ETSITS 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

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

| Intelle | ectual Property Rights | 6 |
|----------------------|---|----|
| Forew | word | 6 |
| Moda | al verbs terminology | 6 |
| 1 | Scope | 7 |
| 2 | References | 7 |
| 2.1 | Normative references | |
| 2.2 | Informative references | |
| | | |
| 3 | Definitions and abbreviations | |
| 3.1 | Definitions | |
| 3.2 | Abbreviations | 8 |
| 4 | Test Suite Structure (TSS) | 9 |
| 4.1 | Structure for Security tests | |
| _ | · | |
| 5 | Test Purposes (TP) | |
| 5.1 | Introduction | |
| 5.1.1 5.1.2 | TP Identifier remine conventions | |
| 5.1.2 | TP Identifier naming conventions | |
| 5.1.3 | Sources of TP definitions | |
| 5.1.5 | Mnemonics for PICS reference | |
| 5.2 | Sending behaviour | |
| 5.2.1 | Check the message protocol version | |
| 5.2.2 | Check that AT certificate is used to sign communication messages of ITS-S | |
| 5.2.3 | Check Signature ECC point type | |
| 5.2.4 | CAM profile | |
| 5.2.4.1 | 1 Check header fields | 12 |
| 5.2.4.2 | 2 Check that IUT sends digest as sender info | 13 |
| 5.2.4.3 | | |
| 5.2.4.4 | | |
| 5.2.4.5 | 1 | |
| 5.2.4.6 | | |
| 5.2.4.7 | e e e e e e e e e e e e e e e e e e e | |
| 5.2.4.8 | | |
| 5.2.4.9 5.2.4.1 | | |
| 5.2.4.1 5.2.4.1 | • | |
| 5.2.4.1 5.2.4.1 | 1 | |
| 5.2. 4 .1 | DENM profile | |
| 5.2.5.1 | | |
| 5.2.5.2 | | |
| 5.2.5.3 | S C C C C C C C C C C C C C C C C C C C | |
| 5.2.5.4 | | |
| 5.2.5.5 | 5 Check secured DENM its_aid value | 27 |
| 5.2.5.6 | 6 Check Payload | 27 |
| 5.2.5.7 | | |
| 5.2.5.8 | S C C C C C C C C C C C C C C C C C C C | |
| 5.2.6 | Generic signed message profile | |
| 5.2.6.1 | | |
| 5.2.6.2 | · · · · · · · · · · · · · · · · · · · | |
| 5.2.6.3 5.2.6.7 | <u> </u> | |
| 5.2.6.4 5.2.6.5 | | |
| 5.2.6.c 5.2.6.6 | * • | |
| 5.2.0.0 5.2.7 | Profiles for certificates | |
| 5.2.7 5.2.7.1 | | |
| | | |

| 5.2.7.2 | Check the certificate chain | |
|---|---|--|
| 5.2.7.3 | Geographical regions | |
| 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 | |
| 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 | |
| 5.2.7.7.3 | Check that signer info is a digest | 47 |
| 5.2.7.7.4 | Check subject attributes presence and order | |
| 5.2.7.7.5 | Check the time_start_and_end presence | |
| 5.2.7.7.6 | Check verification key validity | |
| 5.2.7.7.7 | Check ITS-AID | |
| 5.2.7.7.8 | Check that AA cert is signed by Root cert | |
| 5.2.7.7.9 | Check validity restriction presence and order | |
| 5.2.7.8 | AT certificate profile | |
| 5.2.7.8.1 | Check subject type | |
| 5.2.7.8.2 | Check that signer info is a digest | |
| 5.2.7.8.3 | Check subject name | |
| 5.2.7.8.4 | Check the presence and the order of subject attributes | |
| 5.2.7.8.5 | Check presence of time_start_and_end validity restriction | |
| 5.2.7.8.6 | Check verification key validity | |
| 5.2.7.8.7 | Check ITS-AID-SSP | |
| 5.2.7.8.8 | Check that AT certificate is signed by AA cert | |
| 5.2.7.8.9 | Check assurance level | |
| 5.2.7.8.10 | | |
| 5.3 | Receiver Behaviour | |
| 5.3.1 | Overview | |
| 5.3.2 | CAM Profile | |
| 5.3.2.1 | Check that IUT accepts well-formed Secured CAM | |
| 5.3.2.2 | Check the message protocol version | |
| 5.3.2.3 | Check header fields | |
| 5.3.2.4 | Check signer info | |
| 5.3.2.5 | Check generation time | |
| 5.3.2.6 | Check its_aid | |
| 5.3.2.7 | Check payload | |
| 5.3.2.8 | Check presence of trailer field | |
| 5.3.2.9 | Check signature | |
| 5.3.2.10 | Check signing certificate type | |
| 5.3.3 | DENM Profile | |
| 5.3.3.1 | Check that IUT accepts well-formed Secured DENM | |
| 5.3.3.2 | Check the message protocol version | |
| 5.3.3.3 | Check header fields | |
| 5.3.3.4 | | |
| | Check signer info | |
| 3.3.3.3 | Check signer info | |
| 5.3.3.5 5.3.3.6 | Check generation time | 91 |
| 5.3.3.6 | Check generation time | 91 93 |
| 5.3.3.6 5.3.3.7 | Check generation time Check its_aid Check generation location | 91 93 93 |
| 5.3.3.6 5.3.3.7 5.3.3.8 | Check generation time | 91 93 93 |
| 5.3.3.6 5.3.3.7 5.3.3.8 5.3.3.9 | Check generation time Check its_aid Check generation location Check Payload Check presence of trailer field. | |
| 5.3.3.6 5.3.3.7 5.3.3.8 5.3.3.9 5.3.3.10 | Check generation time Check its_aid Check generation location Check Payload Check presence of trailer field Check signature | 91 93 93 95 95 97 |
| 5.3.3.6 5.3.3.7 5.3.3.8 5.3.3.9 5.3.3.10 5.3.3.11 | Check generation time Check its_aid Check generation location Check Payload Check presence of trailer field Check signature Check signing certificate type | 91 93 93 95 95 97 98 |
| 5.3.3.6 5.3.3.7 5.3.3.8 5.3.3.9 5.3.3.10 5.3.3.11 5.3.4 | Check generation time Check its_aid Check generation location Check Payload Check presence of trailer field Check signature. Check signing certificate type. Generic Signed Message Profile. | 91 93 93 95 95 97 98 99 |
| 5.3.3.6 5.3.3.7 5.3.3.8 5.3.3.9 5.3.3.10 5.3.3.11 5.3.4 5.3.4.1 | Check generation time Check its_aid Check generation location Check Payload Check presence of trailer field Check signature Check signing certificate type Generic Signed Message Profile Check that IUT accepts well-formed GN Beacon message | 91 93 93 95 95 97 98 99 100 |
| 5.3.3.6 5.3.3.7 5.3.3.8 5.3.3.9 5.3.3.10 5.3.3.11 5.3.4.1 5.3.4.1 | Check generation time Check its_aid Check generation location Check Payload Check presence of trailer field Check signature Check signing certificate type Generic Signed Message Profile Check that IUT accepts well-formed GN Beacon message Check the message protocol version | 91 93 95 95 97 98 99 100 100 |
| 5.3.3.6 5.3.3.7 5.3.3.8 5.3.3.9 5.3.3.10 5.3.3.11 5.3.4 5.3.4.1 5.3.4.2 5.3.4.3 | Check generation time Check its_aid Check generation location Check Payload Check presence of trailer field Check signature Check signing certificate type Generic Signed Message Profile Check that IUT accepts well-formed GN Beacon message Check the message protocol version Check header fields | 91 93 93 95 95 97 98 99 100 100 |
| 5.3.3.6 5.3.3.7 5.3.3.8 5.3.3.9 5.3.3.10 5.3.3.11 5.3.4 5.3.4.1 5.3.4.2 5.3.4.3 5.3.4.3 | Check generation time Check its_aid Check generation location Check Payload Check presence of trailer field Check signature Check signing certificate type Generic Signed Message Profile Check that IUT accepts well-formed GN Beacon message Check the message protocol version Check header fields Check signer info | 91 93 93 95 97 98 99 100 100 106 |
| 5.3.3.6 5.3.3.7 5.3.3.8 5.3.3.9 5.3.3.10 5.3.3.11 5.3.4 5.3.4.1 5.3.4.2 5.3.4.3 | Check generation time Check its_aid Check generation location Check Payload Check presence of trailer field Check signature Check signing certificate type Generic Signed Message Profile Check that IUT accepts well-formed GN Beacon message Check the message protocol version Check header fields | 91 93 93 95 95 97 98 99 100 106 107 110 |

| 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 | |
| 5.3.5.1 | Check that certificate version is 2 | |
| 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 | |
| 5.3.5.6 | Check circular region of subordinate certificate | |
| 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 | |
| 5.3.5.13 | Check AID-SSP subject attribute value conforming to the issuing certificate | 145 |
| Annex A | (informative): Bibliography | 146 |
| History | | 147 |
| | | |

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 <u>ETSI Drafting Rules</u> (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></x></sn></rn></sgr></gr></tgt></root> | | |
|------------|---|------|--------------------------|
| | <root> = root</root> | SEC | |
| | <tgt> = target</tgt> | ITSS | ITS-S data transfer |
| | | AA | ITS-S - AA authorization |
| | | EA | ITS-S - EA enrolment |
| | <gr> = group</gr> | SND | Sending behaviour |
| | | RCV | Receiving behaviour |
| | <sgr> =sub- group</sgr> | MSG | Generic messages |
| | | CAM | CAM testing |
| | | DENM | DENM testing |
| | | CERT | Certificate testing |
| | <rn> = requirement sequential number</rn> | | 01 to 99 |
| | <sn> = test purpose sequential number</sn> | | 01 to 99 |
| | <x> = category</x> | BV | Valid Behaviour tests |
| | | ВО | 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
                 ETSI TS 103 097 [1], clause 5.2
Reference
PICS Selection
                 PICS_GN_SECURITY
                                          Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
    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
                 Check that when IUT sends the message signed with the digest, then this digest points to the AT
Summary
                 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 ld | 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 |
| the IUT being } ensure that { when { the IUT is r } then { the IUT send containing containi contai indi contai contai | <pre>in the 'authorized' state requested to include certificate in the next CAM equested to send a next CAM s a SecuredMessage header_fields ['signer_info'] { ng signer { ning type cating 'certificate' ning certificate aining subject_info.subject_type dicating 'authorization_ticket'</pre> |

5.2.3 Check Signature ECC point type

| TP Id | TP_SEC_ITSS_SND_MSG_05_01_BV | | |
|--|---|--|--|
| Summary | ummary 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>} ensure that { when { the IUT is r } then { the IUT send containing containi indica and contai containi containi contai indi contai indi contai contai indi or i</pre> | equested to send a CAM s a SecuredMessage { header_fields ['its_aid'] ng its_aid ting 'AID_CAM' ning trailer_fields['signature'] ng signature.ecdsa_signature ning R.type cating compressed_lsb_y_0 ndicating compressed_lsb_y_1 ndicating x_coordinate_only | | |
| } } } | | | |

5.2.4 CAM profile

5.2.4.1 Check header fields

| TP ld | 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 |
| <pre>} ensure that { when { the IUT is r } then { the IUT send containing containinindica and containinindicati and containininininininininininininininininini</pre> | equested to send a CAM s a SecuredMessage { header_fields[0] ng type ting 'signer_info' ning header_fields [n].type ng value < header_fields [n+1].type ning header_fields ['generation_time'] ning header_fields['its_aid'] ng 'AID_CAM' ntaining header_fields['generation_time_standard_deviation'] ntaining header_fields['expiration'] ntaining header_fields['encryption_parameters'] ntaining header_fields['recipient_info'] |

5.2.4.2 Check that IUT sends digest as sender info

| TP ld | 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 |
| and the IUT is and the IUT ha containing h indicating contains hea | in the 'authorized' state s configured to send more than one CAM per second aving sent a CAM leader_fields['signer_info'].signer.type g 'certificate' lder_fields['generation_time'] g TIME_LAST |
| | ds one of the next SecuredMessage g header_fields['signer_info'] { |
| containi contai indi | .ng signer { .ning type .cating 'certificate' .ning certificate |
| indicati } then { this message contains h | <pre>g header_fields['its_aid'] ing 'AID_CAM' deader_fields['generation_time'] ing TIME (TIME >= TIME_LAST + 1sec)</pre> |

| TP ld | 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 | | |
| Guillillai y | 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 hav | ving sent a CAM | | |
| _ | eader_fields['signer_info'].signer.type | | |
| indicating | 'certificate' | | |
| at TIME_1 | | | |
| } | | | |
| ensure that { | | | |
| when { | | | |
| | equested to send next CAM right after 1 second after the TIME_1 | | |
| } then { | To Garward Marraya (| | |
| | s a SecuredMessage { | | |
| _ | containing header_fields['its_aid'] | | |
| | indicating 'AID_CAM' | | |
| | <pre>containing header_fields ['signer_info'] { containing signer {</pre> | | |
| | containing signer { containing type | | |
| | indicating 'certificate' | | |
| | containing certificate | | |
| } | } | | |
| } ' | | | |
| } ' | | | |
| } | | | |
| } | | | |

5.2.4.3 Check that IUT sends cert to unknown ITS-S

| TP ld | TP_SEC_ITSS_SND_CAM_06_01_BV |
|----------------|---|
| Summary | Check that ITS-S sends a Secured CAM containing the signer_info of type certificate when the ITS-S received a CAM from an unknown ITS-S |
| 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 already sent CAM at TIME_1
   containing header_fields['signer_info'].signer.type
     indicating 'certificate'
 and the IUT having received a SecuredMessage
             at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec)
    containing header_fields['its_aid']
     indicating 'AID_CAM'
   containing header_fields['signer_info'] {
     containing signer
       containing type
         indicating 'certificate_digest_with_sha256'
       containing digest
         indicating HashedId3 value
           referenced to unknown certificate
   }
ensure that {
 when {
   the IUT is requested to send CAM
         at TIME_3 (TIME_1 < TIME_2 < TIME_3 < TIME_1 + 1sec)
  } then {
   the IUT sends a SecuredMessage {
     containing header_fields['its_aid']
      indicating 'AID_CAM'
     containing header_fields[0] {
       containing type
         indicating 'signer_info'
       containing signer {
         containing type
           indicating 'certificate'
         containing certificate
     }
 }
```

5.2.4.4 Check that IUT restarts the timer when the certificate has been sent

| TP Id TP_SEC_ITSS_SND_CAM_07a_01_TI Summary Check that IUT restarts the certificate sending timer when the certificate has been sent Reference ETSI TS 103 097 [1], clause 7.1 PICS Selection PICS_GN_SECURITY Expected behaviour |
|---|
| Reference ETSI TS 103 097 [1], clause 7.1 PICS Selection PICS_GN_SECURITY |
| 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 already sent CAM at TIME_1 containing header_fields['signer_info'].signer.type indicating 'certificate' and the IUT having received a CAM</pre> |

5.2.4.5 Check that IUT sends certificate when requested

| TP ld | TP_SEC_ITSS_SND_CAM_08_01_BV |
|----------------|---|
| Summary | Check that the IUT sends the Secured CAM containing the signer_info of type certificate when it received a CAM containing a request of unrecognized certificate that matches with the currently used AT certificate ID of the IUT |
| 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 already sent CAM at {\tt TIME\_1}
   containing header_fields['signer_info'].signer.type
     indicating 'certificate'
 and the IUT having received a SecuredMessage
           at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec)
   containing header_fields['request_unrecognized_certificate']
     containing digests {
       containing HashedId3 value
         referencing to the AT certificate
       and not containing HashedId3 value
         referencing to the AA certificate
ensure that {
 when {
   the IUT is requested to send a CAM
       at TIME_3 (TIME_1 < TIME_2 < TIME_3 < TIME_1+1sec)
   the IUT sends a SecuredMessage {
     containing security_profile
       indicating '1'
     containing header_fields['signer_info'] {
       containing signer {
         containing type
           indicating 'certificate'
         containing certificate
           referenced by the requested digest
 }
```

5.2.4.6 Check that IUT send certificate_chain when requested

| TP ld | TP_SEC_ITSS_SND_CAM_09_01_BV | | |
|----------------|---|--|--|
| Summary | Check that the sent secured CAM contains the signer_info of type certificate_chain when the ITS-S has received a CAM containing a request of unrecognized certificate that matches with the AA certificate ID that issued its currently used AT certificate ID of the IUT | | |
| Reference | ETSI TS 103 097 [1], clause 7.1 | | |
| PICS Selection | PICS_GN_SECURITY | | |
| | Expected behaviour | | |
| and the IUT is | in the 'authorized' state s configured to send more than one CAM per second aving already sent a CAM | | |

```
containing header_fields['signer_info'].signer.type
     indicating 'certificate'
   at TIME_1
 and the IUT having received a SecuredMessage
   containing header_fields['request_unrecognized_certificate'] {
     containing digests {
       containing HashedId3 value
         referencing to the AA certificate
   at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec)
ensure that {
 when {
   the IUT is requested to send a CAM
     at TIME_3 (TIME_1 < TIME_2 < TIME_3 < TIME_1+1sec)
   the IUT sends a SecuredMessage {
     containing header_fields['its_aid']
       indicating 'AID_CAM'
     containing header_fields['signer_info'] {
       containing signer {
         containing type
           indicating 'certificate_chain'
         containing certificates[last]
           indicating the AT certificate
         containing certificates[last-1]
           indicating the AA certificate
     }
   }
 }
```

5.2.4.7 Check generation time

```
TP Id
                 TP_SEC_ITSS_SND_CAM_10_01_BV
                 Check that message generation time is inside the validity period of the signing certificate;
Summary
                 Check that message generation time value is realistic
                 ETSI TS 103 097 [1], clauses 5.4 and 7.1
Reference
                 PICS_GN_SECURITY
PICS Selection
                                           Expected behaviour
  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 CAM
  } then {
    the IUT sends a SecuredMessage {
      containing header_fields ['generation_time'] {
        containing generation_time
          indicating TIME_1 (CUR_TIME - 5min <= TIME_1 <= CUR_TIME + 5min)</pre>
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate {
            not containing validity_restrictions['time_start_and_end']
            or containing validity_restrictions['time_start_and_end'] \{
              containing start_validity
                indicating value <= TIME_1
              containing end_validity
                indicating value > TIME_1
          }
        }
      containing its_aid
        indicating 'AID_CAM'
  }
```

5.2.4.8 Check secured CAM its_aid value

| _ | - |
|--|---|
| TP ld | TP_SEC_ITSS_SND_CAM_11_01_BV |
| Summary | Check that the sent Secured CAM contains exactly one 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 |
| with { | |
| <pre>} ensure that { when { the IUT is re } then { the IUT sends containing containing }</pre> | in the 'authorized' state equested to send CAM s a SecuredMessage { header_fields ['its_aid'] { ng its_aid ting 'AID_CAM' |

5.2.4.9 Check sending certificate request to unknown station

```
TP Id
                 TP_SEC_ITSS_SND_CAM_12_01_BV
Summary
                 Check that the IUT sends certificate request when it receives a message from unknown station
                 ETSI TS 103 097 [1], clause 7.1
Reference
PICS Selection
                 PICS_GN_SECURITY
                                          Expected behaviour
with {
  the IUT being in the 'authorized' state
  and the IUT has receiving a SecuredMessage {
    containing header_fields['signer_info'].signer {
      containing type
        indicating 'certificate_digest_with_sha256'
      containing digest
        indicating HashedId3 value DIGEST_A
          referenced to unknown certificate
  }
ensure that {
 when {
    the IUT is requested to send CAM
    the IUT sends a SecuredMessage {
      containing header_fields['request_unrecognized_certificate'] {
        containing digests
          containing HashedId3 value
            indicating DIGEST_A
      containing header_fields ['its_aid'] {
        containing its_aid
          indicating 'AID_CAM'
  }
```

5.2.4.10 Check Payload

| TP Id | TP_SEC_ITSS_SND_CAM_14_01_BV |
|--|--|
| Summary | Check that the Secured CAM contains non-empty payload of type signed |
| Reference | ETSI TS 103 097 [1], clause 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>} ensure that { when { the IUT is r } then { the IUT send containing containing</pre> | in the 'authorized' state equested to send a CAM s a SecuredMessage { header_fields ['its_aid'] { ng its_aid ting 'AID_CAM' payload_field { ng type ting 'signed' ng not-empty data |

5.2.4.11 Check presence of trailer field

Void.

