Secured CAM | 56 |
| 5.3.2.2 | Check the message protocol version | 59 |
| 5.3.2.3 | Check header fields | 60 |
| 5.3.2.4 | Check signer info | 66 |
| 5.3.2.5 | Check generation time | 69 |
| 5.3.2.6 | Check its_aid | 70 |
| 5.3.2.7 | Check payload | 71 |
| 5.3.2.8 | Check presence of trailer field | 73 |
| 5.3.2.9 | Check signature | 74 |
| 5.3.2.10 | Check signing certificate type | 75 |
| 5.3.3 | DENM Profile | 77 |
| 5.3.3.1 | Check that IUT accepts well-formed Secured DENM | 77 |
| 5.3.3.2 | Check the message protocol version | 82 |
| 5.3.3.3 | Check header fields | 83 |
| 5.3.3.4 | Check signer info | 89 |
| 5.3.3.5 | Check generation time | 91 |
| 5.3.3.6 | Check its_aid | 93 |
| 5.3.3.7 | Check generation location | 93 |
| 5.3.3.8 | Check Payload | 95 |
| 5.3.3.9 | Check presence of trailer field | 97 |
| 5.3.3.10 | Check signature | 98 |
| 5.3.3.11 | Check signing certificate type | 99 |
| 5.3.4 | Generic Signed Message Profile | 100 |
| 5.3.4.1 | Check that IUT accepts well-formed GN Beacon message | 100 |
| 5.3.4.2 | Check the message protocol version | 106 |
| 5.3.4.3 | Check header fields | 107 |
| 5.3.4.4 | Check signer info | 110 |
| 5.3.4.5 | Check generation time | 112 |
| 5.3.4.6 | Check generation location | 114 |
| 5.3.4.7 | Check Payload | 116 |

| | | |
|-------------------------------|---|------------|
| 5.3.4.8 | Check presence of trailer field | 117 |
| 5.3.4.9 | Check signature | 118 |
| 5.3.4.10 | Check signing certificate type | 119 |
| 5.3.5 | Profiles for certificates | 120 |
| 5.3.5.1 | Check that certificate version is 2 | 120 |
| 5.3.5.2 | Check that enrolment certificate is not used for sign other certificates | 121 |
| 5.3.5.3 | Check that any certificate signed with AT certificate is not accepted | 121 |
| 5.3.5.4 | Check that AA certificate signed with other AA certificate is not accepted | 122 |
| 5.3.5.5 | Check the certificate signature | 122 |
| 5.3.5.6 | Check circular region of subordinate certificate | 123 |
| 5.3.5.7 | Check rectangular region of subordinate certificate | 126 |
| 5.3.5.8 | Check polygonal region of subordinate certificate | 129 |
| 5.3.5.9 | Check identified region of subordinate certificate | 133 |
| 5.3.5.10 | Check time validity restriction presence | 140 |
| 5.3.5.11 | Check time validity restriction conforming to the issuing certificate | 141 |
| 5.3.5.12 | Check AID subject attribute presence | 143 |
| 5.3.5.13 | Check AID-SSP subject attribute value conforming to the issuing certificate | 145 |
| Annex A (informative): | Bibliography | 146 |
| History | | 147 |

ITEH STANDARD PREVIEW
 (standards.iteh.ai)

Full standard:
<https://standards.iteh.ai/catalog/standards/sist/a14bb3dd-7eb9-453b-9583-17cb868fa30a/etsi-ts-103-096-2-v1.2.1-2015-09>

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 | |
| <pre> 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' } } </pre> | |

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 | |
| <pre> 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' } } } } </pre> | |

| | |
|---|---|
| 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 | |
| <pre> 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' } } } } </pre> | |

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 | |
| <pre> 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 } } } </pre> | |

5.2.4 CAM profile

5.2.4.1 Check header fields

| | |
|---|--|
| TP Id | TP_SEC_ITSS_SND_CAM_02_01_BV |
| Summary | <p>Check that the secured CAM contains exactly one element of these header fields: signer_info, generation_time, its_aid</p> <p>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</p> <p>Check that generation_time_standard_deviation, expiration, encryption_parameters, recipient_info are not used</p> |
| Reference | ETSI TS 103 097 [1], clause 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| <pre> 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'] } } } </pre> | |

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 | |
| <pre> 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) } } </pre> | |

| | |
|--|--|
| 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 | |
| <pre> 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 } } } } } </pre> | |