5.2.4.12 Check signature

```
TP Id

TP_SEC_ITSS_SND_CAM_16_01_BV

Check that the secured CAM contains only one TrailerField of type signature;
Check that the signature contained in the SecuredMessage is calculated over the right fields by cryptographically verifying the signature

Reference
ETSLTS 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 ['signer_info'] {
       containing signer {
         containing type
           indicating 'certificate_digest_with_ecdsap256'
          containing digest
           referenced to the certificate
              containing subject_info.subject_type
                indicating 'authorization_ticket' (2)
              and containing subject_attributes['verification key'] (KEY)
        or containing signer {
          containing type
            indicating 'certificate'
          containing certificate
            containing subject_info.subject_type
             indicating 'authorization_ticket' (2)
            and containing subject_attributes['verification key'] (KEY)
      containing header_fields ['its_aid'] {
       containing its_aid
          indicating 'AID_CAM'
      containing trailer_fields {
       containing single instance of type TrailerField {
          containing type
            indicating 'signature'
          containing signature
           verifiable using KEY
     }
   }
```

5.2.5 DENM profile

5.2.5.1 Check header fields

```
TP Id
                   TP_SEC_ITSS_SND_DENM_02_01_BV
                  Check that the secured DENM contains exactly one element of these header fields: signer_info,
                  generation_time, generation_location, message_type
Summary
                  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_with_confidence (generation_time_standard_deviation) is not used
Reference
                   ETSI TS 103 097 [1], clause 7.2
PICS Selection
                  PICS GN SECURITY
                                             Expected behaviour
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is requested to send DENM
  } then {
    the IUT sends a SecuredMessage {
      containing header_fields[0]
        containing type
           indicating 'signer_info'
      containing header_fields [n].type
        indicating value less than header_fields [n+1].type
      containing header_fields ['generation_time']
      containing header_fields ['generation_location'] containing header_fields ['its_aid'] {
         containing its_aid
           indicating 'AID_DENM'
      not containing header_fields ['generation_time_with_confidence']
  }
```

5.2.5.2 Check that signer info is a certificate

```
TP Id
                  TP_SEC_ITSS_SND_DENM_03_01_BV
Summary
                  Check that secured DENM contains the certificate as a signer_info
Reference
                  ETSI TS 103 097 [1], clause 7.2
PICS Selection
                 PICS_GN_SECURITY
                                           Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
  \quad \text{when } \{
    the IUT is requested to send a DENM
  } then {
    the IUT sends a SecuredMessage {
      containing header_fields['signer_info']{
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate
      }
 }
```

5.2.5.3 Check generation time

| TP ld | TP_SEC_ITSS_SND_DENM_04_01_BV | | |
|--|---|--|--|
| Summary | Check that message generation time is inside the validity period of the signing certificate; Check that message generation time value is realistic | | |
| Reference | ETSI TS 103 097 [1], clauses 5.4 and 7.2 | | |
| 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 DENM
  } then {
    the IUT sends a SecuredMessage {
      containing exactly one header_fields['generation_time'] {
        containing generation_time
          indicating TIME_1 (CUR_TIME - 10min <= TIME_1 <= CUR_TIME + 5min)</pre>
      containing header_fields['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate {
            containing validity_restrictions['time_start_and_end'] {
              containing start_validity
                indicating value <= TIME_1</pre>
              containing end_validity
                indicating value > TIME_1
            or not containing validity_restrictions['time_start_and_end']
        }
     }
   }
```

5.2.5.4 Check generation location

| TP Id | TP_SEC_ITSS_SND_DENM_05_01_BV |
|--|---|
| Summary | Check that the secured DENM contains exactly one HeaderField generation_location when AT certificate does not contain any region restrictions |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY |
| | Expected behaviour |
| with { the IUT has been authorized with the AT certificate (CERT_IUT_A_AT) not containing validity_restrictions['region'] } ensure that { when { the IUT is requested to send DENM } then { the IUT sends a SecuredMessage { containing exactly one header_field ['generation_location'] containing generation_location containing header_field ['its_aid'] { containing its_aid | |

```
TP Id
                 TP_SEC_ITSS_SND_DENM_05_02_BV
                 Check that the secured DENM contains exactly one HeaderField generation_location which is
Summary
                 inside the circular region containing in the validity restriction of the certificate pointed by the
                 signer_info field
                 ETSI TS 103 097 [1], clause 7.2
Reference
PICS Selection
                 PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_CIRCULAR_REGION
                                          Expected behaviour
with {
 the IUT has been authorized with the AT certificate (CERT_IUT_B_AT) {
    containing validity_restrictions ['region'] {
      containing region{
        containing region_type
          indicating 'circle'
        containing circular_region
          indicating REGION
   }
ensure that {
  when {
    the IUT is requested to send a DENM
  } then {
    the IUT sends a SecuredMessage {
      containing exactly one header_field ['generation_location']
        containing generation_location
         indicating value inside the REGION
      containing header_field ['its_aid'] {
        containing its_aid
          indicating 'AID_DENM'
    }
  }
```

| TP Id | TP_SEC_ITSS_SND_DENM_05_03_BV |
|---|--|
| Summary | Check that the secured DENM contains exactly one HeaderField generation_location which is inside the rectangular region containing in the validity restriction of the certificate pointed by the signer_info field |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION |
| | Expected behaviour |
| containing voor containing | en authorized with the AT certificate (CERT_IUT_C_AT) { alidity_restrictions ['region'] { region{ ng region_type ting 'rectangle' ng rectangular_region ning instance of RectangularRegion cating REGION equested to send DENM s a SecuredMessage { exactly one header_field ['generation_location'] ng generation_location ting value inside the REGION header_field ['its_aid'] { ng its_aid ting 'AID_DENM' |

```
TP Id TP_SEC_ITSS_SND_DENM_05_04_BV
Check that the secured DENM contains exactly one HeaderField generation_location which is inside the polygonal region containing in the validity restriction of the certificate pointed by the signer_info field

Reference ETSLTS 103 097 [1], clause 7.2

PICS Selection PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION

Expected behaviour

with {
    the IUT has been authorized with the AT certificate (CERT_IUT_D_AT) {
```

```
the IUT has been authorized with the AT certificate (CERT_IUT_D_AT) {
   containing validity_restrictions ['region'] {
      containing region{
       containing region_type
          indicating 'polygon'
        containing polygonal_region
          indicating REGION
   }
  }
ensure that {
 when {
   the IUT is requested to send a DENM
  } then {
   the IUT sends a SecuredMessage {
     containing exactly one header_field ['generation_location']
       containing generation_location
          indicating value inside the REGION
      containing header_field ['its_aid'] {
        containing its_aid
          indicating 'AID_DENM'
   }
  }
```

| TP Id | TP_SEC_ITSS_SND_DENM_05_05_BV |
|--------------------|---|
| Summary | Check that the secured DENM contains exactly one HeaderField generation_location which is inside the identified region containing in the validity restriction of the certificate pointed by the signer_info field |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION |
| Expected behaviour | |

```
with {
  the IUT has been authorized with the AT certificate (CERT_IUT_E_AT) {
    containing validity_restrictions ['region'] {
     containing region{
        containing region_type
          indicating 'id_region'
        containing identified_region
          indicating REGION
   }
  }
ensure that {
 when {
    the IUT is requested to send a DENM
  } then {
    the IUT sends a SecuredMessage {
      containing header_fields {
        containing exactly one instance of HeaderField {
          containing type
           indicating 'generation_location'
          containing generation_location
            indicating value inside the {\tt REGION}
          containing header_field ['its_aid'] {
            containing its_aid
indicating 'AID_DENM'
    }
 }
```

```
TP Id TP_SEC_ITSS_SND_DENM_05_06_BV

Summary Check that the secured GeoNetworking message contains exactly one HeaderField generation_location and this location is inside the certificate validation restriction

Reference ETSI TS 103 097 [1], clause 7.2

PICS Selection !PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY
```

```
Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is requested to send a DENM
  } then {
   the IUT sends a SecuredMessage {
      containing header_fields['signed_info'].certificate {
        containing validity_restrictions ['region']
          containing region.region_type
            indicating 'circle'
          containing region.circular_region
           indicating REGION
        } or {
          containing region.region_type
            indicating 'rectangle'
          containing region.rectangular_region
            containing array of rectangles
              indicating REGION
          containing region.region_type
           indicating 'polygonal'
          containing region.polygonal_region
            indicating REGION
        } or {
          containing region.region_type
           indicating 'id_region'
          containing region.circular_region
            indicating REGION
       }
      }
      containing exactly one header_field ['generation_location']
        containing generation_location
          indicating location inside the REGION
      containing header_field ['its_aid'] {
        containing its_aid
          indicating 'AID_DENM'
   }
  }
```

5.2.5.5 Check secured DENM its_aid value

| TP ld | TP_SEC_ITSS_SND_DENM_06_01_BV |
|--|---|
| Summary | Check that the sent Secured DENM contains exactly one HeaderField its_aid that is set to 'AID_DENM' |
| Reference | ETSI TS 103 097 [1], clauses 5.4 and 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>} ensure that { when { the IUT is re } then { the IUT sends containing containing }</pre> | in the 'authorized' state equested to send a DENM s a SecuredMessage { header_fields ['its_aid'] ng its_aid ting 'AID_DENM' |

5.2.5.6 Check Payload

| TP Id | TP_SEC_ITSS_SND_DENM_08_01_BV | | |
|---|---|--|--|
| | | | |
| Summary | Check that the Secured DENM contains non-empty payload of type signed | | |
| Reference | ETSI TS 103 097 [1], clause 7.2 | | |
| PICS Selection | PICS_GN_SECURITY | | |
| | Expected behaviour | | |
| with { | | | |
| the IUT being | in the 'authorized' state | | |
| } | | | |
| ensure that { | | | |
| when { | | | |
| | equested to send a DENM | | |
| } then { | | | |
| | the IUT sends a SecuredMessage $\{$ | | |
| _ | header_fields ['its_aid'] { | | |
| | containing its_aid | | |
| indicating 'AID_DENM' | | | |
|] gontaining | } | | |
| <pre>containing payload_field { containing type</pre> | | | |
| indicating 'signed' | | | |
| containing not-empty data | | | |
| } | | | |
| } | | | |
| | | | |
| } | | | |

5.2.5.7 Check trailer field presence

Void.

5.2.5.8 Check signature

| TP Id | TP_SEC_ITSS_SND_DENM_10_01_BV |
|--------------------|--|
| Summary | Check that the secured DENM contains only one TrailerField of type signature; Check that the signature contained in the SecuredMessage is calculated over the right fields by cryptographically verifying the signature |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with {
  the IUT being in the 'authorized' state
ensure that {
  when {
   the IUT is requested to send DENM
  } then {
    the IUT sends a SecuredMessage {
     containing header_field ['signer_info'] {
       containing signer {
         containing type
           indicating 'certificate'
         containing certificate
           containing subject_info.subject_type
             indicating 'authorization_ticket' (2)
           and containing subject_attributes['verification key'] (KEY)
       }
      containing header_fields ['its_aid'] {
       containing its_aid
         indicating 'AID_DENM'
      containing trailer_fields {
       containing single instance of type TrailerField {
         containing type
           indicating 'signature'
          containing signature
           verifiable using KEY
 }
     }
```

5.2.6 Generic signed message profile

5.2.6.1 Check header field

| TP ld | TP_SEC_ITSS_SND_GENMSG_02_01_BV |
|---|---|
| Summary | Check that the generic secured message contains exactly one element of these header fields: signer_info, generation_time, generation_location 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 |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE |
| | Expected behaviour |
| <pre>with { the IUT being in the 'authorized' state } ensure that { when { the IUT is requested to send a Beacon } then { the IUT sends a SecuredMessage { containing header_fields [0].type indicating 'signer_info' containing header_fields [1n] where header_fields [i].type < header_fields [i+1].type containing header_fields ['generation_time'] containing header_fields ['generation_location'] containing header_fields ['its_aid'] indicating 'AID_BEACON' } }</pre> | |

5.2.6.2 Check that signer info is a certificate

```
TP Id
                 TP_SEC_ITSS_SND_GENMSG_03_01_BV
Summary
                 Check that generic secured message contains the certificate as a signer_info
Reference
                 ETSI TS 103 097 [1], clause 7.3
PICS Selection
                 PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE
                                          Expected behaviour
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is requested to send a Beacon
  } then {
    the IUT sends a SecuredMessage {
      containing header_fields ['its_aid']
        indicating 'AID_BEACON'
      containing exactly one header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate
    }
```

5.2.6.3 Check generation time

| TP ld | TP_SEC_ITSS_SND_GENMSG_04_01_BV | |
|---|--|--|
| Summary | Check that message generation time is inside the validity period of the signing certificate; | |
| | Check that message generation time value is realistic | |
| Reference | ETSI TS 103 097 [1], clauses 5.4 and 7.3 | |
| PICS Selection | PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE | |
| | Expected behaviour | |
| with { | | |
| the IUT being | in the 'authorized' state | |
| } | | |
| ensure that { | | |
| when { | requested to send a Beacon | |
| } then { | equested to send a Beacon | |
| the IUT sends a SecuredMessage { | | |
| | header_fields ['its_aid'] | |
| | ng 'AID_BEACON' | |
| | rexactly one header_fields['generation_time'] { | |
| | ng generation_time | |
| indicating TIME_1 (CUR_TIME - 10min <= TIME_1 <= CUR_TIME + 5min) | | |
| } | } | |
| _ | header_fields['signer_info'] { | |
| <pre>containing signer { containing type</pre> | | |
| indicating 'certificate' | | |
| containing certificate { | | |
| | aining validity_restrictions['time_start_and_end'] { | |
| cc | ontaining start_validity | |
| | indicating value <= TIME_1 | |
| CC | ontaining end_validity | |
| indicating value > TIME_1 | | |
| } | or containing unlights workering price of the and and 1 | |
| or n | ot containing validity_restrictions['time_start_and_end'] | |

5.2.6.4 Check generation location

| TP Id TP_SEC_ITSS_SND_GENMSG_05_01_BV | | |
|--|--|--|
| Summary Check that the secured GeoNetworking message contains exactly one HeaderField generation_location when AT certificate does not contain any region restrictions | | |
| Reference | ETSI TS 103 097 [1], clause 7.3 | |
| PICS Selection | PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE | |
| Expected behaviour | | |
| <pre>with { the IUT has been authorized with the AT certificate (CERT_AT_A) does not containing validity_restrictions['region'] } ensure that { when { the IUT is requested to send a Beacon } then { the IUT sends a SecuredMessage { containing header_fields ['its_aid'] indicating 'AID_BEACON' containing exactly one header_fields['generation_location'] containing generation_location } }</pre> | | |

```
TP Id

TP_SEC_ITSS_SND_GENMSG_05_02_BV

Check that the secured GeoNetworking message contains exactly one HeaderField generation_location which is inside the circular region containing in the validity restriction of the certificate pointed by the signer_info field

Reference

ETSI TS 103 097 [1], clause 7.3

PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE, PICS_USE_CIRCULAR_REGION

Expected behaviour

with {
    the IUT has been authorized with the AT certificate (CERT_AT_B) {
    containing validity restrictions ['region'] {
}
```

```
containing validity_restrictions ['region'] {
      containing region{
       containing region_type
          indicating 'circle'
        containing circular_region
          indicating REGION
   }
  }
ensure that {
 when {
   the IUT is requested to send a Beacon
  } then {
   the IUT sends a SecuredMessage {
     containing header_fields ['its_aid']
       indicating 'AID_BEACON'
      containing exactly one header_fields['generation_location']
        containing generation_location
          indicating value inside the REGION
  }
```

| TP ld | TP_SEC_ITSS_SND_GENMSG_05_03_BV |
|---|---|
| C | Check that the secured GeoNetworking message contains exactly one HeaderField |
| Summary | generation_location which is inside the rectangular region containing in the validity restriction of the certificate pointed by the signer_info field |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE, PICS_USE_RECTANGULAR_REGION |
| | Expected behaviour |
| with { | 2 |
| the IUT has be | en authorized with the AT certificate (CERT_AT_C) { |
| | validity_restrictions ['region'] { |
| containing | |
| | ng region_type |
| | ting 'rectangle' |
| | ng rectangular_region |
| | ning instance of RectangularRegion |
| indi | cating REGION |
| } | |
| } | |
| 1 | |
| ensure that { | |
| when { | |
| the IUT is requested to send a Beacon | |
| then { | |
| the IUT sends a SecuredMessage { | |
| containing header_fields ['its_aid'] | |
| indicating 'AID_BEACON' | |
| containing exactly one header_fields['generation_location'] | |
| containing generation_location | |
| indica | ting value inside the REGION |
| } | |

```
TP Id
                  TP_SEC_ITSS_SND_GENMSG_05_04_BV
                  Check that the secured GeoNetworking message contains exactly one HeaderField
Summary
                  generation_location which is inside the polygonal region containing in the validity restriction of the
                  certificate pointed by the signer_info field
Reference
                  ETSI TS 103 097 [1], clause 7.3
                  PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE,
PICS Selection
                  PICS_USE_POLYGONAL_REGION
                                           Expected behaviour
with {
 the IUT has been authorized with the AT certificate (CERT_AT_D) {
    containing validity_restrictions ['region'] {
      containing region{
```

```
containing region_type
          indicating 'polygon'
        containing polygonal_region
          indicating REGION
   }
  }
ensure that {
 when \{
    the IUT is requested to send a Beacon
  } then {
    the IUT sends a SecuredMessage {
     containing header_fields ['its_aid']
        indicating 'AID_BEACON'
      containing exactly one header_fields['generation_location']
        containing generation_location
          indicating value inside the REGION
   }
  }
```

TP_SEC_ITSS_SND_GENMSG_05_05_BV

containing exactly one header_fields['generation_location']

containing generation_location

indicating value inside the REGION

TP Id

}

| Summary | Check that the secured GeoNetworking message contains exactly one HeaderField generation_location which is inside the identified region containing in the validity restriction of the certificate pointed by the signer_info field | |
|---|--|--|
| Reference | ETSI TS 103 097 [1], clause 7.3 | |
| PICS Selection | PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE, PICS_USE_IDENTIFIED_REGION | |
| Expected behaviour | | |
| with { | | |
| <pre>the IUT has been authorized with the AT certificate (CERT_AT_E) { containing validity_restrictions ['region'] { containing region{ containing region_type indicating 'id_region' containing identified_region indicating REGION } } }</pre> | | |
| when { the IUT is n } then { the IUT send containing | requested to send a Beacon ds a SecuredMessage { g header_fields ['its_aid'] | |
| indicating 'AID_BEACON' | | |

```
TP Id TP_SEC_ITSS_SND_GENMSG_05_06_BV

Summary Check that the secured GeoNetworking message contains exactly one HeaderField generation_location and this location is inside the certificate validation restriction

Reference ETSI TS 103 097 [1], clause 7.3

PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE
```

```
Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is requested to send a Beacon
  } then {
   the IUT sends a SecuredMessage {
      containing header_fields['signed_info'].certificate {
        containing validity_restrictions ['region']
          containing region.region_type
            indicating 'none'
        } or {
          containing region.region_type
            indicating 'circle'
          containing region.circular_region
           indicating REGION
        } or {
          containing region.region_type
            indicating 'rectangle'
          containing region.rectangular_region
            containing array of rectangles
              indicating REGION
        } or {
          containing region.region_type
            indicating 'polygonal'
          containing region.polygonal_region
           indicating REGION
        } or {
          containing region.region_type
            indicating 'id_region'
          containing region.circular_region
            indicating REGION
      containing exactly one header_fields['generation_location']
        containing generation_location
          indicating location inside the REGION
      containing header_fields ['its_aid']
        indicating 'AID_BEACON'
  }
```

5.2.6.5 Check payload

```
TP Id
                 TP_SEC_ITSS_SND_GENMSG_06_01_BV
                 Check that the secured message contains the Payload element of type signed, signed_external or
Summary
                 signed_and_encrypted
                 ETSI TS 103 097 [1], clause 7.3
Reference
                 PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE
PICS Selection
                                          Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
    the IUT is requested to send a Beacon
  } then {
    the IUT sends a SecuredMessage {
      containing header_fields ['its_aid']
        indicating 'AID_BEACON'
      and containing payload_field {
        containing type
          indicating 'signed' or 'signed_external' or 'signed_and_encrypted'
    }
  }
```

5.2.6.6 Check signature

```
TP Id
                  TP_SEC_ITSS_SND_GENMSG_07_01_BV
                  Check that the secured message contains only one TrailerField of type signature;
Summary
                  Check that the signature contained in the SecuredMessage is calculated over the right fields by
                  cryptographically verifying the signature
                  ETSI TS 103 097 [1], clause 7.3
Reference
PICS Selection
                  PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE
                                           Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is requested to send a Beacon
  } then {
    the IUT sends a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate
            indicating CERT
      containing header_fields ['its_aid']
        indicating 'AID_BEACON'
      containing trailer_fields ['signature']
        containing signature
          verifiable using CERT.subject_attributes['verification_key']
   }
```

5.2.7 Profiles for certificates

5.2.7.1 Check that certificate version is 2

```
TP Id
                       TP_SEC_ITSS_SND_CERT_01_01_BV
Summary
                       Check that AT certificate has version 2
Reference
                       ETSI TS 103 097 [1], clauses 6.1 and 7.4
PICS Selection
                       PICS_GN_SECURITY
                                          Expected behaviour
with {
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate in the SecuredMessage
} ensure that {
  when {
    the IUT is requested to send a SecuredMessage
  } then {
    the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
        containing type
          indicating certificate
        containing certificate {
         containing version
            indicating '2
      }
```

```
TP Id
                       TP_SEC_ITSS_SND_CERT_01_02_BV
Summary
                       Check that AA certificate has version 2
Reference
                       ETSI TS 103 097 [1], clauses 6.1 and 7.4
PICS Selection
                       PICS_GN_SECURITY
                                          Expected behaviour
with {
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate chain in the next CAM
} ensure that {
   when {
    the IUT is requested to send a CAM
  } then {
    the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
        containing type
         indicating certificate_chain
        containing certificates.length >1
        containing certificates[last-1] {
          containing version
            indicating '2
      }
  }
```

5.2.7.2 Check the certificate chain

| TP Id | TP_SEC_ITSS_SND_CERT_02_01_BV | |
|---|---|--|
| Summan. | Check that the certificate chain is valid | |
| Summary | Check signer_info | |
| Reference | ETSI TS 103 097 [1], clause 4.2.10 | |
| PICS Selection | PICS_GN_SECURITY | |
| | Expected behaviour | |
| with { | | |
| the IUT being in the | 'authorized' state | |
| | ed to include certificate chain in the next CAM | |
| } ensure that { | | |
| when { | | |
| | the IUT is requested to send a CAM | |
| } then { | | |
| the IUT sends a Sec | 9 | |
| _ | _fields['signer_info'].signer { | |
| containing type | rtificate chain | |
| containing cert | _ | |
| containing si | | |
| containing | | |
| indicating 'certificate_digest_with_sha256' | | |
| containing digest | | |
| referenced to the certificates[N - 1] | | |
| } | | |
| } | | |
| } | | |
| } | | |
| [} | | |

5.2.7.3 Geographical regions

TP Id

5.2.7.3.1 Check Rectangular regions

TP_SEC_ITSS_SND_CERT_04_01_BV

| | Check that the rectangular certificate validity region contains not more than six valid rectangles Check that the rectangular certificate validity region is continuous and does not contain any holes | | |
|---|---|--|--|
| Reference | ETSI TS 103 097 [1], clauses 4.2.20 and 4.2.23 | | |
| PICS Selection | PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION | | |
| | Expected behaviour | | |
| with { | | | |
| 9 | n the 'authorized' state. | | |
| _ | requested to include certificate in the next CAM | | |
| } ensure that { | | | |
| when { | | | |
| | equested to send a CAM | | |
| } then { | | | |
| | s a SecuredMessage | | |
| | header_fields['signer_info'].signer { | | |
| containir | J 11 | | |
| | ing 'certificate' | | |
| | ng certificate { ning no validity restriction or validity_restrictions['region']{ | | |
| | aining no variatly restriction of variatly_restrictions(region){ | | |
| | dicating 'rectangle' | | |
| | containing rectangular_region { | | |
| | licating length <= 6 | | |
| | containing elements of type RectangularRegion | | |
| indicating continuous region without holes | | | |
| containing northwest and southeast | | | |
| indicating northwest is on the north from southeast | | | |
| } | | | |
| } | | | |
| } | | | |
| } | | | |
| } | | | |

```
TP Id
                    TP_SEC_ITSS_SND_CERT_04_02_BV
                    Check that the rectangular certificate validity region of the subordinate certificate is well formed
Summary
                    and inside the validity region of the issuing certificate
Reference
                    ETSI TS 103 097 [1], clauses 4.2.20 and 4.2.23
                    PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY,
PICS Selection
                    PICS_USE_RECTANGULAR_REGION
                                          Expected behaviour
with {
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate chain in the next CAM
 ensure that {
   when {
    the IUT is requested to send a CAM
  } then {
    the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
        containing type
         indicating 'certificate_chain'
        containing certificates
          indicating CERTIFICATES {
            containing CERTIFICATES[N] {
              containing validity_restrictions['region'] {
                containing region_type
                  indicating 'rectangle'
                containing rectangular_region {
                  indicating length <= 6
                  and containing elements of type RectangularRegion
                    containing northwest and southeast
                      indicating northwest on the north from southeast
                  and indicating continuous region without holes
                    which is inside the CERTIFICATES[N-1].validity_restrictions['region'] if region
validity restriction is contained in certificate CERTIFICATES[N-1]
         }
      }
```

}

5.2.7.3.2 Check Polygonal Region

| TP ld | TP_SEC_ITSS_SND_CERT_05_01_BV | | |
|---|--|--|--|
| Summary | Check that the polygonal certificate validity region contains at least three and no more than 12 points Check that the polygonal certificate validity region does not contain intersections and holes | | |
| Reference | ETSI TS 103 097 [1], clause 4.2.24 | | |
| PICS Selection | PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION | | |
| | Expected behaviour | | |
| with { the IUT being in the 'authorized' state the IUT being requested to include certificate in the next CAM | | | |

```
ensure that {
 \quad \text{when } \{
  the IUT is requested to send a CAM
} then {
  the IUT sends a SecuredMessage
    containing header_fields['signer_info'].signer {
      containing type
        indicating 'certificate'
      containing certificate {
       containing validity_restrictions['region']{
          containing region_type
            indicating 'polygon'
          containing polygonal_region {
            indicating length >= 3 and <= 12
            indicating continuous region without holes and intersections
   } }
}
```

```
TP_Id

TP_SEC_ITSS_SND_CERT_05_02_BV

Check that the polygonal certificate validity region is inside the validity region of the issuing certificate
Check that the issuing polygonal certificate validity region contains at least three and no more than 12 points
Check that the issuing polygonal certificate validity region does not contain intersections and holes

Reference
ETSI TS 103 097 [1], clause 4.2.24

PICS Selection
PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION
Expected behaviour
```

```
with {
 the IUT being in the 'authorized' state
 the IUT being requested to include certificate chain in the next CAM
 ensure that {
  when {
   the IUT is requested to send a CAM
 } then {
   the IUT sends a SecuredMessage
     containing header_fields['signer_info'].signer {
       containing type
         indicating 'certificate_chain'
       containing certificates
         indicating CERTIFICATES {
           containing CERTIFICATES[N] {
             containing validity_restrictions['region'] {
               containing region_type
                 indicating 'polygon'
               containing polygonal_region {
                  indicating length >=3 and <=12
                  indicating continuous region without holes and intersections
                    which is inside the CERTIFICATES[N-1]
                    .validity_restrictions['region'].polygonal_region
                    if region validity restriction is contained in CERTIFICATES[N-1]
        } }
     }
 }
```

5.2.7.3.3 Check Identified Region

| TP ld | TP_SEC_ITSS_SND_CERT_06_01_BV |
|--------------------|---|
| Summary | Check that the identified certificate validity region contains values that correspond to numeric country codes as defined in ISO 3166-1 [9] |
| Reference | ETSI TS 103 097 [1], clause 4.2.26 |
| | PICS_USE_ISO31661_REGION_DICTIONARY, PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION |
| Expected behaviour | |

```
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 CAM
  } then {
   the IUT sends a SecuredMessage
     containing header_fields['signer_info'].signer {
       containing type
         indicating 'certificate'
       containing certificate {
         containing validity_restrictions['region']{
           containing region_type
             indicating 'id'
           containing id_region {
             containing region_dictionary
               indicating 'iso_3166_1' (0)
             containing region_identifier
               indicating valid value according to 'iso_3166_1'
    } }
             containing local_region
 }
```

```
with {
 the IUT being in the 'authorized' state
 the IUT being requested to include certificate chain in the next CAM
 ensure that {
  when \{
   the IUT is requested to send a CAM
  } then {
   the IUT sends a SecuredMessage
     containing header_fields['signer_info'].signer {
       containing type
         indicating 'certificate_chain'
       containing certificates
         indicating CERTIFICATES {
            containing CERTIFICATES[0] {
             containing validity_restrictions['region'] {
                containing region_type
                 indicating 'id'
                containing id_region {
                 containing region_dictionary
                   indicating 'iso_3166_1' (0)
                  containing region_identifier
                    indicating valid value according to 'iso_3166_1' dictionary
                  containing local_region
                }
            containing CERTIFICATES[n] (1..N) {
             containing no validity restriction of type region
             or containing validity_restrictions['region'] {
                containing region_type
                  indicating 'id'
                containing id_region
                 containing region_dictionary
                   indicating 'iso_3166_1' (0)
                  containing region_identifier
                    indicating CERTIFICATES[n-1]
                     .validity_restrictions['region'].id_region.region_identifier
                 containing local_region
                    indicating CERTIFICATES[n-1]
                      .validity_restrictions['region'].id_region.local_region
                    or indicating any value if CERTIFICATES[n-1]
                      .validity_restrictions['region'].id_region.local_region == 0
        } }
     }
 }
```

```
TP Id
                 TP_SEC_ITSS_SND_CERT_06_03_BV
                 Check that the identified certificate validity region contains values that correspond to numeric
Summary
                 country codes as defined by United Nations Statistics Division [10]
Reference
                 ETSI TS 103 097 [1], clause 4.2.26
                 PICS_USE_UN_STATS_REGION_DICTIONARY, PICS_CERTIFICATE_SELECTION,
PICS Selection
                 PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION
                                          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 CAM
  } then {
    the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
        containing type
         indicating 'certificate'
        containing certificate {
          containing validity_restrictions['region']{
            containing region_type
              indicating 'id'
            containing id_region {
              containing region_dictionary
                indicating 'un_stats' (1)
              containing region_identifier
                indicating valid value according to UN-Stats dictionary
              containing local_region
         }
       }
```

}

}

```
TP Id TP_SEC_ITSS_SND_CERT_06_04_BV

Check that the identified certificate validity region contains values that correspond to numeric country codes as defined by United Nations Statistics Division [10]
Check that the identified certificate validity region contains values defining the region which is inside the validity region of the issuing certificate

Reference ETSI TS 103 097 [1], clause 4.2.26

PICS Selection PICS_USE_UN_STATS_REGION_DICTIONARY, PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION

Expected behaviour
```

```
with {
 the IUT being in the 'authorized' state
 the IUT being requested to include certificate chain in the next CAM
 ensure that
  when {
   the IUT is requested to send a CAM
  } then {
   the IUT sends a SecuredMessage
     containing header_fields['signer_info'].signer {
       containing type
         indicating 'certificate_chain'
       containing certificates
          indicating CERTIFICATES {
            containing CERTIFICATES[0] {
              containing validity_restrictions['region'] {
                containing region_type
                  indicating 'id'
                containing id_region {
                  containing region_dictionary
                    indicating 'un_stats' (1)
                  containing region_identifier
                    indicating valid value according to UnStats document
                  containing local_region
                }
              }
            containing CERTIFICATES[n] (1..N) {
              containing no validity restriction of type region
              or containing validity_restrictions['region'] {
                containing region_type
                  indicating 'id'
                containing id_region
                  containing region_dictionary
                    indicating 'un_stats' (1)
                  containing region_identifier
                    indicating CERTIFICATES[n-1]
                        .validity_restrictions['region'].id_region
                          .region_identifier
                    or indicating any valid value according to
                        UnStats document correspondent to the subregion of
                        CERTIFICATES[n-1].validity_restrictions['region']
                          . \verb|id_region.region_identifier|\\
                  containing local_region
                    indicating CERTIFICATES[n-1]
                        .validity_restrictions['region'].id_region.local_region
                    or indicating any value if CERTIFICATES[n-1]
        } }
                        .validity_restrictions['region'].id_region.local_region == 0
     }
 }
```

5.2.7.4 Check ECC point type of the certificate signature

```
TP Id
                 TP_SEC_ITSS_SND_CERT_07_01_BV
                 Check that the certificate signature contains ECC point of type set to either compressed_lsb_y_0,
Summary
                 compressed_lsb_y_1 or x_coordinate_only
                 ETSI TS 103 097 [1], clause 4.2.9
Reference
                 PICS_GN_SECURITY
PICS Selection
                                           Expected behaviour
  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 CAM
  } then {
    the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
        containing type
          indicating 'certificate'
        containing certificate {
          containing signature.ecdsa_signature
            containing R.type
              indicating compressed_lsb_y_0
              or indicating compressed_lsb_y_1
              or indicating x_coordinate_only
      }
  }
```

5.2.7.5 Check ECC point type of the certificate verification key

```
TP Id
                 TP_SEC_ITSS_SND_CERT_08_01_BV
                 Check that the certificate verification key contains ECC point of type set to either
Summary
                 compressed_lsb_y_0, compressed_lsb_y_1 or uncompressed
Reference
                 ETSI TS 103 097 [1], clause 4.2.4
                 PICS GN SECURITY
PICS Selection
                                           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 CAM
  } then {
    the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
        containing type
          indicating 'certificate
        containing certificate {
          containing subject_attributes['verification_key']
          containing key.public_key.type
            indicating compressed_lsb_y_0
            or indicating compressed_lsb_y_1
            or indicating uncompressed
      }
  }
```

5.2.7.6 Check the certificate signature

```
TP Id
                         TP_SEC_ITSS_SND_CERT_09_01_BV
Summary
                         Check the certificate signature
Reference
                         ETSI TS 103 097 [1], clauses 6.1 and 7.4
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 {\tt CAM}
  } then {
    the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
        containing type
          indicating 'certificate'
        containing certificate {
          containing signer_info {
            containing type
              indicating 'certificate_digest_with_sha256'
            containing digest
              referenced to the certificate CERT
          containing signature
            verifiable using CERT.subject_attributes['verification_key'].key
      }
  }
```

| TP Id | TP_SEC_ITSS_SND_CERT_09_02_BV |
|--------------------|---|
| Summary | Check the signatures of the certificates in the chain |
| Reference | ETSI TS 103 097 [1], clauses 6.1 and 7.4 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with {
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate chain in the next CAM
 ensure that {
   when {
   the IUT is requested to send a CAM
  } then {
    the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
        containing type
          indicating 'certificate_chain'
        containing certificates
          indicating CERTIFICATES {
            containing CERTIFICATES[N] {
              containing signer_info {
                containing type
                  indicating 'certificate_digest_with_sha256'
                containing digest
                  referenced to the certificate CERTIFICATES[N-1]
              containing signature
                verifiable using CERTIFICATES[N-1]
                  .subject_attributes['verification_key'].key
            }
       }
      }
  }
```

5.2.7.7 AA certificate profile

5.2.7.7.1 Check the subject type

| TP ld | TP_SEC_ITSS_SND_CERT_AA_01_01_BV |
|---|--|
| Summary | Check that the subject_type of the AA certificate is set to authorization_authority |
| Reference | ETSI TS 103 097 [1], clause 7.4.3 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| the IUT being: } ensure that { when { the IUT is red; } then { the IUT send; containing containing indica; containing containing containing | in the 'authorized' state requested to include certificate chain in the next CAM equested to send a CAM s a SecuredMessage header_fields['signer_info'].signer { ng type ting certificate_chain ng certificates[last-1] { ning subject_info.subject_type cating 'authorization_authority' (2) |

5.2.7.7.2 Check AA certificate subject name

| TP Id | TP_SEC_ITSS_SND_CERT_AA_02_01_BV |
|--|--|
| Summary | The subject_name variable-length vector shall have a maximum length of 32 bytes |
| Reference | ETSI TS 103 097 [1], clause 6.2 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| the IUT being: } ensure that { when { the IUT is r } then { the IUT send containing containining containinindica containinindica containininindica | in the 'authorized' state requested to include certificate chain in the next CAM equested to send a CAM s a SecuredMessage header_fields['signer_info'].signer { ng type ting certificate_chain ng certificates[last-1] { ning subject_info.subject_name cating length <= 32 bytes |

5.2.7.7.3 Check that signer info is a digest

```
TP Id
                     TP_SEC_ITSS_SND_CERT_AA_04_01_BV
                     Check that signer info of the AA certificate is a digest
Summary
Reference
                     ETSI TS 103 097 [1], clause 7.4.3
PICS Selection
                     PICS_GN_SECURITY
                                             Expected behaviour
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate chain in the next \mathtt{CAM}
  ensure that {
   when {
    the IUT is requested to send a CAM
  } then {
    the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
        containing type
          indicating certificate_chain
        containing certificates[last-1] {
           containing signer_info {
            containing type
indicating 'certificate_digest_with_sha256'
containing digest
      }
  }
```

5.2.7.7.4 Check subject attributes presence and order

| TP ld | TP_SEC_ITSS_SND_CERT_AA_05_01_BV |
|---|--|
| Summary | Check that all necessary subject attributes are present and arranged in ascending order |
| Reference | ETSI TS 103 097 [1], clauses 6.1, 7.4 and 7.4.3 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| the IUT being } ensure that { when { the IUT is r } then { the IUT send containing containing containi indica contain contai indi | <pre>in the 'authorized' state requested to include certificate chain in the next CAM equested to send a CAM s a SecuredMessage header_fields['signer_info'].signer { ng type ting certificate_chain ng certificates[last-1] { ning subject_attributes [0N] { cating subject_attributes[n].type < subject_attributes[n].type aining subject_attributes['verification_key'] aining subject_attributes['assurance_level'] aining subject_attributes['its_aid_list']</pre> |

5.2.7.7.5 Check the time_start_and_end presence

```
TP Id
                 TP_SEC_ITSS_SND_CERT_AA_06_01_BV
                 Check that time_start_and_end is included in the AA certificate validation restrictions
Summary
                 Check that end_validity is greater than start_validity
Reference
                 ETSI TS 103 097 [1], clauses 6.7, 7.4 and 7.4.3
PICS Selection
                 PICS_GN_SECURITY
                                           Expected behaviour
with {
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate chain in the next CAM
 ensure that {
   when {
    the IUT is requested to send a CAM
  } then {
    the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
        containing type
          indicating certificate_chain
        containing certificates[last-1] {
          containing validity_restrictions [0..N] {
            not containing validity_restrictions['time_end']
            and not containing
                  validity_restrictions['time_start_and_duration']
            and containing validity_restrictions['time_start_and_end']
              containing start_validity
                indicating START_AA_VALIDITY
              containing end_validity
                indicating END_AA_VALIDITY >=START_AA_VALIDITY
        }
      }
```

5.2.7.7.6 Check verification key validity

Void.

}

5.2.7.7.7 Check ITS-AID

| TP ld | TP_SEC_ITSS_SND_CERT_AA_08_01_BV |
|--|--|
| Summary | Check that all AIDs containing in the in the its_aid_list in AA certificate are unique |
| Summary | Check that AID list contains not more than 31 items |
| Reference | ETSI TS 103 097 [1], clauses 6.9 and 7.4.3 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| with { | |
| | in the 'authorized' state |
| 9 | requested to include certificate chain in the next CAM |
| } ensure that { | |
| when { | |
| | equested to send a CAM |
| } then { | |
| | s a SecuredMessage |
| _ | header_fields['signer_info'].signer { |
| containi | 5 11 |
| | ting certificate_chain ng certificates[last-1] { |
| | ning subject_attributes['its_aid_list'] |
| | |
| <pre>containing its_aid_list[0N] containing unique items</pre> | |
| 1 | meaniting anityde teeme |
| } | |
| } | |
| } | |
| } ' | |
| יי | |

5.2.7.7.8 Check that AA cert is signed by Root cert

Void.

TP Id

5.2.7.7.9 Check validity restriction presence and order

TP_SEC_ITSS_SND_CERT_AT_01_01_BV

| TP Id | TP_SEC_ITSS_SND_CERT_AA_10_01_BV |
|--|---|
| Summary | Check that all mandatory validity restrictions are present and arranged in ascending order |
| Reference | ETSI TS 103 097 [1], clause 6.1 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| the IUT being: } ensure that { when { the IUT is reflection } then { the IUT sends containing containing indicated containing containing containing containing containing containing | in the 'authorized' state requested to include certificate chain in the next CAM equested to send a CAM s a SecuredMessage header_fields['signer_info'].signer { ng type ting certificate_chain ng certificates[last-1] { ning validity_restrictions cating validity_restrictions[n].type < validity_restrictions[n+1].type |

5.2.7.8 AT certificate profile

5.2.7.8.1 Check subject type

| Summary | Check that the subject_type of the AT certificate is set to 'authorization_ticket' (1) |
|--|---|
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| the IUT being of the sure that { when { the IUT is red the IUT sends containing containing indicate containing cont | in the 'authorized' state requested to include certificate in the next CAM equested to send a CAM s a SecuredMessage header_fields['signer_info'].signer { ng type ting 'certificate' ng certificate { ning subject_info.subject_type cating 'authorization_ticket' (1) |

5.2.7.8.2 Check that signer info is a digest

```
TP Id
                  TP_SEC_ITSS_SND_CERT_AT_02_01_BV
                  Check that signer info of the AA certificate is a digest
Summary
Reference
                  ETSI TS 103 097 [1], clauses 6.1, 7.4 and 7.4.1
PICS Selection
                  PICS_GN_SECURITY
                                           Expected behaviour
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate in the next {\tt CAM}
} ensure that {
   when {
    the IUT is requested to send a CAM
  } then {
    the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
        containing type
          indicating 'certificate'
        containing certificate
          containing signer_info {
            containing type
              indicating 'certificate_digest_with_sha256'
            containing digest
      }
  }
```

5.2.7.8.3 Check subject name

```
TP Id
                 TP_SEC_ITSS_SND_CERT_AT_03_01_BV
Summary
                 Check that the subject_name variable-length vector is empty for AT certificates
                 ETSI TS 103 097 [1], clause 7.4.1
Reference
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 CAM
  } then {
    the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
        containing type
          indicating 'certificate'
        containing certificates {
          containing subject_info.subject_name
            indicating length = 0
      }
  }
```

5.2.7.8.4 Check the presence and the order of subject attributes

```
TP Id
                 TP_SEC_ITSS_SND_CERT_AT_04_01_BV
Summary
                 Check that subject attributes are present and arranged in ascending order
Reference
                 ETSI TS 103 097 [1], clauses 7.4 and 7.4.1
PICS Selection
                 PICS_GN_SECURITY
                                          Expected behaviour
  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 CAM
  } then {
   the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
        containing type
         indicating 'certificate'
        containing certificate {
          containing subject_attributes [0..N] {
            indicating subject_attributes[n].type
                  < subject_attributes[n+1].type
            containing subject_attributes['verification_key']
            containing subject_attributes['assurance_level']
            containing subject_attributes['its_aid_ssp_list']
     }
 }
```

5.2.7.8.5 Check presence of time_start_and_end validity restriction

```
TP Id TP_SEC_ITSS_SND_CERT_AT_05_01_BV

Summary Check that time_start_and_end is included in the AT certificate validation restrictions
Check that time_start_and_end is inside the AA certificate time restrictions

Reference ETSI TS 103 097 [1], clause 7.4.1

PICS Selection PICS_GN_SECURITY

Expected behaviour

with {
    the IUT being in the 'authorized' state
```

```
the IUT being requested to include certificate chain in the next CAM
ensure that {
 when {
  the IUT is requested to send a CAM
} then {
  the IUT sends a SecuredMessage
    containing header_fields['signer_info'].signer {
      containing type
        indicating certificate_chain
      containing certificates[last-1] {
        containing subject_info.subject_type
          indicating 'authorization_authority' (2)
        containing validity_restrictions['time_start_and_end']
          containing start_validity
            indicating START_AA_VALIDITY
          containing end_validity
            indicating END_AA_VALIDITY
        }
      containing certificates[last] {
        containing subject_info.subject_type
          indicating 'authorization_ticket' (1)
         containing validity_restrictions [0..N] {
         not containing validity_restrictions['time_end']
         and not containing validity_restrictions['time_start_and_duration']
         and containing validity_restrictions['time_start_and_end']
          containing start_validity
            indicating START_AT_VALIDITY
              (START_AT_VALIDITY >= START_AA_VALIDITY )
          containing end_validity
            indicating END_AT_VALIDITY
              (END_AT_VALIDITY >= START_AT_VALIDITY <= END_AA_VALIDITY)
      }
    }
}
```

5.2.7.8.6 Check verification key validity

Void.

5.2.7.8.7 Check ITS-AID-SSP

| TP ld | TP_SEC_ITSS_SND_CERT_AT_07_01_BV |
|----------------|--|
| Summary | Check that all AIDs containing in the its_aid_ssp_list in AT certificate are unique Check that all AIDs containing in the its_aid_ssp_list in AT certificate are also containing in the its_aid_list in the correspondent AA certificate Check that the length of SSP of each AID is 31 octets maximum |
| Reference | ETSI TS 103 097 [1], clauses 6.9 and 7.4.1 |
| PICS Selection | PICS_GN_SECURITY |

```
Expected behaviour
with {
 the IUT being in the 'authorized' state
 the IUT being requested to include certificate chain in the next CAM
 ensure that {
  when {
   the IUT is requested to send a CAM
 } then {
   the \overline{\text{IUT}} sends a \overline{\text{SecuredMessage}}
      containing header_fields['signer_info'].signer {
       containing type
         indicating certificate_chain
       containing certificates[last-1] {
         containing subject_info.subject_type
            indicating 'authorization_authority' (2)
          containing subject_attributes['its_aid_list']
            containing its_aid_list[0..N]
              indicating ITS_AID_LIST_AA
          }
       containing certificates[last] {
          containing subject_info.subject_type
            indicating 'authorization_ticket' (1)
          containing subject_attributes['its_aid_ssp_list']
            containing its_aid_ssp_list[0..N] {
              containing its_aid_ssp_list[n]{
                containing its_aid
                  indicating unique value containing in the ITS_AID_LIST_AA
                containing service_specific_permissions
                  indicating length <= 31 octet
    } }
```

5.2.7.8.8 Check that AT certificate is signed by AA cert

| TP ld | TP_SEC_ITSS_SND_CERT_AT_08_01_BV |
|----------------|--|
| Summary | Check that AT certificate is signed by AA cert |
| Reference | ETSI TS 103 097 [1], clause 6.3 |
| PICS Selection | PICS_GN_SECURITY |

```
Expected behaviour
 the IUT being in the 'authorized' state
 the IUT being requested to include certificate chain in the next \mathtt{CAM}
} ensure that {
   the IUT is requested to send a CAM
 } then {
   the IUT sends a SecuredMessage
     containing header_fields['signer_info'].signer {
       containing type
        indicating certificate_chain
       containing certificates[last-1] (CERT_AA) {
         containing subject_info.subject_type
          indicating 'authorization_authority' (2)
         and containing subject_attributes['verification key'] (KEY)
       containing certificates[last] {
         containing subject_info.subject_type
          indicating 'authorization_ticket' (1)
         and containing signer_info{
           containing type
             indicating 'certificate_digest_with_ecdsap256'
           containing digest
             referencing to CERT_AA
         and containing signature
           verifiable using KEY
     }
```

5.2.7.8.9 Check assurance level

```
TP Id
                 TP_SEC_ITSS_SND_CERT_AT_09_01_BV
                 Check that the assurance level of the subordinate certificate is equal to or less than the assurance
Summary
                 level of the issuing certificate
Reference
                 ETSI TS 103 097 [1], clause 7.4
PICS Selection
                 PICS_GN_SECURITY
                                           Expected behaviour
with {
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate chain in the next CAM
 ensure that {
   when {
    the IUT is requested to send a CAM
  } then {
    the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
        containing type
         indicating certificate_chain
        containing certificates[last-1] (CERT_AA) {
          containing subject_attributes ['assurance_level']
            containing assurance_level
              containing bits [5-7]
                indicating assurance level AL_AA
        containing certificates[last] (CERT_AT) {
          containing subject_attributes ['assurance_level']
            containing assurance_level
              containing bits [5-7]
                indicating assurance level AL_AT (AL_AT <= AL_AA)
      }
  }
```

5.2.7.8.10 Check validity restriction presence and order

| TP Id | TP_SEC_ITSS_SND_CERT_AT_10_01_BV |
|--|--|
| - | |
| Summary | Check that all necessary validity restrictions are present and arranged in ascending order |
| Reference | ETSI TS 103 097 [1], clause 6.1 |
| 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 r | equested to send a CAM |
| } then { | |
| the IUT send | s a SecuredMessage |
| containing | header_fields['signer_info'].signer { |
| containi | ng type |
| | ting 'certificate' |
| containing certificate { | |
| containing validity_restrictions | |
| indicating validity_restrictions[n].type < validity_restrictions[n+1].type | |
| } | |
| } | |
| } | |
| [} | |

5.3 Receiver Behaviour

5.3.1 Overview

All test purposes of receiving behaviour are considered optional.

5.3.2 CAM Profile

5.3.2.1 Check that IUT accepts well-formed Secured CAM

| · · | | |
|---|--|--|
| TP Id | TP_SEC_ITSS_RCV_CAM_01_01_BV | |
| Summary | Check that IUT accepts a well-formed Secured CAM containing certificate in signer_info | |
| 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 { | | |
| • | eceiving a SecuredMessage | |
| | protocol_version | |
| indicati | ng value '2' | |
| | ning header_fields[0] | |
| containin | | |
| | ting 'signer_info' aining signer { | |
| | ning type | |
| | cating 'certificate' | |
| and con | ntaining certificate (CERT_AT_A) { | |
| | aining subject_info.subject_type | |
| | dicating 'authorization_ticket' (2) | |
| and (| containing subject_attributes['verification key'] (KEY) | |
| } | | |
| and contain | ning header_fields [1] { | |
| containi | | |
| | ting 'generation_time' | |
| | ng generation_time | |
| indica | ting CURRENT_TIME | |
| and contain | ning header_fields[2] { | |
| containi | | |
| | ting 'its_aid' | |
| | ng its_aid | |
| indicating 'AID_CAM' | | |
| } | | |
| <pre>and containing payload_field { containing type</pre> | | |
| | indicating type | |
| | containing data | |
| | indicating length > 0 | |
| containing CAM payload | | |
| } and containing trailer fields { | | |
| <pre>and containing trailer_fields { containing single instance of type TrailerField {</pre> | | |
| containing type | | |
| indicating 'signature' | | |
| containing signature | | |
| verifiable using KEY | | |
| } | | |
| } then { | | |
| the IUT accepts the message | | |
| [} | | |
| } | | |

| TP ld | TP_SEC_ITSS_RCV_CAM_01_02_BV |
|----------------|--|
| Summary | Check that IUT accepts a well-formed Secured CAM containing certificate digest of the known certificate in signer_info |
| Reference | ETSI TS 103 097 [1], clause 7.1 |
| PICS Selection | PICS_GN_SECURITY |

```
Expected behaviour
with {
  the IUT being in the 'authorized' state
  the IUT already received a Secured message containing certificate (CERT_TS_AT_A)
   containing subject_info.subject_type
      indicating 'authorization_ticket' (2)
   and containing subject_attributes['verification key'] (KEY)
ensure that {
 when {
    the IUT is receiving a SecuredMessage
     containing protocol_version
       indicating value '2'
      and containing header_fields[0]
       containing type
          indicating 'signer_info'
        and containing signer {
          containing type
           indicating 'certificate_digest_with_sha256'
          and containing digest
           referencing to certificate (CERT_TS_AT_A)
      and containing header_fields [1] {
       containing type
         indicating 'generation_time'
       containing generation_time
          indicating CURRENT_TIME
      and containing header_fields[2] {
       containing type
         indicating 'its_aid'
        containing its_aid
         indicating 'AID_CAM'
      and containing payload_field {
       containing type
          indicating 'signed'
        containing data
          indicating length > 0
          containing CAM payload
      and containing trailer_fields {
       containing single instance of type TrailerField {
          containing type
            indicating 'signature'
          containing signature
            verifiable using KEY
      }
  } then {
   the IUT accepts the message
```

```
TP Id TP_SEC_ITSS_RCV_CAM_01_03_BV

Summary Check that IUT accepts a well-formed Secured CAM containing certificate chain in signer_info

Reference ETSI TS 103 097 [1], clause 7.1

PICS Selection PICS_GN_SECURITY
```

```
Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage
      containing protocol_version
       indicating value '2'
      and containing header_fields[0]
        containing type
          indicating 'signer_info'
        and containing signer {
          containing type
           indicating 'certificate_chain'
          and containing certificates
            containing certificate (CERT_TS_AA_A) at index 0 {
              containing subject_info.subject_type
                indicating 'authorization_authority'
              and containing subject_attributes['verification key'] (KEY_TS_AA)
            and containing certificate (CERT_TS_AT_A) at index 1 {
              containing subject_info.subject_type
                indicating 'authorization_ticket
              and containing signer_info {
                containing type
                  indicating 'certificate_digest_with_sha256'
                containing digest
                  referencing to the CERT_TS_AA_A
              and containing signature
               verifiable using KEY_TS_AA
              and containing subject_attributes['verification key'] (KEY_TS_AT)
            }
      and containing header_fields [1] {
        containing type
          indicating 'generation_time'
        containing generation_time
          indicating CURRENT_TIME
      and containing header_fields[2] {
        containing type
          indicating 'its_aid'
        containing its_aid
          indicating 'AID_CAM'
      and containing payload_field {
       containing type
         indicating 'signed'
        containing data
          indicating length > 0
          containing CAM payload
      and containing trailer_fields {
        containing single instance of type TrailerField {
          containing type
            indicating 'signature'
          containing signature
            verifiable using KEY_TC_AT
      }
  } then {
   the IUT accepts the message
  }
```

5.3.2.2 Check the message protocol version

| TP ld | TP_SEC_ITSS_RCV_CAM_02_01_BO |
|--|--|
| Summary | Check that IUT discards a Secured CAM containing protocol version set to a value less than 2 |
| Reference | ETSI TS 103 097 [1], clause 5.2 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| ensure that { when { the IUT is recontaining indication containing indication then { then { | eceiving a SecuredMessage (CAM) protocol_version ng 1 header_fields['its_aid'] ng 'AID_CAM' ards a SecuredMessage |

| TP Id | TP_SEC_ITSS_RCV_CAM_02_02_BO |
|---|--|
| Summary | Check that IUT discards a Secured CAM containing protocol version set to a value greater than 2 |
| Reference | ETSI TS 103 097 [1], clause 5.2 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| ensure that { when { the IUT is recontaining indicating containing indicating then { | <pre>in the 'authorized' state eceiving a SecuredMessage (CAM) protocol_version ng 3 header_fields['its_aid'] ng 'AID_CAM' ards a SecuredMessage</pre> |

5.3.2.3 Check header fields

| TP Id | TP_SEC_ITSS_RCV_CAM_04_01_BO | |
|--|--|--|
| Summary | Check that IUT discards a secured CAM if the header_fields contains more than one element of | |
| | header field type: signer_info | |
| Reference | ETSI TS 103 097 [1], clause 7.1 | |
| PICS Selection | PICS_GN_SECURITY | |
| | Expected behaviour | |
| with { | · | |
| | in the 'authorized' state | |
| } | | |
| ensure that { | | |
| when { | | |
| the IUT is r | eceiving a SecuredMessage (CAM) | |
| containing | header_fields[0].type | |
| indicati | ng 'signer_info' | |
| and contain | and containing header_fields[1].type | |
| indicati | indicating 'signer_info' | |
| and contain | and containing header_fields[2].type | |
| indicati | indicating 'generation_time' | |
| and containing header_fields[3] { | | |
| containi | containing type | |
| indica | indicating 'its_aid' | |
| containing its_aid | | |
| indicating 'AID_CAM' | | |
| } | | |
| and not containing other header fields | | |
| } then { | | |
| the IUT disc | the IUT discards a SecuredMessage | |
| } | | |

| TP ld | TP_SEC_ITSS_RCV_CAM_04_02_BO | |
|--|--|--|
| | Check that IUT discards a secured CAM if the header_fields does not contain the header field type: | |
| | signer_info | |
| 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 { | and in the second Market (GDM) | |
| | receiving a SecuredMessage (CAM) | |
| _ | containing header_fields[0].type | |
| | indicating 'generation_time' | |
| | <pre>and containing header_fields[1]{ containing type</pre> | |
| | indicating type | |
| | ng its aid | |
| | indicating 'AID CAM' | |
| } | - | |
| and not containing other header fields | | |
| } then { | | |
| the IUT disc | ards a SecuredMessage | |
| } | | |
| } | | |

```
TP Id
                 TP_SEC_ITSS_RCV_CAM_04_03_BO
Summary
                 Check that IUT is able to receive a secured CAM if the signer_info header field is not encoded first
Reference
                 ETSI TS 103 097 [1], clause 7.1
PICS Selection
                 PICS_GN_SECURITY
                                          Expected behaviour
with {
 the IUT being in the 'authorized' state
  the IUT is sending CAMs
ensure that {
 when {
    the IUT is receiving a SecuredMessage (CAM) {
     containing header_fields[0].type
       indicating 'signer_info'
      and containing header_fields[1].type
       indicating 'generation_time'
      and containing header_fields[2].type
       indicating 'signer_info'
      and containing header_fields[3] {
        containing type
          indicating 'its_aid'
        containing its_aid
          indicating 'AID_CAM'
      and not containing other header fields
  } then {
    the IUT keeps sending CAMs
```

| r | | |
|--|--|--|
| TP Id | TP_SEC_ITSS_RCV_CAM_04_04_BO | |
| Cummoru | Check that IUT discards a secured CAM if the header_fields contains more than one element of | |
| Summary | header field type: generation_time | |
| 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 { | | |
| | eceiving a SecuredMessage (CAM) | |
| _ | header_fields[0].type | |
| | indicating 'signer_info' | |
| _ | containing header_fields[1].type | |
| | <pre>indicating 'generation_time'</pre> | |
| | ning header_fields[2].type | |
| | ng 'generation_time' _ | |
| | <pre>and containing header_fields[3] {</pre> | |
| | containing type | |
| | indicating 'its_aid' | |
| | containing its_aid | |
| indicating 'AID_CAM' | | |
| } | | |
| and not containing other header fields | | |
| } then { | | |
| the IUT disc | ards a SecuredMessage | |
| } | | |
| } | | |

```
TP Id
                  TP_SEC_ITSS_RCV_CAM_04_05_BO
                  Check that IUT discards a secured CAM if the header_fields does not contain the element of header
Summary
                  field of type: generation_time
Reference
                  ETSI TS 103 097 [1], clause 7.1
                  PICS_GN_SECURITY
PICS Selection
                                             Expected behaviour
with {
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage (CAM) containing header_fields[0].type
        indicating 'signer_info'
      and containing header_fields[1] {
        containing type
          indicating 'its_aid'
        containing its_aid
          indicating 'AID_CAM'
      and not containing other header fields
  } then {
    the IUT discards a SecuredMessage
```

| TP ld | TP SEC ITSS RCV CAM 04 06 BO | |
|--|---|--|
| | | |
| Summary | Check that IUT discards a secured CAM if the header_fields contain more than one element of | |
| D (| header field of type: its_aid | |
| 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 { | (911) | |
| | receiving a SecuredMessage (CAM) | |
| - | | |
| | <pre>indicating 'signer_info' and containing header_fields[1].type</pre> | |
| | In generation time | |
| | <pre>lning generation_time lning header_fields[2] {</pre> | |
| | containing header_ffetds[2] { | |
| | ating 'its_aid' | |
| | ing its_aid | |
| indicating 'AID_CAM' | | |
| } | | |
| and contai | and containing header_fields[3] { | |
| containi | containing type | |
| | indicating 'its_aid' | |
| containing its_aid | | |
| indicating 'AID_DENM' | | |
| } | | |
| and not containing other header fields | | |
| } then { | cards a SecuredMessage | |
|) | atus a secureumessaye | |
| } | | |
| ل | | |

```
TP Id TP_SEC_ITSS_RCV_CAM_04_08_BO

Summary Check that IUT ignores the HeaderFields generation_time_standard_deviation of received Secured CAM

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 receiving a SecuredMessage (CAM)
     containing header_fields[0].type
       indicating 'signer_info'
      containing header_fields[1]{
       containing type
         indicating 'generation_time'
       containing generation_time
         indicating TIME_1 inside the validity period of the signer certificate
      containing header_fields[2] {
       containing type
         indicating 'generation_time_with_standard_deviation'
        containing generation_time_with_standard_deviation
         indicating TIME_2 outside the validity period of the signer certificate
      and containing header_fields[3] {
       containing type
         indicating 'its_aid'
        containing its_aid
         indicating 'AID_CAM'
      and not containing other header fields
  } then {
   the IUT discards a SecuredMessage
```

| TP ld | TP_SEC_ITSS_RCV_CAM_04_09_BO |
|----------------|--|
| Sillininary | Check that IUT ignores the HeaderFields generation_time_standard_deviation of received Secured CAM |
| Reference | ETSI TS 103 097 [1], clause 7.1 |
| PICS Selection | PICS_GN_SECURITY |

```
Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage (CAM)
     containing header_fields[0].type
       indicating 'signer_info'
      containing header_fields[1]{
       containing type
         indicating 'generation_time'
        {\tt containing \ generation\_time}
          indicating TIME_1 outside the validity period of the signer certificate
      containing header_fields[2] {
        containing type
          indicating 'generation_time_with_standard_deviation'
        containing generation_time_with_standard_deviation
         indicating TIME_2 inside the validity period of the signer certificate
      and containing header_fields[3] {
        containing type
         indicating 'its_aid'
        containing its_aid
          indicating 'AID_CAM'
      and not containing other header fields
  } then {
   the IUT discards a SecuredMessage
```

```
TP Id TP_SEC_ITSS_RCV_CAM_04_10_BO

Summary Check that IUT ignores the HeaderFields expiry_time of received Secured CAM

Reference ETSI TS 103 097 [1], clause 7.1

PICS Selection PICS_GN_SECURITY
```

```
PICS Selection
                                          Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
 when {
the IUT is receiving a SecuredMessage (CAM)
      containing header_fields[0].type
       indicating 'signer_info'
      containing header_fields[1]{
        containing type
          indicating 'generation_time'
        containing generation_time
          indicating TIME_1 ( TIME_1 < CURRENT_TIME - 1min )</pre>
      containing header_fields[2] {
        containing type
         indicating 'expiration'
        containing expiry_time
          indicating TIME_2 (TIME_1 < TIME_2 < CURRENT_TIME)</pre>
      and containing header_fields[3] {
        containing type
          indicating 'its_aid'
        containing its_aid
          indicating 'AID_CAM'
      and not containing other header fields
  } then {
    the IUT accepts a SecuredMessage
```

```
TP Id
                 TP_SEC_ITSS_RCV_CAM_04_11_BO
Summary
                 Check that IUT ignores the HeaderFields generation_location of received Secured CAM
Reference
                 ETSI TS 103 097 [1], clause 7.1
PICS Selection
                 PICS_GN_SECURITY
                                          Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
 when {
the IUT is receiving a SecuredMessage (CAM)
      containing header_fields[0] {
        containing type
         indicating 'signer_info'
        containing signer {
         containing type
            indicating certificate
          containing certificate
            indicating CERT_TS_AT_B
      and containing header_fields[1].type
       indicating 'generation_time'
      and containing header_fields[2] {
        containing type
          indicating 'generation_location'
        containing generation_location
          indicating position outside of the validity restriction of CERT_TS_AT_B
      and containing header_fields[3] {
        containing type
         indicating 'its_aid'
        containing its_aid
          indicating 'AID_CAM'
```

5.3.2.4 Check signer info

the $\overline{\text{IUT}}$ accepts a SecuredMessage

} then {

and not containing other header fields

| TP Id | TP_SEC_ITSS_RCV_CAM_05_01_BO |
|---|--|
| Summary | Check that IUT discards a secured CAM if the header_fields contains a signer of type 'self' |
| Reference | ETSI TS 103 097 [1], clause 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>ensure that { when { the IUT is recontaining containing containing and contain and contain and contain and contain and contain and contain and contain and contain and contain and contain and contain and contain and contain and contain and contain and contain and contain and contain and contain and contain and contain</pre> | eceiving a SecuredMessage (CAM) { header_fields['signer_info'] ng signer.type ting 'self' ning header_fields['generation_time'] ning header_fields['its_aid'] ng 'AID_CAM' ntaining other header fields ards a SecuredMessage |

```
TP Id
                    TP_SEC_ITSS_RCV_CAM_05_02_BO
                    Check that IUT discards a secured CAM if the header_fields contains a signer of type
Summary
                    certificate_digest_with_other_algorithm
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 receiving a SecuredMessage (CAM) {
    containing header_fields['signer_info']
         containing signer.type
           indicating 'certificate_digest_with_other_algorithm'
      and containing header_fields['generation_time'] and containing header_fields['its_aid']
         indicating 'AID_CAM'
       and not containing other header fields
  } then {
    the IUT discards a SecuredMessage
  }
```

| TP Id | TP SEC ITSS RCV CAM 05 03 BO |
|--|---|
| Summary | Check that IUT discards a secured CAM if the header_fields contains a signer of type certificate_chain and the chain is empty |
| Reference | ETSI TS 103 097 [1], clause 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>} ensure that { when { the IUT is recontaining containing contain indice contain indice } and contain and contain indice indice indice indice indice indice indice indice indice indiceating indiceating</pre> | eceiving a SecuredMessage (CAM) { header_fields['signer_info'] ng signer { ing type cating 'certificate_chain' ning certificates cating length = 0 ning header_fields['generation_time'] ning header_fields['its_aid'] ng 'AID_CAM' ntaining other header fields |
| the IUT discards a SecuredMessage } } | |

```
TP Id
                   TP_SEC_ITSS_RCV_CAM_05_04_BO
                   Check that IUT discards a secured CAM if the header_fields contains a signer of type
Summary
                   certificate_chain and the chain contains only one certificate
Reference
                   ETSI TS 103 097 [1], clause 7.1
                   PICS_GN_SECURITY
PICS Selection
                                               Expected behaviour
with {
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage (CAM) {
   containing header_fields['signer_info']
         containing signer {
           containing type
             indicating 'certificate_chain'
           containing certificates
             indicating length = 1
       and containing header_fields['generation_time']
      and containing header_fields['its_aid']
indicating 'AID_CAM'
       and not containing other header fields
  } then {
```

the IUT discards a SecuredMessage

5.3.2.5 Check generation time

| TP Id | TP_SEC_ITSS_RCV_CAM_06_01_BO |
|----------------|---|
| Summary | Check that IUT discards message containing generation_time before the certificate validity period |
| Reference | ETSI TS 103 097 [1], clauses 5.4 and 7.1 |
| PICS Selection | PICS_GN_SECURITY |

```
Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage {
      containing header_fields[0] {
       containing type
         indicating 'signer_info'
       and containing signer {
         containing type
           indicating 'certificate'
         and containing certificate (CERT_TS_AT_A) {
           containing validity_restrictions['time_start_and_end'] {
             containing start_validity
               indicating TIME_CERT_TS_AT_START
             and containing end_validity
               indicating TIME_CERT_TS_AT_END
            }
         }
       }
      and containing header_fields [1] {
       containing type
         indicating 'generation_time'
       containing generation_time
         indicating TIME_1 < TIME_CERT_TS_AT_START
      and containing header_fields[2] {
       containing type
         indicating 'its_aid'
       containing its_aid
         indicating 'AID_CAM'
  } then {
   the IUT discards the message
```

```
TP Id TP_SEC_ITSS_RCV_CAM_06_02_BO

Summary Check that IUT discards message containing generation_time after the certificate validity period

Reference ETSI TS 103 097 [1], clauses 5.4 and 7.1

PICS Selection PICS_GN_SECURITY

Expected behaviour

with {
    the IUT being in the 'authorized' state
}
ensure that {
    when {
```

```
the IUT is receiving a SecuredMessage {
   containing header_fields[0] {
     containing type
       indicating 'signer_info'
     and containing signer {
       containing type
          indicating 'certificate'
       and containing certificate (CERT_TS_AT_A) {
         containing validity_restrictions['time_start_and_end'] {
            containing start_validity
              indicating TIME_CERT_TS_AT_START
            and containing end_validity
              indicating TIME_CERT_TS_AT_END
          }
       }
     }
   and containing header_fields [1] {
     containing type
       indicating 'generation_time'
      containing generation_time
       indicating TIME_1 > TIME_CERT_TS_AT_END
   and containing header_fields[2] {
     containing type
       indicating 'its_aid'
      containing its_aid
       indicating 'AID_CAM'
} then {
 the IUT discards the message
```

5.3.2.6 Check its_aid

| TP ld | TP_SEC_ITSS_RCV_CAM_07_01_BO |
|----------------|---|
| Summary | Check that IUT discards secured CAM when its_aid value is not AID_CAM |
| 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 receiving a SecuredMessage (CAM)
     containing header_fields['its_aid']
       indicating AID_DENM
      and containing payload_field {
        containing type
          indicating 'signed'
        containing data
          containing CAM payload
  } then {
    the IUT discards the message
  }
```

5.3.2.7 Check payload

| TP ld | TP_SEC_ITSS_RCV_CAM_09_02_BO | |
|---|---|--|
| Summary | Check that IUT discards the Secured CAM containing empty payload of type 'signed' | |
| 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 receiving a SecuredMessage { containing header_fields['its_aid'] indicating 'AID_CAM' and containing payload_field { containing type indicating 'signed' containing data indicating length 0 } } then { the IUT discards the message }</pre> | | |

| TP Id | TP_SEC_ITSS_RCV_CAM_09_03_BO | | |
|---|--|--|--|
| Summary | Check that IUT discards the Secured CAM containing non-empty payload of type 'unsecured' | | |
| 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 { | | | |
| | receiving a SecuredMessage { | | |
| _ | g header_fields['its_aid'] | | |
| | ng 'AID_CAM' | | |
| | and containing payload_field { | | |
| containi | containing type | | |
| indica | indicating 'unsecured' | | |
| } | | | |
| } | | | |
| } then { | | | |
| the IUT disc | the IUT discards the message | | |
| } | | | |
| } | | | |
|) | | | |

```
TP Id
                  TP_SEC_ITSS_RCV_CAM_09_04_BO
Summary
                  Check that IUT discards the Secured CAM containing non-empty payload of type 'encrypted'
Reference
                  ETSI TS 103 097 [1], clause 7.1
PICS Selection
                 PICS_GN_SECURITY
                                            Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
 when {
the IUT is receiving a SecuredMessage {
      containing header_fields['its_aid']
        indicating 'AID_CAM'
      and containing payload_field {
        containing type
indicating 'encrypted'
  } then {
    the IUT discards the message
```

| TP ld | TP_SEC_ITSS_RCV_CAM_09_05_BO | | |
|------------------------------|--|--|--|
| Summary | Check that IUT discards the Secured CAM containing non-empty payload of type 'signed_external' | | |
| 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 r | the IUT is receiving a SecuredMessage $\{$ | | |
| containing | containing header_fields['its_aid'] | | |
| | ng 'AID_CAM' | | |
| and contain | ning payload_field { | | |
| containi | ng type | | |
| indicating 'signed_external' | | | |
| } | | | |
| } | | | |
| } then { | | | |
| the IUT discards the message | | | |
| } | | | |
| } | | | |

```
TP Id
                    TP_SEC_ITSS_RCV_CAM_09_06_BO
                    Check that IUT discards the Secured CAM containing non-empty payload of type
Summary
                    'signed_and_encrypted'
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 receiving a SecuredMessage {
   containing header_fields['its_aid']
   indicating 'AID_CAM'
      and containing payload_field {
        containing type
           indicating 'signed_and_encrypted'
      }
  } then {
    the IUT discards the message
```

5.3.2.8 Check presence of trailer field

| | - | |
|--|---|--|
| TP ld | TP_SEC_ITSS_RCV_CAM_10_01_BO | |
| Summary | Check that IUT discards the Secured CAM if the message does not contain the trailer field of type | |
| | 'signature' | |
| 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 receiving a SecuredMessage $\{$ | | |
| - | containing header_fields['its_aid'] | |
| | ng 'AID_CAM' | |
| | and containing trailer_fields | |
| | not containing any instance of type TrailerField { | |
| | containing type | |
| indicating 'signature' | | |
| } | | |
| } | | |
| } then { | | |
| the IUT disca | ards the message | |
| } | | |
| } | | |

```
TP Id
                   TP_SEC_ITSS_RCV_CAM_10_02_BO
                   Check that IUT discards the Secured CAM containing more than one instance of TrailerField of type
Summary
                   'signature'
Reference
                   ETSI TS 103 097 [1], clause 7.1
                  PICS_GN_SECURITY
PICS Selection
                                              Expected behaviour
with {
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
    containing header_fields['its_aid']
        indicating 'AID_CAM'
      and containing trailer_fields[0]
        containing type
           indicating 'signature'
      and containing trailer_fields[1]
        containing type
           indicating 'signature'
  } then {
    the IUT discards the message
```

5.3.2.9 Check signature

TP_SEC_ITSS_RCV_CAM_11_01_BO

TP Id

} then {

the IUT discards the message

| Summary | verification key from the certificate contained in the message's signer info | |
|-----------------------------|--|--|
| Reference | ETSI TS 103 097 [1], clause 7.1 | |
| PICS Selection | PICS_GN_SECURITY | |
| | Expected behaviour | |
| with { | | |
| the IUT being | in the 'authorized' state | |
| <pre>} ensure that {</pre> | | |
| when { | | |
| the IUT is | receiving a SecuredMessage { | |
| | g header_fields ['signer_info'] { | |
| | ing signer { | |
| | ining type | |
| | icating 'certificate' | |
| | ining certificate | |
| | taining subject_info.subject_type | |
| | ndicating 'authorization_ticket' (2) | |
| | containing subject_attributes['verification key'] ontaining key (KEY) | |
| ì | ontaining key (KEY) | |
| } | | |
| containin | g header_fields['its_aid'] | |
| · · | ing 'AID_CAM' | |
| containing trailer_fields { | | |
| · · | ing single instance of type TrailerField { | |
| conta | ining type | |
| ind | icating 'signature' | |
| conta | ining signature | |
| NOT | verifiable using KEY | |
| } | | |
| } | | |

Check that the IUT discards Secured message containing signature that is not verified using the

```
TP Id TP_SEC_ITSS_RCV_CAM_11_02_BO

Summary Check that the IUT discards Secured message containing signature that is not verified using the verification key from the certificate, referenced by the digest contained in the message's signer info

Reference ETSI TS 103 097 [1], clause 7.1

PICS Selection PICS_GN_SECURITY

Expected behaviour
```

```
the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage {
     containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate_digest_with_sha256'
          containing digest
            referencing to the certificate
              {\tt containing \; subject\_info.subject\_type}
                indicating 'authorization_ticket' (2)
              and containing subject_attributes['verification key']
                containing key (KEY)
        }
      containing header_fields['its_aid']
        indicating 'AID_CAM'
      containing trailer_fields {
        containing single instance of type TrailerField {
         containing type
           indicating 'signature'
          containing signature
            NOT verifiable using KEY
     }
  } then {
    the IUT discards the message
```

5.3.2.10 Check signing certificate type

| TP Id | TP_SEC_ITSS_RCV_CAM_12_01_BO |
|--|---|
| Summary | Check that IUT discards a Secured CAM if the signer certificate of the message contains the subject type "enrolment_credential" |
| Reference | ETSI TS 103 097 [1], clauses 7.1 and 7.4 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>with { the IUT being ; } ensure that {</pre> | in the 'authorized' state |
| <pre>ensure that { when { the IUT is receiving a SecuredMessage containing header_fields ['signer_info'] { containing signer.type indicating 'certificate' containing signer.certificate (CERT_TS_EC_A) containing subject_info.subject_type indicating 'enrolment_credentials' } containing header_fields['its_aid'] indicating 'AID_CAM' } then { the IUT discards the message</pre> | |
| } | |

```
TP Id
                  TP_SEC_ITSS_RCV_CAM_12_02_BO
                  Check that IUT discards a Secured CAM if the signer certificate of the message contains the subject
Summary
                  type "authorization_authority"
                  ETSI TS 103 097 [1], clauses 7.1 and 7.4
Reference
                  PICS_GN_SECURITY
PICS Selection
                                             Expected behaviour
with {
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage containing header_fields ['signer_info'] {
        containing signer.type
          indicating 'certificate'
        containing signer.certificate (CERT_TS_AA_A)
          containing subject_info.subject_type
             indicating 'authorization_authority'
      containing header_fields['its_aid']
        indicating 'AID_CAM'
  } then {
    the IUT discards the message
```

5.3.3 DENM Profile

5.3.3.1 Check that IUT accepts well-formed Secured DENM

| TP ld | TP_SEC_ITSS_RCV_DENM_01_01_BV | |
|--|--|--|
| Cummoni | Check that IUT accepts a well-formed Secured DENM signed with the certificate without region | |
| Summary | validity restriction | |
| Reference | ETSI TS 103 097 [1], clause 7.2 | |
| PICS Selection | PICS_GN_SECURITY | |
| | Expected behaviour | |
| with { | Exposited Bolletifodi | |
| ` | in the 'authorized' state | |
| ensure that { when { | | |
| the IUT is r | eceiving a SecuredMessage | |
| containing | header_fields[0] | |
| containi | | |
| | ting 'signer_info' | |
| | aining signer { | |
| | ning type | |
| | cating 'certificate' | |
| | ntaining certificate (CERT_TS_AT_A) { aining subject_info.subject_type | |
| | dicating 'authorization_ticket' (2) | |
| | containing subject_attributes['verification key'] | |
| | ntaining key (KEY) | |
| | not containing validity_restrictions['region'] | |
| } | 3 | |
| } | | |
| and contain | ning header_fields [1] | |
| containi | ng type | |
| indica | ting 'generation_time' | |
| | ng generation_time | |
| | indicating CURRENT_TIME | |
| | and containing header_fields [2] | |
| containi | | |
| | ting 'generation_location' | |
| | containing generation_location | |
| <pre>and containing header_fields[3] containing type</pre> | | |
| indicating 'its_aid' | | |
| containing its_aid | | |
| indicating 'AID_DENM' | | |
| and containing payload_field { | | |
| containing type | | |
| indicating 'signed' | | |
| | containing data | |
| indicating length > 0 | | |
| contain | ning DENM payload | |
| } and contain | ning trailer_fields { | |
| | ng single instance of type TrailerField { | |
| containing type | | |
| indicating 'signature' | | |
| containing signature | | |
| | verifiable using KEY | |
| } | | |
| } | | |
| } then { | | |
| the IUT acce | pts the message | |

```
TP Id TP_SEC_ITSS_RCV_DENM_01_02_BV

Summary Check that IUT accepts a well-formed Secured DENM signed with the certificate with a circular region validity restriction

Reference ETSI TS 103 097 [1], clause 7.2

PICS Selection PICS_GN_SECURITY
```

```
Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage
      and containing header_fields[0]
       containing type
          indicating 'signer_info'
        and containing signer {
          containing type
            indicating 'certificate'
          and containing certificate (CERT_AT_B) {
            containing subject_info.subject_type
              indicating 'authorization_ticket' (2)
            and containing subject_attributes['verification key'] (KEY)
            and containing validity_restrictions['region'] {
              containing region{
                containing region_type
                  indicating 'circle'
                and containing circular_region
                  indicating REGION
          }
      and containing header_fields [1]
        containing type
         indicating 'generation_time'
        containing generation_time
          indicating CURRENT_TIME
      and containing header_fields [2]
       containing type
         indicating 'generation_location'
        containing generation_location
          indicating position inside the REGION
      and containing header_fields[3]
       containing type
          indicating 'its_aid'
        containing its_aid
          indicating 'AID_DENM'
      and not containing any other header_fields
      and containing payload_fields {
        containing type
          indicating 'signed'
        containing data
          indicating length > 0
          containing DENM payload
      and containing trailer_fields
       containing single instance of type TrailerField {
          containing type
            indicating 'signature'
          containing signature
            verifiable using KEY
      }
  } then {
   the IUT accepts the message
```

```
TP Id TP_SEC_ITSS_RCV_DENM_01_03_BV

Summary Check that IUT accepts a well-formed Secured DENM signed with the certificate with a rectangular region validity restriction

Reference ETSI TS 103 097 [1], clause 7.2

PICS Selection PICS_GN_SECURITY
```

```
Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage
     containing protocol_version
       indicating value '2'
      and containing header_fields[0]
        containing type
          indicating 'signer_info'
        and containing signer {
          containing type
            indicating 'certificate'
          and containing certificate (CERT_AT_C) {
            containing subject_info.subject_type
              indicating 'authorization_ticket' (2)
            and containing subject_attributes['verification key'] (KEY)
            and containing validity_restrictions['region'] {
              containing region{
                containing region_type
                  indicating 'rectangle'
                and containing rectangular_regions
                  indicating REGIONS
          }
      and containing header_fields [1]
       containing type
          indicating 'generation_time'
        containing generation_time
          indicating CURRENT_TIME
      and containing header_fields [2]
        containing type
          indicating 'generation_location'
        containing generation_location
          indicating position inside the REGION
      and containing header_fields[3]
        containing type
          indicating 'its_aid'
        containing its_aid
          indicating 'AID_DENM'
      and not containing any other header_fields
      and containing payload_field {
       containing type
          indicating 'signed'
        containing data
          indicating length > 0
          containing DENM payload
      and containing trailer_fields
        containing single instance of type TrailerField {
          containing type
            indicating 'signature'
          containing signature
            verifiable using KEY
  } then {
   the IUT accepts the message
```

```
TP Id TP_SEC_ITSS_RCV_DENM_01_04_BV

Summary Check that IUT accepts a well-formed Secured DENM signed with the certificate with a polygonal region validity restriction

Reference ETSI TS 103 097 [1], clause 7.2

PICS Selection PICS_GN_SECURITY
```

```
Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage
     containing protocol_version
       indicating value '2'
      and containing header_fields[0]
        containing type
          indicating 'signer_info'
        and containing signer {
          containing type
            indicating 'certificate'
          and containing certificate (CERT_AT_D) {
            containing subject_info.subject_type
              indicating 'authorization_ticket' (2)
            and containing subject_attributes['verification key'] (KEY)
            and containing validity_restrictions['region'] {
              containing region{
                containing region_type
                  indicating 'polygon'
                and containing polygonal_region
                  indicating REGION
          }
      and containing header_fields [1]
       containing type
          indicating 'generation_time'
        containing generation_time
          indicating CURRENT_TIME
      and containing header_fields [2]
        containing type
          indicating 'generation_location'
        containing generation_location
          indicating position inside the REGION
      and containing header_fields[3]
        containing type
          indicating 'its_aid'
        containing its_aid
          indicating 'AID_DENM'
      and not containing any other header_fields
      and containing payload_field {
       containing type
          indicating 'signed'
        containing data
          indicating length > 0
          containing DENM payload
      and containing trailer_fields
        containing single instance of type TrailerField {
          containing type
           indicating 'signature'
          containing signature
            verifiable using KEY
  } then {
   the IUT accepts the message
```

```
TP Id TP_SEC_ITSS_RCV_DENM_01_05_BV

Summary Check that IUT accepts a well-formed Secured DENM signed with the certificate with a identified region validity restriction

Reference ETSI TS 103 097 [1], clause 7.2

PICS Selection PICS_GN_SECURITY
```

```
Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage
     containing protocol_version
       indicating value '2'
      and containing header_fields[0]
        containing type
          indicating 'signer_info'
        and containing signer {
          containing type
            indicating 'certificate'
          and containing certificate (CERT_AT_E) {
            containing subject_info.subject_type
              indicating 'authorization_ticket' (2)
            and containing subject_attributes['verification key'] (KEY)
            and containing validity_restrictions['region'] {
              containing region{
                containing region_type
                  indicating 'id_region'
                and containing identified_region
                  indicating REGION
          }
      and containing header_fields [1]
       containing type
          indicating 'generation_time'
        containing generation_time
          indicating CURRENT_TIME
      and containing header_fields [2]
        containing type
          indicating 'generation_location'
        containing generation_location
          indicating position inside the REGION
      and containing header_fields[3]
        containing type
          indicating 'its_aid'
        containing its_aid
          indicating 'AID_DENM'
      and not containing any other header_fields
      and containing payload_field {
       containing type
          indicating 'signed'
        containing data
          indicating length > 0
          containing DENM payload
      and containing trailer_fields
        containing single instance of type TrailerField {
          containing type
           indicating 'signature'
          containing signature
            verifiable using KEY
  } then {
   the IUT accepts the message
```

5.3.3.2 Check the message protocol version

| TP ld | TP_SEC_ITSS_RCV_DENM_02_01_BO |
|---|--|
| Summary | Check that IUT discards a Secured DENM containing protocol version set to a value less than 2 |
| Reference | ETSI TS 103 097 [1], clause 5.2 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>} ensure that { when { the IUT is recontaining indicati: containing indicati: then { }</pre> | eceiving a SecuredMessage (DENM) protocol_version ng 1 header_fields['its_aid'] ng 'AID_DENM' ards a SecuredMessage |

| TP ld | TP_SEC_ITSS_RCV_DENM_02_02_BO |
|--|--|
| Summary | Check that IUT discards a Secured DENM containing protocol version set to a value greater than 2 |
| Reference | ETSI TS 103 097 [1], clause 5.2 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| ensure that { when { the IUT is recontaining indicating containing indicating then { | eceiving a SecuredMessage (DENM) protocol_version ng 3 header_fields['its_aid'] ng 'AID_DENM' ards a SecuredMessage |

5.3.3.3 Check header fields

```
TP Id
                 TP_SEC_ITSS_RCV_DENM_04_01_BO
                 Check that IUT discards a secured DENM if the header_fields contains more than one element of
Summary
                 header field type: signer_info
Reference
                 ETSI TS 103 097 [1], clause 7.2
PICS Selection
                 PICS_GN_SECURITY
                                          Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
    the IUT is receiving a SecuredMessage (DENM)
      containing header_fields[0].type
        indicating 'signer_info'
      and containing header_fields[1].type
        indicating 'signer_info'
      and containing header_fields[2].type
        indicating 'generation_time'
      and containing header_fields[3].type
       indicating 'generation_location'
      and containing header_fields[4] {
        containing type
          indicating 'its_aid'
        containing 'its_aid'
          indicating 'AID_DENM'
      and not containing other header fields
  } then {
    the IUT discards a SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_DENM_04_02_BO | |
|----------------|--|--|
| Cummoni | Check that IUT discards a secured DENM if the header_fields does not contain the header field | |
| Summary | type: signer_info | |
| Reference | ETSI TS 103 097 [1], clause 7.2 | |
| PICS Selection | PICS_GN_SECURITY | |
| | Expected behaviour | |
| with { | | |
| the IUT being | in the 'authorized' state | |
| } | | |
| ensure that { | | |
| when { | Control of the contro | |
| | eceiving a SecuredMessage (DENM) | |
| | containing header_fields[0].type | |
| | indicating 'generation_time' | |
| | <pre>and containing header_fields[1].type indicating 'generation location'</pre> | |
| | ning header_fields[2]{ | |
| containi | | |
| | ting 'its aid' | |
| | | |
| | containing its_aid indicating 'AID DENM' | |
| } | CING ALD_DIAM | |
| and not co | ntaining other header fields | |
| then { | | |
| , | the IUT discards a SecuredMessage | |
| } | | |
| } | | |
| L ^z | | |

```
TP Id
                 TP_SEC_ITSS_RCV_DENM_04_04_BO
                 Check that IUT discards a secured DENM if the header_fields contains more than one element of
Summary
                 header field type: generation_time
Reference
                 ETSI TS 103 097 [1], clause 7.2
                 PICS_GN_SECURITY
PICS Selection
                                          Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
    the IUT is receiving a SecuredMessage (DENM)
     containing header_fields[0].type
       indicating 'signer_info'
      containing header_fields[1].type
        indicating 'generation_time
      and containing header_fields[2].type
        indicating 'generation_time'
      and containing header_fields[3].type
       indicating 'generation_location'
      and containing header_fields[4] {
        containing type
          indicating 'its_aid'
        containing its_aid
          indicating 'AID_DENM'
      and not containing other header fields
  } then {
    the IUT discards a SecuredMessage
  }
```

| TP Id | TP_SEC_ITSS_RCV_DENM_04_05_BO | |
|--|---|--|
| Cummon | Check that IUT discards a secured DENM if the message does not contain the header field of type | |
| Summary | generation_time | |
| Reference | ETSI TS 103 097 [1], clause 7.2 | |
| PICS Selection | PICS_GN_SECURITY | |
| | Expected behaviour | |
| with { | | |
| the IUT being | in the 'authorized' state | |
| } | | |
| ensure that { | | |
| when { | | |
| | eceiving a SecuredMessage (DENM) | |
| | containing header_fields[0].type | |
| | indicating 'signer_info' | |
| _ | header_fields[1].type | |
| | ng 'generation_location' | |
| | ning header_fields[2] { | |
| containi | | |
| | ting 'its_aid' | |
| | containing its_aid | |
| indica | ting 'AID_DENM' | |
| } | | |
| and not containing other header fields | | |
| } then { | | |
| the IUT disc | ards a SecuredMessage | |
| } | | |
| } | | |

```
TP Id
                 TP_SEC_ITSS_RCV_DENM_04_06_BO
                 Check that IUT discards a secured DENM if the header_fields contains more than one element of
Summary
                 header field of type its_aid
Reference
                 ETSI TS 103 097 [1], clause 7.2
                 PICS_GN_SECURITY
PICS Selection
                                           Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
    the IUT is receiving a SecuredMessage (DENM)
      containing header_fields[0].type
        indicating 'signer_info'
      and containing header_fields[1].type
        indicating 'generation_time'
      and containing header_fields[2].type
        indicating 'generation_location'
      and containing header_fields[3] {
        containing type
          indicating 'its_aid'
        containing its_aid
          indicating 'AID_DENM'
      and containing header_fields[4] {
        containing type indicating 'its_aid'
        containing its_aid
          indicating 'AID_CAM'
      and not containing other header fields
  } then {
    the IUT discards a SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_DENM_04_07_BO | |
|--|---|--|
| IT IU | | |
| Summary | Check that IUT discards a secured DENM if the header_fields contains more than one element of | |
| | header field of type generation_location | |
| Reference | ETSI TS 103 097 [1], clause 7.2 | |
| PICS Selection | PICS_GN_SECURITY | |
| | Expected behaviour | |
| with { | | |
| the IUT being | in the 'authorized' state | |
| } | | |
| ensure that { | | |
| when { | | |
| | eceiving a SecuredMessage (DENM) | |
| | header_fields[0].type | |
| | ng 'signer_info' | |
| | and containing header_fields[1].type | |
| | indicating 'generation_time' | |
| | ning header_fields[2].type | |
| | ng 'generation_location' | |
| | ning header_fields[3].type | |
| indicating 'generation_location' | | |
| | and containing header_fields[4] { | |
| containing type | | |
| indicating 'its_aid' | | |
| containing its_aid | | |
| indicating 'AID_DENM' | | |
| } | | |
| <pre>and not containing other header fields } then {</pre> | | |
| , | <pre>then { the IUT discards a SecuredMessage</pre> | |
| l che ioi disca | arus a secureumessage | |
| | | |
| J | | |

```
TP Id
                  TP_SEC_ITSS_RCV_DENM_04_08_BO
                  Check that IUT discards a secured DENM if the message does not contain the header field of type
Summary
                  generation_location
                  ETSI TS 103 097 [1], clause 7.2
Reference
                  PICS_GN_SECURITY
PICS Selection
                                            Expected behaviour
with {
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage (DENM) containing header_fields[0].type
        indicating 'signer_info'
      containing header_fields[1].type
        indicating 'generation_time
      and containing header_fields[2] {
        containing type
          indicating 'its_aid'
        containing its_aid
          indicating 'AID_DENM'
      and not containing other header fields
  } then {
    the IUT discards a SecuredMessage
```

```
TP Id TP_SEC_ITSS_RCV_DENM_04_10_BO
Summary Check that IUT ignores the HeaderFields generation_time_standard_deviation of received Secured CAM

Reference ETSI TS 103 097 [1], clause 7.2

PICS Selection PICS_GN_SECURITY
```

```
Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage (DENM)
     containing header_fields[0].type
       indicating 'signer_info'
       containing signer
          containing certificate
           indicating CERT_TS_AT_A
      and containing header_fields[1] {
        containing type
         indicating 'generation_time_with_standard_deviation'
        containing generation_time_with_standard_deviation
          indicating TIME_2 inside the validity period of CERT_TS_AT_A
      and containing header_fields[2]{
       containing type
         indicating 'generation_time'
       containing generation_time
          indicating TIME_1 outside the validity period of CERT_TS_AT_A
      and containing header_fields[3].type
       indicating 'generation_location'
      and containing header_fields[4] {
       containing type
         indicating 'its_aid'
        containing its_aid
          indicating 'AID_DENM'
      and not containing other header fields
  } then {
   the IUT discards a SecuredMessage
```

```
TP Id TP_SEC_ITSS_RCV_DENM_04_11_BO

Summary Check that IUT ignores the HeaderFields generation_time_standard_deviation of received Secured CAM

Reference ETSI TS 103 097 [1], clause 7.2

PICS Selection PICS_GN_SECURITY
```

```
Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage (DENM)
     containing header_fields[0].type
       indicating 'signer_info'
       containing signer
          containing certificate
           indicating CERT_TS_AT_A
      and containing header_fields[1]{
        containing type
         indicating 'generation_time'
        containing generation_time
          indicating TIME_1 inside the validity period of CERT_TS_AT_A
      and containing header_fields[2] {
       containing type
         indicating 'generation_time_with_standard_deviation'
       containing generation_time_with_standard_deviation
          indicating TIME_2 outside the validity period of CERT_TS_AT_A
      and containing header_fields[3].type
       indicating 'generation_location'
      and containing header_fields[4] {
       containing type
         indicating 'its_aid'
       containing its_aid
          indicating 'AID_DENM'
      and not containing other header fields
  } then {
   the IUT accepts a SecuredMessage
```

```
TP Id
                 TP_SEC_ITSS_RCV_DENM_04_12_BV
Summary
                 Check that IUT ignores the HeaderFields expiry_time of received Secured DENM
Reference
                 ETSI TS 103 097 [1], clause 7.2
PICS Selection
                 PICS_GN_SECURITY
                                          Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
 when {
    the IUT is receiving a SecuredMessage (DENM)
      containing header_fields[0].type
       indicating 'signer_info'
      containing header_fields[1]{
        containing type
          indicating 'generation_time'
        containing generation_time
          indicating TIME_1 ( TIME_1 < CURRENT_TIME - 1min )</pre>
      and containing header_fields[2] {
        containing type
          indicating 'expiration'
        containing expiry_time
          indicating TIME_2 (TIME_1 < TIME_2 < CURRENT_TIME)</pre>
      and containing header_fields[3].type
       indicating 'generation_location
      and containing header_fields[4] {
```

5.3.3.4 Check signer info

containing type

} then {

} then {

indicating 'its_aid'
containing its_aid
indicating 'AID_DENM'

the IUT accepts a SecuredMessage

and not containing other header fields

and containing header_fields['its_aid']

and not containing other header fields

indicating 'AID_DENM'

the IUT discards a SecuredMessage

| TP ld | TP_SEC_ITSS_RCV_DENM_05_01_BO | | |
|---|--|--|--|
| Summary | Check that IUT discards a secured DENM if the header_fields contains a signer of type 'self' | | |
| Reference | ETSI TS 103 097 [1], clause 7.2 | | |
| PICS Selection | PICS_GN_SECURITY | | |
| | Expected behaviour | | |
| <pre>with { the IUT being } ensure that {</pre> | in the 'authorized' state | | |
| <pre>when { the IUT is receiving a SecuredMessage (DENM) { containing header_fields['signer_info'] containing signer.type indicating 'self' and containing header_fields['generation_time'] and containing header_fields['generation_location']</pre> | | | |

```
TP Id
                    TP_SEC_ITSS_RCV_DENM_05_02_BO
                    Check that IUT discards a secured DENM if the header_fields contains a signer of type
Summary
                    certificate_digest_with_other_algorithm'
Reference
                    ETSI TS 103 097 [1], clause 7.2
                    PICS_GN_SECURITY
PICS Selection
                                                Expected behaviour
with {
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage (DENM) {
    containing header_fields['signer_info']
         containing signer.type
           indicating 'certificate_digest_with_other_algorithm'
       and containing header_fields['generation_time'] and containing header_fields['generation_location']
       and containing header_fields['its_aid']
         indicating 'AID_DENM'
       and not containing other header fields
  } then {
    the IUT discards a SecuredMessage
```

| TP Id | TP SEC ITSS RCV DENM 05 03 BO |
|--|---|
| Summary | Check that IUT discards a secured DENM if the header_fields contains a signer of type certificate_chain |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| ensure that { when { the IUT is recontaining containing | in the 'authorized' state ceceiving a SecuredMessage (DENM) { header_fields['signer_info'] .ng signer { .ning type .cating 'certificate_chain' .ning header_fields['generation_time'] .ning header_fields['generation_location'] .ning header_fields['its_aid'] .ning header_fields['its_aid'] .ng 'AID_DENM' ontaining other header fields |
| <pre>} } then { the IUT discards a SecuredMessage } </pre> | |

5.3.3.5 Check generation time

| TP Id | TP_SEC_ITSS_RCV_DENM_06_01_BO |
|----------------|---|
| Summary | Check that IUT discards message containing generation_time before the certificate validity period |
| Reference | ETSI TS 103 097 [1], clauses 5.4 and 7.2 |
| PICS Selection | PICS_GN_SECURITY |

```
Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage (DENM) {
      containing header_fields[0] {
       containing type
         indicating 'signer_info'
       and containing signer {
         containing type
           indicating 'certificate'
          and containing certificate (CERT_TS_AT_A) {
           containing validity_restrictions['time_start_and_end'] {
              containing start_validity
               indicating TIME_CERT_TS_AT_START
              and containing end_validity
                indicating TIME_CERT_TS_AT_END
            }
          }
       }
      and containing header_fields [1] {
       containing type
         indicating 'generation_time'
       containing generation_time
          indicating TIME_1 < TIME_CERT_TS_AT_START</pre>
      and containing header_fields [2] {
       containing type
          indicating 'generation_location'
      and containing header_fields[3] {
       containing type
         indicating 'its_aid'
       containing its_aid
          indicating 'AID_DENM'
  } then {
   the IUT discards the message
```

```
TP Id TP_SEC_ITSS_RCV_DENM_06_02_BO

Summary Check that IUT discards message containing generation_time after the certificate validity period

Reference ETSI TS 103 097 [1], clauses 5.4 and 7.2

PICS Selection PICS_GN_SECURITY
```

```
Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage (DENM) {
      containing header_fields[0] {
       containing type
         indicating 'signer_info'
       and containing signer {
          containing type
            indicating 'certificate'
          and containing certificate (CERT_TS_AT_A) {
           containing validity_restrictions['time_start_and_end'] {
              containing start_validity
                indicating TIME_CERT_TS_AT_START
              and containing end_validity
                indicating TIME_CERT_TS_AT_END
            }
          }
      and containing header_fields [1] {
       containing type
          indicating 'generation_time'
       containing generation_time
          indicating TIME_1 > TIME_CERT_TS_AT_END
      and containing header_fields [2] {
       containing type
          indicating 'generation_location'
      and containing header_fields[3] {
       containing type
         indicating 'its_aid'
       containing its_aid
          indicating 'AID_DENM'
  } then {
   the IUT discards the message
```

5.3.3.6 Check its_aid

```
TP Id
                 TP_SEC_ITSS_RCV_DENM_07_01_BO
Summary
                 Check that IUT discards secured DENM when its_aid value is not AID_DENM
Reference
                 ETSI TS 103 097 [1], clause 7.2
PICS Selection
                 PICS_GN_SECURITY
                                          Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage (DENM)
      containing header_fields['its_aid']
        indicating AID_CAM
      and containing payload_field {
        containing type
          indicating 'signed'
        containing data
          containing DENM payload
      }
  } then {
    the IUT discards the message
```

5.3.3.7 Check generation location

```
TP Id
              TP_SEC_ITSS_RCV_DENM_08_01_BO
              Check that IUT discards Secured DENM if the HeaderField generation_location is outside of the circular
Summary
              validity region of the signing certificate
Reference
              ETSI TS 103 097 [1], clause 7.2
PICS Selection PICS_GN_SECURITY, PICS_USE_CIRCULAR_REGION
                                           Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
 when {
    the IUT is receiving a SecuredMessage
      and containing header_fields ['signer_info'].type
        indicating certificate
      and containing header_fields ['signer_info'].certificate (CERT_TS_AT_B)
        containing validity_restrictions ['region'] {
          containing region{
            containing region_type
              indicating 'circle
            containing circular_region
              indicating REGION
        }
      and containing header_fields ['generation_location']
        {\tt containing \ generation\_location}
          indicating value outside of the REGION
      and containing header_fields['its_aid']
        indicating 'AID_DENM'
  } then {
    the IUT discards the message
```

```
TP Id
                  TP_SEC_ITSS_RCV_DENM_08_02_BO
                  Check that IUT discards Secured DENM if the HeaderField generation_location is outside of the
Summary
                  rectangular validity region of the signing certificate
Reference
                  ETSI TS 103 097 [1], clause 7.2
                  PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION
PICS Selection
                                            Expected behaviour
with {
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info'].type
        indicating certificate
      and containing header_fields ['signer_info'].certificate (CERT_TS_AT_C)
        containing validity_restrictions ['region'] {
          containing region{
            containing region_type
              indicating 'rectangle'
             containing rectangular_regions
               indicating REGION
      and containing header_fields ['generation_location']
        containing generation_location
      indicating value outside of the REGION and containing header_fields['its_aid']
        indicating 'AID_DENM'
  } then {
    the IUT discards the message
```

| Summary Check that IUT discards Secured DENM if the HeaderField generation_location is outside of the polygonal validity region of the signing certificate Reference ETSI TS 103 097 [1], clause 7.2 PICS Selection PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION Expected behaviour | | | |
|--|----------------|---|--|
| polygonal validity region of the signing certificate Reference ETSI TS 103 097 [1], clause 7.2 PICS Selection PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION Expected behaviour with { the IUT being in the 'authorized' state } ensure that { when { the IUT is receiving a SecuredMessage containing header_fields ['signer_info'].type indicating certificate and containing header_fields ['signer_info'].certificate (CERT_TS_AT_D) containing validity_restrictions ['region'] { containing region_type indicating region_type indicating 'polygon' containing polygonal_region indicating REGION } } and containing header_fields ['generation_location'] containing generation_location indicating value outside of the REGION and containing header_fields['its_aid'] indicating 'AID_DENM' } then { | TP Id | TP_SEC_ITSS_RCV_DENM_08_03_BO | |
| Reference ETSITS 103 097 [1], clause 7.2 PICS Selection PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION Expected behaviour with { the IUT being in the 'authorized' state } ensure that { when { the IUT is receiving a SecuredMessage containing header_fields ['signer_info'].type indicating certificate and containing header_fields ['signer_info'].certificate (CERT_TS_AT_D) containing region{ containing region_type | Cummoru | Check that IUT discards Secured DENM if the HeaderField generation_location is outside of the | |
| PICS Selection PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION Expected behaviour with { the IUT being in the 'authorized' state } ensure that { when { the IUT is receiving a SecuredMessage | Summar y | polygonal validity region of the signing certificate | |
| <pre>with { the IUT being in the 'authorized' state } ensure that { when { the IUT is receiving a SecuredMessage containing header_fields ['signer_info'].type indicating certificate and containing header_fields ['signer_info'].certificate (CERT_TS_AT_D) containing validity_restrictions ['region'] { containing region{ containing region_type indicating 'polygon' containing polygonal_region indicating REGION</pre> | Reference | ETSI TS 103 097 [1], clause 7.2 | |
| <pre>with { the IUT being in the 'authorized' state } ensure that { when { the IUT is receiving a SecuredMessage containing header_fields ['signer_info'].type indicating certificate and containing header_fields ['signer_info'].certificate (CERT_TS_AT_D) containing validity_restrictions ['region'] { containing region{ containing region_type</pre> | PICS Selection | PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION | |
| <pre>the IUT being in the 'authorized' state } ensure that { when { the IUT is receiving a SecuredMessage containing header_fields ['signer_info'].type indicating certificate and containing header_fields ['signer_info'].certificate (CERT_TS_AT_D) containing validity_restrictions ['region'] { containing region_type indicating 'polygon' containing polygonal_region indicating REGION } } and containing header_fields ['generation_location'] containing generation_location indicating value outside of the REGION and containing header_fields['its_aid'] indicating 'AID_DENM' } then {</pre> | | Expected behaviour | |
| <pre>Pensure that { when { the IUT is receiving a SecuredMessage containing header_fields ['signer_info'].type indicating certificate and containing header_fields ['signer_info'].certificate (CERT_TS_AT_D) containing validity_restrictions ['region'] { containing region{ containing region_type</pre> | with { | | |
| <pre>when { the IUT is receiving a SecuredMessage containing header_fields ['signer_info'].type indicating certificate and containing header_fields ['signer_info'].certificate (CERT_TS_AT_D) containing validity_restrictions ['region'] { containing region{ containing region_type</pre> | the IUT being | in the 'authorized' state | |
| <pre>when { the IUT is receiving a SecuredMessage containing header_fields ['signer_info'].type indicating certificate and containing header_fields ['signer_info'].certificate (CERT_TS_AT_D) containing validity_restrictions ['region'] { containing region{ containing region_type</pre> | } | | |
| <pre>the IUT is receiving a SecuredMessage containing header_fields ['signer_info'].type indicating certificate and containing header_fields ['signer_info'].certificate (CERT_TS_AT_D) containing validity_restrictions ['region'] { containing region{ containing region_type indicating 'polygon' containing polygonal_region indicating REGION } } and containing header_fields ['generation_location'] containing generation_location indicating value outside of the REGION and containing header_fields['its_aid'] indicating 'AID_DENM' } then {</pre> | , | | |
| <pre>containing header_fields ['signer_info'].type indicating certificate and containing header_fields ['signer_info'].certificate (CERT_TS_AT_D) containing validity_restrictions ['region'] { containing region{ containing region_type indicating 'polygon' containing polygonal_region indicating REGION } } and containing header_fields ['generation_location'] containing generation_location indicating value outside of the REGION and containing header_fields['its_aid'] indicating 'AID_DENM' } then {</pre> | | and taking a Garage Manager | |
| <pre>indicating certificate and containing header_fields ['signer_info'].certificate (CERT_TS_AT_D) containing validity_restrictions ['region'] { containing region{ containing region_type</pre> | | g g | |
| <pre>and containing header_fields ['signer_info'].certificate (CERT_TS_AT_D) containing validity_restrictions ['region'] { containing region{ containing region_type</pre> | _ | | |
| <pre>containing validity_restrictions ['region'] { containing region{ containing region_type indicating 'polygon' containing polygonal_region indicating REGION } } and containing header_fields ['generation_location'] containing generation_location indicating value outside of the REGION and containing header_fields['its_aid'] indicating 'AID_DENM' } then {</pre> | | | |
| <pre>containing region{ containing region_type indicating 'polygon' containing polygonal_region indicating REGION } and containing header_fields ['generation_location'] containing generation_location indicating value outside of the REGION and containing header_fields['its_aid'] indicating 'AID_DENM' } then {</pre> | | | |
| <pre>containing region_type indicating 'polygon' containing polygonal_region indicating REGION } } and containing header_fields ['generation_location'] containing generation_location indicating value outside of the REGION and containing header_fields['its_aid'] indicating 'AID_DENM' } then {</pre> | | | |
| <pre>containing polygonal_region indicating REGION } and containing header_fields ['generation_location'] containing generation_location indicating value outside of the REGION and containing header_fields['its_aid'] indicating 'AID_DENM' } then {</pre> | | | |
| <pre>indicating REGION } and containing header_fields ['generation_location'] containing generation_location indicating value outside of the REGION and containing header_fields['its_aid'] indicating 'AID_DENM' } then {</pre> | in | dicating 'polygon' | |
| <pre>} } and containing header_fields ['generation_location'] containing generation_location indicating value outside of the REGION and containing header_fields['its_aid'] indicating 'AID_DENM' } then {</pre> | cont | aining polygonal_region | |
| <pre>containing generation_location indicating value outside of the REGION and containing header_fields['its_aid'] indicating 'AID_DENM' } then {</pre> | in | indicating REGION | |
| <pre>containing generation_location indicating value outside of the REGION and containing header_fields['its_aid'] indicating 'AID_DENM' } then {</pre> | } | | |
| <pre>containing generation_location indicating value outside of the REGION and containing header_fields['its_aid'] indicating 'AID_DENM' } then {</pre> | } | | |
| <pre>indicating value outside of the REGION and containing header_fields['its_aid'] indicating 'AID_DENM' } then {</pre> | | | |
| <pre>and containing header_fields['its_aid'] indicating 'AID_DENM' } then {</pre> | | 3 3 = | |
| indicating 'AID_DENM' } then { | g · | | |
| } then { | | | |
| | | ng http://doi.org/ | |
| } | , | ards the message | |
| ' _} | } | 5 | |
| | } | | |

```
TP Id
                  TP_SEC_ITSS_RCV_DENM_08_04_BO
                  Check that IUT discards Secured DENM if the HeaderField generation_location is outside of the
Summary
                  identified validity region of the signing certificate
Reference
                  ETSI TS 103 097 [1], clause 7.2
                  PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION
PICS Selection
                                            Expected behaviour
with {
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info'].type
        indicating certificate
      and containing header_fields ['signer_info'].certificate (CERT_TS_AT_E)
        containing validity_restrictions ['region'] {
          containing region{
            containing region_type
               indicating 'id_region'
             and containing identified_region
               indicating REGION
      and containing header_fields ['generation_location']
        containing generation_location
      indicating value outside of the REGION and containing header_fields['its_aid']
        indicating 'AID_DENM'
  } then {
    the IUT discards the message
```

5.3.3.8 Check Payload

| TP Id | TP_SEC_ITSS_RCV_DENM_09_02_BO | |
|------------------------------|--|--|
| Summary | Check that IUT discards the Secured DENM containing empty payload of type 'signed' | |
| Reference | ETSI TS 103 097 [1], clause 7.2 | |
| PICS Selection | PICS_GN_SECURITY | |
| | Expected behaviour | |
| with { | | |
| the IUT being | in the 'authorized' state | |
| } | | |
| ensure that { | | |
| when { | | |
| the IUT is r | eceiving a SecuredMessage { | |
| containin | containing header_fields['its_aid'] | |
| indicati | indicating 'AID_DENM' | |
| and contain | ning payload_field { | |
| containi | ng type | |
| indica | ting 'signed' | |
| containi | containing data | |
| indica | indicating length 0 | |
| } | | |
| } | | |
| } then { | | |
| the IUT discards the message | | |
| } | | |
| } | | |

```
TP Id
                  TP_SEC_ITSS_RCV_DENM_09_03_BO
Summary
                  Check that IUT discards the Secured DENM containing non-empty payload of type 'unsecured'
Reference
                  ETSI TS 103 097 [1], clause 7.2
PICS Selection
                 PICS_GN_SECURITY
                                           Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
 when {
the IUT is receiving a SecuredMessage {
      containing header_fields['its_aid']
        indicating 'AID_DENM'
      and containing payload_field {
        containing type
indicating 'unsecured'
  } then {
    the IUT discards the message
```

| TP_SEC_ITSS_RCV_DENM_09_04_BO | |
|---|--|
| Check that IUT discards the Secured DENM containing non-empty payload of type 'encrypted' | |
| ETSI TS 103 097 [1], clause 7.2 | |
| PICS_GN_SECURITY | |
| Expected behaviour | |
| | |
| in the 'authorized' state | |
| | |
| | |
| | |
| the IUT is receiving a SecuredMessage { | |
| containing header_fields['its_aid'] | |
| ng 'AID DENM' | |
| ning payload_field { | |
| ng type | |
| indicating 'encrypted' | |
| | |
| } | |
| } then { | |
| the IUT discards the message | |
| - | |
| | |
| 1 | |

| TP ld | TP_SEC_ITSS_RCV_DENM_09_05_BO | |
|----------------|---|--|
| Summary | Check that IUT discards the Secured DENM containing non-empty payload of type 'signed_external' | |
| Reference | ETSI TS 103 097 [1], clause 7.2 | |
| PICS Selection | PICS_GN_SECURITY | |
| | Expected behaviour | |
| with { | | |
| the IUT being | in the 'authorized' state | |
| } | | |
| ensure that { | | |
| when { | | |
| the IUT is re | eceiving a SecuredMessage { | |
| containing | containing header_fields['its_aid'] | |
| indicati | indicating 'AID_DENM' | |
| and contain | and containing payload_field { | |
| containi | ng type | |
| indica | indicating 'signed_external' | |
| } | } | |
| } | | |
| } then { | | |
| the IUT disc | the IUT discards the message | |
| } | | |
| } | | |

```
TP Id
                   TP_SEC_ITSS_RCV_DENM_09_06_BO
                   Check that IUT discards the Secured DENM containing exactly one non-empty payload of type
Summary
                   'signed_and_encrypted'
Reference
                   ETSI TS 103 097 [1], clause 7.2
PICS Selection
                   PICS_GN_SECURITY
                                                Expected behaviour
with {
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
   containing header_fields['its_aid']
   indicating 'AID_DENM'
      and containing payload_field {
        containing type
           indicating 'signed_and_encrypted'
      }
  } then {
    the IUT discards the message
```

5.3.3.9 Check presence of trailer field

| TP Id | TP_SEC_ITSS_RCV_DENM_10_01_BO | | |
|------------------------|--|--|--|
| Cummoru | Check that IUT discards the Secured DENM if the message does not contain the trailer field of type | | |
| Summary | signature | | |
| Reference | ETSI TS 103 097 [1], clause 7.2 | | |
| PICS Selection | PICS_GN_SECURITY | | |
| | Expected behaviour | | |
| with { | | | |
| the IUT being | in the 'authorized' state | | |
| } | | | |
| ensure that { | | | |
| when { | and in the state of the state o | | |
| | the IUT is receiving a SecuredMessage { | | |
| _ | containing header_fields['its_aid'] | | |
| | ng 'AID_DENM' | | |
| | ning trailer_fields | | |
| | aining any instance of type TrailerField { | | |
| | containing type | | |
| indicating 'signature' | | | |
| } | | | |
| } | | | |
| then { | | | |
| tne IUT disca | the IUT discards the message | | |
| , } | | | |
| } | | | |

```
TP Id
                   TP_SEC_ITSS_RCV_DENM_10_02_BO
                   Check that IUT discards the Secured DENM containing more than one instance of TrailerField of
Summary
                   type 'signature'
Reference
                   ETSI TS 103 097 [1], clause 7.2
PICS Selection
                   PICS_GN_SECURITY
                                               Expected behaviour
with {
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
   containing header_fields['its_aid']
   indicating 'AID_DENM'
      and containing trailer_fields[0]
        containing type
           indicating 'signature'
      and containing trailer_fields[1]
         containing type
           indicating 'signature'
  } then {
    the IUT discards the message
```

5.3.3.10 Check signature

TP SEC ITSS RCV DENM 11 01 BO

TP Id

| Check that the IUT discards Secured DENM containing signature that is not verified using the | |
|--|--|
| verification key from the certificate contained in the message's signer info | |
| ETSI TS 103 097 [1], clause 7.2 | |
| PICS_GN_SECURITY | |
| Expected behaviour | |
| | |
| in the 'authorized' state | |
| | |
| | |
| | |
| receiving a SecuredMessage { | |
| g header_fields ['signer_info'] { | |
| ing signer { ining type | |
| icating 'certificate' | |
| ining certificate (CERT_TS_AT_A) | |
| taining subject_info.subject_type | |
| ndicating 'authorization_ticket' (2) | |
| containing subject_attributes['verification key'] | |
| ontaining key (KEY) | |
| | |
| | |
| g header_fields['its_aid'] | |
| ing 'AID_DENM' | |
| g trailer_fields { | |
| ing single instance of type TrailerField { | |
| <pre>containing type indicating 'signature'</pre> | |
| containing signature | |
| NOT verifiable using KEY | |
| | |
| | |
| | |
| | |
| cards the message | |
| | |
| | |

5.3.3.11 Check signing certificate type

| TP Id | TP_SEC_ITSS_RCV_DENM_12_01_BO |
|--|--|
| Summary | Check that IUT discards a Secured DENM if the signer certificate of the message contains the subject type 'enrolment_credential' |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>with { the IUT being } ensure that { when {</pre> | in the 'authorized' state |
| <pre>the IUT is receiving a SecuredMessage containing header_fields ['signer_info'] { containing signer.type indicating 'certificate' containing signer.certificate (CERT_TS_EA_A) containing subject_info.subject_type indicating 'enrolment_credentials' }</pre> | |
| <pre>containing header_fields['its_aid'] indicating 'AID_DENM' } then { the IUT discards the message } </pre> | |

| _ | |
|---|--|
| TP Id | TP_SEC_ITSS_RCV_DENM_12_02_BO |
| Summary | Check that IUT discards a Secured DENM if the signer certificate of the message contains the subject type "authorization_authority" |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>} ensure that { when { the IUT is r containing containin indica containi contai indi } containing</pre> | <pre>in the 'authorized' state eceiving a SecuredMessage header_fields ['signer_info'] { ng signer.type ting 'certificate' ng signer.certificate (CERT_TS_AA_A) ning subject_info.subject_type cating 'authorization_authority' header_fields['its_aid'] ng 'AID DENM'</pre> |
| <pre>} then { the IUT disc }</pre> | ards the message |

5.3.4 Generic Signed Message Profile

5.3.4.1 Check that IUT accepts well-formed GN Beacon message

| TP Id | TP_SEC_ITSS_RCV_GENMSG_01_01_BV |
|-------------------------------------|---|
| | Check that IUT accepts a well-formed Secured GN Beacon signed with the certificate without region |
| Summary | validity restriction |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| 1 100 delection | Expected behaviour |
| 1.1 | Expected benaviour |
| <pre>with { the IUT being }</pre> | in the 'authorized' state |
| ensure that { | |
| when { the TUT is a | receiving a SecuredMessage |
| | g protocol_version |
| | ing value '2' |
| | ning header_fields[0] |
| containi | |
| indica | ating 'signer_info' |
| and cont | aining signer { |
| contai | ning type |
| indi | cating 'certificate' |
| | ontaining certificate (CERT_TS_AT_A) { |
| | caining subject_info.subject_type |
| | ndicating 'authorization_ticket' (2) |
| | containing subject_attributes['verification key'] (KEY) |
| l . | not containing validity_restrictions['region'] |
| } | |
| and contai | ining header_fields [1] { |
| containi | |
| | ating 'generation_time' |
| | ing generation_time |
| | ating CURRENT_TIME |
| } | |
| and contain | ining header_fields [2] { |
| containi | · |
| indica | ating 'generation_location' |
| containi | ing generation_location |
| } | |
| and contain | ining header_fields[3] { |
| containi | ing type |
| | ating 'its_aid' |
| | ing its_aid |
| indica | ating 'AID_BEACON' |
| } | uine manland field (|
| | <pre>lning payload_field {</pre> |
| | ing type |
| | ating 'signed' |
| | ing data ating length > 0 |
| l | acting tength > 0 |
| and contai | ining trailer_fields { |
| | ing single instance of type TrailerField { |
| | Ining type |
| | Loating 'signature' |
| | Ining signature |
| | Ifiable using KEY |
| } | |
| } ' | |
| } then { | |
| the IUT acce | epts the message |
| ı l | |

```
TP Id TP_SEC_ITSS_RCV_GENMSG_01_02_BV

Summary Check that IUT accepts a well-formed Secured GN Beacon signed with the certificate with a circular region validity restriction

Reference ETSI TS 103 097 [1], clause 7.3

PICS Selection PICS_GN_SECURITY
```

```
Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage
     containing protocol_version
       indicating value '2'
      and containing header_fields[0] {
        containing type
          indicating 'signer_info'
        and containing signer {
          containing type
            indicating 'certificate'
          and containing certificate (CERT_TS_AT_B) {
            containing subject_info.subject_type
              indicating 'authorization_ticket' (2)
            and containing subject_attributes['verification key'] (KEY)
            and containing validity_restrictions['region'] {
              containing region{
                containing region_type
                  indicating 'circle'
                and containing circular_region
                  indicating REGION
          }
       }
      and containing header_fields [1] {
        containing type
          indicating 'generation_time'
        containing generation_time
          indicating CURRENT_TIME
      and containing header_fields [2] {
        containing type
         indicating 'generation_location'
        containing generation_location
          indicating position inside the REGION
      and containing header_fields[3] {
       containing type
          indicating 'its_aid'
        containing its_aid
          indicating 'AID_BEACON'
      and containing payload_field {
        containing type
         indicating 'signed'
        containing data
          indicating length > 0
      and containing trailer_fields {
       containing single instance of type TrailerField {
         containing type
            indicating 'signature'
          containing signature
            verifiable using KEY
      }
  } then {
    the IUT accepts the message
```

```
TP Id TP_SEC_ITSS_RCV_GENMSG_01_03_BV

Summary Check that IUT accepts a well-formed Secured GN Beacon signed with the certificate with a rectangular region validity restriction

Reference ETSI TS 103 097 [1], clause 7.3

PICS Selection PICS_GN_SECURITY
```

```
Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage
     containing protocol_version
       indicating value '2'
      and containing header_fields[0]
        containing type
          indicating 'signer_info'
        and containing signer {
          containing type
            indicating 'certificate'
          and containing certificate (CERT_TS_AT_C) {
            containing subject_info.subject_type
              indicating 'authorization_ticket' (2)
            and containing subject_attributes['verification key'] (KEY)
            and containing validity_restrictions['region'] {
              containing region{
                containing region_type
                  indicating 'rectangle'
                and containing rectangular_regions
                  indicating REGIONS
          }
      and containing header_fields [1] {
       containing type
          indicating 'generation_time'
        containing generation_time
          indicating CURRENT_TIME
      and containing header_fields [2] {
        containing type
          indicating 'generation_location'
        containing generation_location
          indicating position inside the REGION
      and containing header_fields[3] {
       containing type
         indicating 'its_aid
        containing its_aid
          indicating 'AID_BEACON'
      and containing payload_field {
        containing type
          indicating 'signed'
        containing data
          indicating length > 0
      and containing trailer_fields {
        containing single instance of type TrailerField {
          containing type
           indicating 'signature'
          containing signature
            verifiable using KEY
      }
  } then {
    the IUT accepts the message
```

```
TP Id TP_SEC_ITSS_RCV_GENMSG_01_04_BV

Summary Check that IUT accepts a well-formed Secured GN Beacon signed with the certificate with a polygonal region validity restriction

Reference ETSI TS 103 097 [1], clause 7.3

PICS Selection PICS_GN_SECURITY
```

```
Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage
     containing protocol_version
       indicating value '2'
      and containing header_fields[0]
        containing type
          indicating 'signer_info'
        and containing signer {
          containing type
            indicating 'certificate'
          and containing certificate (CERT_TS_AT_D) {
            containing subject_info.subject_type
              indicating 'authorization_ticket' (2)
            and containing subject_attributes['verification key'] (KEY)
            and containing validity_restrictions['region'] {
              containing region{
                containing region_type
                  indicating 'polygon'
                and containing polygonal_region
                  indicating REGION
          }
      and containing header_fields [1] {
       containing type
          indicating 'generation_time'
        containing generation_time
          indicating CURRENT_TIME
      and containing header_fields [2] {
        containing type
          indicating 'generation_location'
        containing generation_location
          indicating position inside the REGION
      and containing header_fields[3] {
       containing type
         indicating 'its_aid
        containing its_aid
          indicating 'AID_BEACON'
      and containing payload_field {
        containing type
          indicating 'signed'
        containing data
          indicating length > 0
      and containing trailer_fields {
        containing single instance of type TrailerField {
          containing type
           indicating 'signature'
          containing signature
            verifiable using KEY
      }
  } then {
    the IUT accepts the message
```

```
TP Id TP_SEC_ITSS_RCV_GENMSG_01_05_BV

Summary Check that IUT accepts a well-formed Secured GN Beacon signed with the certificate with an identified region validity restriction

Reference ETSI TS 103 097 [1], clause 7.3

PICS_GN_SECURITY
```

```
Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage
     containing protocol_version
       indicating value '2'
      and containing header_fields[0]
        containing type
          indicating 'signer_info'
        and containing signer {
          containing type
            indicating 'certificate'
          and containing certificate (CERT_TS_AT_E) {
            containing subject_info.subject_type
              indicating 'authorization_ticket' (2)
            and containing subject_attributes['verification key'] (KEY)
            and containing validity_restrictions['region'] {
              containing region{
                containing region_type
                  indicating 'id_region'
                and containing identified_region
                  indicating REGION
          }
      and containing header_fields [1] {
       containing type
          indicating 'generation_time'
        containing generation_time
          indicating CURRENT_TIME
      and containing header_fields [2] {
        containing type
          indicating 'generation_location'
        containing generation_location
          indicating position inside the REGION
      and containing header_fields[3] {
       containing type
         indicating 'its_aid
        containing its_aid
          indicating 'AID_BEACON'
      and containing payload_field {
        containing type
          indicating 'signed'
        containing data
          indicating length > 0
      and containing trailer_fields {
        containing single instance of type TrailerField {
          containing type
           indicating 'signature'
          containing signature
            verifiable using KEY
      }
  } then {
    the IUT accepts the message
```

```
TP Id
                                                                                                               TP_SEC_ITSS_RCV_GENMSG_01_06_BV
                                                                                                               Check that IUT accepts a well-formed Secured GN Message containing payload of type
 Summary
                                                                                                              signed_external
Reference
                                                                                                               ETSI TS 103 097 [1], clause 7.3
                                                                                                              PICS_GN_SECURITY
PICS Selection
                                                                                                                                                                                                                                                                             Expected behaviour
 with {
            the IUT being in the 'authorized' state
 ensure that {
            when {
                         the IUT is receiving a SecuredMessage {
                                      and containing header_fields[0] {
                                                   containing type
                                                               indicating 'signer_info'
                                                   and containing signer.type
                                                           indicating 'certificate'
                                                   and containing signer.certificate % \frac{1}{2}\left( \frac{1}{2}\right) =\frac{1}{2}\left( \frac{1
                                                                 indicating CERT_TS_AT_A
                                      and containing header_fields['its_aid'] indicating 'AID_BEACON'
                                       and containing payload\_field
                                                   containing type
                                                                 indicating 'signed_external'
              } then {
                          the IUT accepts the message
```

| TP ld | TP_SEC_ITSS_RCV_GENMSG_01_07_BV |
|---|--|
| Summary | Check that IUT accepts a well-formed Secured GN Message containing payload of type signed_and_encrypted |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>} ensure that { when { the IUT is r and contain indical and contai indical and contai indical and contai indical and contail indicating indicating</pre> | ting 'signer_info' aining signer.type ting 'certificate' aining signer.certificate ting CERT_TS_AT_A ning header_fields['its_aid'] ng 'AID_BEACON' ning payload_field |

5.3.4.2 Check the message protocol version

| TP ld | TP_SEC_ITSS_RCV_GENMSG_02_01_BO |
|--|--|
| Summary | Check that IUT discards a Secured GN Message containing protocol version set to a value less than 2 |
| Reference | ETSI TS 103 097 [1], clause 5.2 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>} ensure that { when { the IUT is recontaining indicating and containing indicating } }</pre> | eceiving a SecuredMessage protocol_version ng 1 ning header_fields['its_aid'] ng 'AID_BEACON' ards a SecuredMessage |

| TP ld | TP_SEC_ITSS_RCV_GENMSG_02_02_BO |
|--|---|
| Silininary | Check that IUT discards a Secured GN Message containing protocol version set to a value greater than 2 |
| Reference | ETSI TS 103 097 [1], clause 5.2 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>} ensure that { when { the IUT is recontaining indicatir and contair indicatir indicatir } then {</pre> | eceiving a SecuredMessage protocol_version ng 3 ning header_fields['its_aid'] ng 'AID_BEACON' ards a SecuredMessage |

5.3.4.3 Check header fields

| TP ld | TP_SEC_ITSS_RCV_GENMSG_04_01_BO | |
|--|---|--|
| Summary | Check that IUT discards a secured GN Beacon if the header_fields contains more than one element of header field type: signer_info | |
| Reference | ETSI TS 103 097 [1], clause 7.3 | |
| PICS Selection | PICS_GN_SECURITY | |
| Expected behaviour | | |
| with { the IUT being in the 'authorized' state } ensure that { when { the IUT is receiving a SecuredMessage containing header_fields[0].type indicating 'signer_info' and containing header_fields[1].type indicating 'signer_info' and containing header_fields[2].type indicating 'generation_time' and containing header_fields[3].type indicating 'generation_location' and containing header_fields['its_aid'] indicating 'AID_BEACON' and not containing other header fields } then { the IUT discards a SecuredMessage } | | |

| TP Id | TP_SEC_ITSS_RCV_GENMSG_04_02_BO |
|--|--|
| Summary | Check that IUT discards a secured GN Beacon if the header_fields does not contain the header field type: signer_info |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>} ensure that { when { the IUT is r containing indicati and contai indicati and contai indicati and contai indicati and rot co } then {</pre> | eceiving a SecuredMessage header_fields[0].type ng 'generation_time' ning header_fields[1].type ng 'generation_location' ning header_fields['its_aid'] ng 'AID_BEACON' ntaining other header fields ards a SecuredMessage |

```
TP Id
                  TP_SEC_ITSS_RCV_GENMSG_04_04_BO
                  Check that IUT discards a secured GN Beacon if the header_fields contains more than one element
Summary
                 of header field type: generation_time
Reference
                  ETSI TS 103 097 [1], clause 7.3
                 PICS_GN_SECURITY
PICS Selection
                                           Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
    the IUT is receiving a SecuredMessage
      containing header_fields[0].type
        indicating 'signer_info'
      containing header_fields[1].type
        indicating 'generation_time
      and containing header_fields[2].type
        indicating 'generation_time'
      and containing header_fields[3].type
       indicating 'generation_location'
      and containing header_fields['its_aid']
indicating 'AID_BEACON'
      and not containing other header fields
  } then {
    the IUT discards a SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_GENMSG_04_05_BO |
|--|--|
| Summary | Check that IUT discards a secured GN Beacon if the message does not contain the header field of type 'generation_time' |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| with { | |
| } ensure that { when { | in the 'authorized' state receiving a SecuredMessage |
| indicati and contai indicati and contai indicati and not co } then { | ng header_fields[0].type ng 'signer_info' ning header_fields[1].type ng 'generation_location' ning header_fields['its_aid'] ng 'AID_BEACON' ontaining other header fields eards a SecuredMessage |

```
TP Id
                  TP_SEC_ITSS_RCV_GENMSG_04_06_BO
                  Check that IUT discards a secured GN Beacon if the header_fields contains more than one element
Summary
                  of type: generation_location
Reference
                  ETSI TS 103 097 [1], clause 7.3
                 PICS_GN_SECURITY
PICS Selection
                                           Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
    the IUT is receiving a SecuredMessage
      containing header_fields[0].type
        indicating 'signer_info'
      and containing header_fields[1].type
        indicating 'generation_time'
      and containing header_fields[2].type
        indicating 'generation_location'
      and containing header_fields[3].type
       indicating 'generation_location'
      and containing header_fields['its_aid'] indicating 'AID_BEACON'
      and not containing other header fields
  } then {
    the IUT discards a SecuredMessage
```

| TP ld | TP_SEC_ITSS_RCV_GENMSG_04_07_BO | |
|--|---|--|
| Summary | Check that IUT discards a secured GN Beacon if the header_fields contains no element of header field type generation_location | |
| Reference | ETSI TS 103 097 [1], clause 7.3 | |
| PICS Selection | PICS_GN_SECURITY | |
| | Expected behaviour | |
| with { | | |
| the IUT being | in the 'authorized' state | |
|]} | | |
| | ensure that { | |
| , | when { | |
| | receiving a SecuredMessage g header_fields[0].type | |
| | ing 'signer_info' | |
| | ining header_fields[1].type | |
| | ing 'generation_time' | |
| | ining beader_fields['its_aid'] | |
| | • | |
| indicating 'AID_BEACON' and not containing other header fields | | |
| then { | | |
| the IUT discards a SecuredMessage | | |
| } | datab a beenteamenbage | |
| } | | |
| ال | | |

```
TP Id
                  TP_SEC_ITSS_RCV_GENMSG_04_09_BV
                  Check that IUT accepts SecuredMessage with GN Beacon payload and its_aid set to
                  AID_BEACON, containing in addition to the required fields the following optional HeaderFields:
Summary
                  expiry_time
                  ETSI TS 103 097 [1], clause 7.3
Reference
PICS Selection
                  PICS_GN_SECURITY
                                           Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
    the IUT is receiving a SecuredMessage
      containing header_fields[0].type
        indicating 'signer_info'
        containing signer
          containing certificate
            indicating CERT_TS_AT_A
      and containing header_fields[1]{
        containing type
          indicating 'generation_time'
        containing generation_time
          indicating TIME_1 inside the validity period of CERT_TS_AT_A
      and containing header_fields[2] {
        containing type
          indicating 'expiration'
        containing expiry_time
indicating TIME_2 (TIME_2 > CURRENT_TIME)
      and containing header_fields[3].type
        indicating 'generation_location
      and containing header_fields['its_aid']
        indicating 'AID_BEACON'
      and not containing other header fields
  } then {
    the IUT discards a SecuredMessage
```

5.3.4.4 Check signer info

| TP ld | TP SEC ITSS RCV GENMSG 05 01 BO |
|--|--|
| Summary | Check that IUT discards a secured GN Beacon if the header_fields contains a signer of type 'self' |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>ensure that { when { the IUT is recontaining containing indicae and contained and rot contained a</pre> | ecciving a SecuredMessage { header_fields['signer_info'] ng signer.type ting 'self' ning header_fields['generation_time'] ning header_fields['generation_location'] ning header_fields['its_aid'] ning header_fields['its_aid'] ng 'AID_BEACON' ntaining other header fields ards a SecuredMessage |

```
TP Id
                    TP_SEC_ITSS_RCV_GENMSG_05_02_BO
                    Check that IUT discards a secured GN Beacon if the header_fields contains a signer of type
Summary
                    certificate_digest_with_other_algorithm
Reference
                    ETSI TS 103 097 [1], clause 7.3
                   PICS_GN_SECURITY
PICS Selection
                                                Expected behaviour
with {
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
    containing header_fields['signer_info']
         containing signer.type
           indicating 'certificate_digest_with_other_algorithm'
      and containing header_fields['generation_time'] and containing header_fields['generation_location']
       and containing header_fields['its_aid']
         indicating 'AID_BEACON'
       and not containing other header fields
  } then {
    the IUT discards a SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_GENMSG_05_03_BO |
|--|--|
| Summary | Check that IUT discards a secured GN Beacon if the header_fields contains a signer of type certificate_chain |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>with { the IUT being } ensure that {</pre> | in the 'authorized' state |
| <pre>Pensure that { when { the IUT is receiving a SecuredMessage { containing header_fields['signer_info'] containing signer { containing type</pre> | |

5.3.4.5 Check generation time

| TP Id | TP_SEC_ITSS_RCV_GENMSG_06_01_BO |
|----------------|---|
| Summary | Check that IUT discards message containing generation_time before the certificate validity period |
| Reference | ETSI TS 103 097 [1], clauses 5.4 and 7.3 |
| PICS Selection | PICS_GN_SECURITY |

```
Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage \{
      containing header_fields[0] {
       containing type
         indicating 'signer_info'
       and containing signer {
         containing type
           indicating 'certificate'
          and containing certificate (CERT_TS_AT_A) {
           containing validity_restrictions['time_start_and_end'] {
              containing start_validity
               indicating TIME_CERT_TS_AT_START
              and containing end_validity
                indicating TIME_CERT_TS_AT_END
            }
          }
       }
      and containing header_fields [1] {
       containing type
          indicating 'generation_time'
       containing generation_time
          indicating TIME_1 < TIME_CERT_TS_AT_START</pre>
      and containing header_fields [2] {
       containing type
          indicating 'generation_location'
      and containing header_fields['its_aid']
        indicating 'AID_BEACON'
  } then {
   the IUT discards the message
```

```
TP Id TP_SEC_ITSS_RCV_GENMSG_06_02_BO

Summary Check that IUT discards message containing generation_time after the certificate validity period

Reference ETSI TS 103 097 [1], clauses 5.4 and 7.3

PICS_GN_SECURITY
```

```
Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage {
      containing header_fields[0] {
        containing type
         indicating 'signer_info'
        and containing signer {
          containing type
            indicating 'certificate'
          and containing certificate (CERT_TS_AT_A) {
            containing validity_restrictions['time_start_and_end'] {
              containing start_validity
                indicating TIME_CERT_TS_AT_START
              and containing end_validity
                indicating TIME_CERT_TS_AT_END
            }
          }
      and containing header_fields [1] {
        containing type
          indicating 'generation_time'
        containing generation_time
          indicating TIME_1 > TIME_CERT_TS_AT_END
      and containing header_fields [2] {
        containing type
          indicating 'generation_location'
      and containing header_fields['its_aid']
        indicating 'AID_BEACON'
  } then {
    the IUT discards the message
  }
```

5.3.4.6 Check generation location

```
TP Id
              TP_SEC_ITSS_RCV_GENMSG_08_01_BO
              Check that IUT discards Secured GN Message if the HeaderField generation_location is outside of the
Summary
              circular validity region of the signing certificate
              ETSI TS 103 097 [1], clause 7.3
Reference
PICS Selection PICS_GN_SECURITY, PICS_USE_CIRCULAR_REGION
                                          Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
 when {
    the IUT is receiving a SecuredMessage
      and containing header_fields ['signer_info'] {
        containing type
          indicating certificate
        and containing certificate (CERT_TS_AT_B)
          containing validity_restrictions ['region']
            containing region{
              containing region_type
                indicating 'circle'
              containing circular_region
                indicating REGION
      and containing header_fields ['generation_location']
        containing generation_location
          indicating value outside of the {\tt REGION}
      and containing header_fields['its_aid']
        indicating 'AID_BEACON'
  } then {
    the IUT discards the message
```

| TP Id | TP SEC ITSS RCV GENMSG 08 02 BO | |
|---|---|--|
| I F IU | | |
| Summary | Check that IUT discards Secured GN Message if the HeaderField generation_location is outside of | |
| | the rectangular validity region of the signing certificate | |
| Reference | ETSI TS 103 097 [1], clause 7.3 | |
| PICS Selection | PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION | |
| | Expected behaviour | |
| with { | | |
| the IUT being | in the 'authorized' state | |
| } | | |
| ensure that { | | |
| when { | | |
| | eceiving a SecuredMessage | |
| | ning header_fields ['signer_info'] { | |
| containi | | |
| | ting certificate | |
| | and containing certificate (CERT_TS_AT_C) | |
| | <pre>containing validity_restrictions ['region'] containing region{</pre> | |
| | | |
| | ntaining region_type indicating 'rectangle' | |
| | ntaining rectanguer ntaining rectangular_regions | |
| | indicating REGION | |
| ١ | indreating Region | |
| \ | | |
| and contai | ning header_fields ['generation_location'] | |
| containing generation location | | |
| indicating value outside of the REGION | | |
| and containing header_fields['its_aid'] | | |
| indicating 'AID_BEACON' | | |
| } then { | * = | |
| the IUT disc | the IUT discards the message | |
| } | | |
| } | | |

```
TP Id
                 TP_SEC_ITSS_RCV_GENMSG_08_03_BO
                 Check that IUT discards Secured GN Message if the optional HeaderField generation_location is
Summary
                 outside of the polygonal validity region of the signing certificate
Reference
                 ETSI TS 103 097 [1], clause 7.3
                 PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION
PICS Selection
                                          Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
    the IUT is receiving a SecuredMessage
      and containing header_fields ['signer_info'] {
        containing type
          indicating certificate
        and containing certificate (CERT_TS_AT_D)
          containing validity_restrictions ['region']
            containing region {
              containing region_type
                indicating 'polygon'
              containing polygonal_region
                indicating REGION
      and containing header_fields ['generation_location']
        containing generation_location
          indicating value outside of the REGION
      and containing header_fields['its_aid']
        indicating 'AID_BEACON'
  } then {
    the IUT discards the message
```

| TP ld | TP_SEC_ITSS_RCV_GENMSG_08_04_BO | |
|---|---|--|
| Cummoru | Check that IUT discards Secured GN Message if the optional HeaderField generation_location is | |
| Summary | outside of the identified validity region of the signing certificate | |
| Reference | ETSI TS 103 097 [1], clause 7.3 | |
| PICS Selection | PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION | |
| | Expected behaviour | |
| with { | | |
| the IUT being : | in the 'authorized' state | |
| } | | |
| ensure that { | | |
| when { | | |
| | eceiving a SecuredMessage | |
| _ | header_fields ['signer_info'] { | |
| containin | 5 11 | |
| | ting certificate aining certificate (CERT_TS_AT_E) | |
| | | |
| | <pre>containing validity_restrictions ['region'] containing region {</pre> | |
| | ntaining region_type | |
| | indicating 'id_region' | |
| | d containing identified_region | |
| | indicating REGION | |
| } | } | |
| } ' | | |
| and contain | and containing header_fields ['generation_location'] | |
| containin | containing generation location | |
| indicating value outside of the REGION | | |
| and containing header_fields['its_aid'] | | |
| indicating 'AID_BEACON' | | |
| } then { | | |
| the IUT disca | ards the message | |
| } | | |
| } | | |

5.3.4.7 Check Payload

| TP Id | TP_SEC_ITSS_RCV_GENMSG_09_02_BO |
|--|--|
| Summary | Check that IUT discards the Secured GN Message containing empty payload of type 'signed' |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>} ensure that { when { the IUT is r containing indicati and contain indicati containi indica containi indica containi indica } } } then {</pre> | ting 'signed' |

| TP ld | TP_SEC_ITSS_RCV_GENMSG_09_03_BO | |
|----------------|---|--|
| Summary | Check that IUT discards the Secured GN Message containing payload element of type 'unsecured' | |
| Reference | ETSI TS 103 097 [1], clause 7.3 | |
| PICS Selection | PICS_GN_SECURITY | |
| | Expected behaviour | |
| with { | | |
| the IUT being | in the 'authorized' state | |
| } | | |
| ensure that { | | |
| when { | | |
| | receiving a SecuredMessage $\{$ | |
| | g header_fields['its_aid'] | |
| | ng 'AID_BEACON' | |
| | ning payload_field { | |
| containi | | |
| indica | ting 'unsecured' | |
| } | | |
| | | |
| } then { | | |
| the IUT disc | the IUT discards the message | |
| } | | |
| } | | |

```
TP Id
                  TP_SEC_ITSS_RCV_GENMSG_09_04_BO
Summary
                  Check that IUT discards the Secured DENM containing payload element of type 'encrypted'
Reference
                  ETSI TS 103 097 [1], clause 7.3
PICS Selection
                 PICS_GN_SECURITY
                                           Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
 when {
the IUT is receiving a SecuredMessage {
      containing header_fields['its_aid']
        indicating 'AID_BEACON'
      and containing payload_field {
        containing type
indicating 'encrypted'
  } then {
    the IUT discards the message
```

5.3.4.8 Check presence of trailer field

| | T | | |
|----------------|--|--|--|
| TP ld | TP_SEC_ITSS_RCV_GENMSG_10_01_BO | | |
| Summary | Check that IUT discards the Secured GN Message if the message does not contain the trailer field | | |
| ourilliar y | of type 'signature' | | |
| Reference | ETSI TS 103 097 [1], clause 7.3 | | |
| PICS Selection | PICS_GN_SECURITY | | |
| | Expected behaviour | | |
| with { | | | |
| the IUT being | in the 'authorized' state | | |
| } | | | |
| ensure that { | | | |
| when { | | | |
| the IUT is re | the IUT is receiving a SecuredMessage { | | |
| containing | containing header_fields['its_aid'] | | |
| indicatir | ng 'AID_BEACON' | | |
| and contain | ning trailer_fields | | |
| not conta | aining any instance of type TrailerField { | | |
| contair | ning type | | |
| indic | indicating 'signature' | | |
| } | } | | |
| } | | | |
| } then { | | | |
| the IUT disca | the IUT discards the message | | |
| } | - | | |
| } | | | |
| <u>-</u> | | | |

```
TP Id
                     TP_SEC_ITSS_RCV_GENMSG_10_02_BO
                     Check that IUT discards the Secured GN Message containing more than one instance of
Summary
                     TrailerField of type 'signature'
Reference
                     ETSI TS 103 097 [1], clause 7.3
PICS Selection
                     PICS_GN_SECURITY
                                                   Expected behaviour
with {
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
   containing header_fields['its_aid']
   indicating 'AID_BEACON'
       and containing trailer_fields
  containing 2 instances of type TrailerField {
            containing type
              indicating 'signature'
  } then {
    the IUT discards the message
```

5.3.4.9 Check signature

| TP Id | TP_SEC_ITSS_RCV_GENMSG_11_01_BO | |
|---------------------------------------|--|--|
| Summary | Check that the IUT discards Secured GN Message containing signature that is not verified using the verification key from the certificate contained in the message's signer info | |
| Reference | ETSI TS 103 097 [1], clause 7.3 | |
| PICS Selection | PICS_GN_SECURITY | |
| | Expected behaviour | |
| with { | · | |
| the IUT being | in the 'authorized' state | |
| } | | |
| ensure that { | | |
| when { | and in the state of the state o | |
| | eceiving a SecuredMessage { header_fields['its_aid'] | |
| _ | neader_fields['lts_aid'] | |
| | ning header_fields ['signer_info'] { | |
| | ng signer { | |
| | ning type | |
| | cating 'certificate' | |
| contai | ning certificate | |
| cont | aining subject_info.subject_type | |
| | dicating 'authorization_ticket' (2) | |
| and | containing subject_attributes['verification key'] (KEY) | |
| } | | |
| } | | |
| | ning payload_field { | |
| containi | ng type ting 'signed' | |
| l | ting signed | |
| and contain | ning trailer_fields { | |
| | containing single instance of type TrailerField { | |
| | ning type | |
| | indicating 'signature' | |
| containing signature | | |
| NOT | verifiable using KEY | |
| } | | |
| } | | |
| } | | |
| } then { | arda the measure | |
| \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ | ards the message | |
| } ' | | |
| נו | | |

5.3.4.10 Check signing certificate type

| TP ld | TP_SEC_ITSS_RCV_GENMSG_12_01_BO |
|---|--|
| Summary | Check that IUT discards a Secured GN Message if the signer certificate of the message contains the subject type "enrolment_credential" |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>} ensure that { when { the IUT is recontaining containing indicate containing indicate and contain } and contain</pre> | eceiving a SecuredMessage header_fields ['signer_info'] { ng signer.type ting 'certificate' ng signer.certificate.subject_info.subject_type ting 'enrolment_credentials' ning header_fields['its_aid'] ng 'AID_BEACON' |
| <pre>} then { the IUT discards the message }</pre> | |

| TP Id | TP_SEC_ITSS_RCV_GENMSG_12_02_BO |
|---|---|
| Summary | Check that IUT discards a Secured GN Message if the signer certificate of the message contains the subject type "authorization_authority" |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>} ensure that { when { the IUT is r containing containini indica containi indica } and contail indicati } then {</pre> | eceiving a SecuredMessage header_fields ['signer_info'] { ng signer.type ting 'certificate' ng signer.certificate.subject_info.subject_type ting 'authorization_authority' ning header_fields['its_aid'] ng 'AID_BEACON' ards the message |

5.3.5 Profiles for certificates

5.3.5.1 Check that certificate version is 2

```
TP Id
                   TP_SEC_ITSS_RCV_CERT_01_01_BO
Summary
                   Check that IUT discards the AT certificate with version 3
Reference
                   ETSI TS 103 097 [1], clauses 6.1 and 7.4
PICS Selection
                  PICS_GN_SECURITY
                                              Expected behaviour
with {
the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
  containing header_fields ['signer_info'] {
         containing signer {
          containing type
             indicating 'certificate'
           containing certificate (CERT_TS_01_01_BO_AT)
             containing version
               indicating '3'
      }
  } then {
    the IUT discards the message
```

| TP ld | TP_SEC_ITSS_RCV_CERT_01_02_BO |
|--|---|
| Summary | Check that IUT discards the AT certificate with version 1 |
| Reference | ETSI TS 103 097 [1], clauses 6.1 and 7.4 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>with { the IUT being in the 'authorized' state } ensure that { when { the IUT is receiving a SecuredMessage { containing header_fields ['signer_info'] { containing signer { containing type indicating 'certificate' containing certificate (CERT_TS_01_02_BO_AT)</pre> | |

```
TP Id
                TP_SEC_ITSS_RCV_CERT_01_03_BO
Summary
                Check that IUT discards the AA certificate with version 3
Reference
                ETSI TS 103 097 [1], clauses 6.1 and 7.4
PICS Selection
                PICS_GN_SECURITY
                                       Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
 containing header_fields ['signer_info'] {
       containing signer {
         containing type
           indicating 'certificate_chain'
         containing certificates[0] (CERT_TS_01_03_BO_AA)
           containing version
             indicating '3'
         containing certificates[1] (CERT_TS_01_03_B0_AT) {
           containing signer_info.type
             indicating 'certificate_digest_with_sha256'
           containing signer_info.digest
             referencing to CERT_TS_01_03_BO_AA
       }
  } then {
   the IUT discards the message
```

| TP ld | TP_SEC_ITSS_RCV_CERT_01_04_BO |
|--|--|
| Summary | Check that IUT discards the AA certificate with version 1 |
| Reference | ETSI TS 103 097 [1], clauses 6.1 and 7.4 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>ensure that { when { the IUT is r containing contai indi contai contai indi contai contai re } } then {</pre> | eceiving a SecuredMessage { header_fields ['signer_info'] { ng signer { ning type cating 'certificate_chain' ning certificates[0] (CERT_TS_01_04_BO_AA) aining version dicating '1' ning certificates[1] (CERT_TS_01_04_BO_AT) { aining signer_info.digest ferencing to CERT_TS_AA_01_04_EB ards the message |

5.3.5.2 Check that enrolment certificate is not used for sign other certificates

Void.

5.3.5.3 Check that any certificate signed with AT certificate is not accepted

Void.

5.3.5.4 Check that AA certificate signed with other AA certificate is not accepted

Void.

5.3.5.5 Check the certificate signature

| TP ld | TP_SEC_ITSS_RCV_CERT_05_01_BO | |
|------------------------------|---|--|
| Summary | Check that IUT discards the message when signing AT certificate has a not valid signature | |
| Reference | ETSI TS 103 097 [1], clauses 6.1 and 7.4 | |
| PICS Selection | PICS_GN_SECURITY | |
| | Expected behaviour | |
| with { | | |
| the IUT being | in the 'authorized' state | |
| } | | |
| ensure that { | | |
| when { | | |
| | eceiving a SecuredMessage { | |
| | <pre>header_fields ['signer_info'] { ng signer {</pre> | |
| | | |
| | <pre>containing type indicating 'certificate'</pre> | |
| | ning certificate (CERT_TS_A_AT) { | |
| | aining signer_info.digest | |
| | referencing to a CERT_TS_A_AA | |
| | containing signature | |
| | NOT verifiable with CERT_TS_A_AA.subject_attributes['verification_key'].key | |
| } | | |
| } | | |
| } | | |
| } | | |
| } then { | | |
| the IUT discards the message | | |
| } | | |
| 1} | | |

| TP ld | TP_SEC_ITSS_RCV_CERT_05_02_BO |
|--|---|
| Summary | Check that IUT discards the message when the issuing AA certificate of the signing AT certificate has a not valid signature |
| Reference | ETSI TS 103 097 [1], clauses 6.1 and 7.4 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| ensure that { when { the IUT is recontaining containing containing containing containing containing containing contain c | eceiving a SecuredMessage { header_fields ['signer_info'] { ng signer { ning type cating 'certificate_chain' ning certificates[0] (CERT_TS_A_AA) { aining signer_info.digest ferencing to a CERT_ROOT aining signature t verifiable with CERT_ROOT.subject_attributes['verification_key'].key ning certificates[1] (CERT_TS_A_AT) { aining signer_info.digest ferencing to a CERT_TS_A_AA |
| } | |
| } then { the IUT disca } | ards the message |

5.3.5.6 Check circular region of subordinate certificate

```
TP Id
                  TP_SEC_ITSS_RCV_CERT_06_01_BV
                  Check that the IUT accepts a message when its signing certificate contains the same circular region
Summary
                  validity restriction as its issuing certificate
Reference
                  ETSI TS 103 097 [1], clause 7.4
PICS Selection
                  PICS_GN_SECURITY, PICS_USE_CIRCULAR_REGION
                                           Expected behaviour
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_06_01_BV_AT) {
            containing validity_restrictions['region'] {
              containing region_type
                indicating 'circle'
              containing circular_region
                 indicating CURCULAR_REGION_AA
            containing signer_info.digest
              referencing to a CERT_TS_B_AA
      }
  } then {
    the IUT accepts the message
```

| Reference E | Check that the IUT accepts a message when its signing certificate contains the validity restriction with circular region which is fully inside in the validity region of its issuing certificate |
|--|---|
| | |
| | TSI TS 103 097 [1], clause 7.4 |
| PICS Selection PI | PICS_GN_SECURITY, PICS_USE_CIRCULAR_REGION |
| | Expected behaviour |
| ensure that { when { the IUT is reconstanting to containing } containing conta | Ing type ating 'certificate' Ing certificate (CERT_TS_06_02_BV_AT) { Ing certificate |

```
TP Id
                   TP_SEC_ITSS_RCV_CERT_06_03_BO
                   Check that the IUT discards a message when its signing certificate does not contain the validity
Summary
                   restriction of type 'region' but its issuing certificate contains the circular region validity restriction
Reference
                   ETSI TS 103 097 [1], clause 7.4
                   PICS_GN_SECURITY, PICS_USE_CIRCULAR_REGION
PICS Selection
                                               Expected behaviour
with {
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
   containing header_fields ['signer_info'] {
         {\tt containing \ signer}\ \{
           containing type
             indicating 'certificate'
           containing certificate (CERT_TS_06_03_BO_AT) {
             not containing validity_restrictions['region']
             and containing signer_info.digest
               referencing to a CERT_TS_B_AA
         }
      }
  } then {
    the IUT discards the message
```

| TP ld | TP_SEC_ITSS_RCV_CERT_06_04_BO | |
|---------------------------------------|---|--|
| Summary | Check that the IUT discards a message when the circular validity region of the signing certificate is outside of the validity region of the issuing certificate | |
| Reference | ETSI TS 103 097 [1], clause 7.4 | |
| PICS Selection | PICS_GN_SECURITY, PICS_USE_CIRCULAR_REGION | |
| | Expected behaviour | |
| with { | | |
| the IUT being | in the 'authorized' state | |
| } | | |
| ensure that { when { | | |
| | eceiving a SecuredMessage { | |
| | header_fields ['signer_info'] { | |
| | ng signer { | |
| contai | ning type | |
| | cating 'certificate' | |
| | ning certificate (CERT_TS_06_04_BO_AT) { | |
| | aining validity_restrictions['region'] { | |
| | containing region_type | |
| | indicating 'circle' ntaining circular_region | |
| | indicating CURCULAR_REGION_AT | |
| } | | |
| cont | aining signer_info.digest | |
| re | ferencing to a CERT_TS_06_04_B0_AA | |
| | containing validity_restrictions['region'] { | |
| | containing region_type | |
| | indicating 'circle' | |
| | containing circular_region | |
| indicating CURCULAR_REGION_AA_OUTSIDE | | |
| } | J | |
| } ' | | |
| } | | |
| } | | |
| } then { | | |
| the IUT disc | ards the message | |
| } | | |
| J | | |

```
TP Id TP_SEC_ITSS_RCV_CERT_06_05_BO

Summary Check that the IUT discards a message when the circular validity region of the signing certificate is not fully covered by the validity region of the issuing certificate

Reference ETSI TS 103 097 [1], clause 7.4

PICS Selection PICS_GN_SECURITY, PICS_USE_CIRCULAR_REGION

Expected behaviour
```

```
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage {
     containing header_fields ['signer_info'] {
       containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_06_05_BO_AT) {
            containing validity_restrictions['region'] {
                containing region_type
                  indicating 'circle'
                containing circular_region
                  indicating CURCULAR_REGION_AT
            containing signer_info.digest
              referencing to a CERT_TS_06_05_BO_AA
                containing validity_restrictions['region'] {
                  containing region_type
                    indicating 'circle'
                  containing circular_region
                    indicating CURCULAR_REGION_AA_INTERSECT
     }
  } then {
   the IUT discards the message
  }
```

5.3.5.7 Check rectangular region of subordinate certificate

```
TP Id
                 TP_SEC_ITSS_RCV_CERT_07_01_BV
                 Check that the IUT accepts a message when its signing certificate contains the same validity
Summary
                 restriction with rectangular regions as its issuing certificate
Reference
                 ETSI TS 103 097 [1], clause 7.4
PICS Selection
                 PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION
                                           Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
 when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_07_01_BV_AT) {
            containing validity_restrictions['region'] {
              containing region_type
                indicating 'rectangle'
              containing rectangular_region[0]
                indicating RECT_REGION_AA
            containing signer_info.digest
              referencing to a CERT_TS_C_AA
  } then {
    the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_07_02_BV |
|--|---|
| Summary | Check that the IUT accepts a message when its signing certificate contains the rectangular validity region which is fully inside of the validity region of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4 |
| PICS Selection | PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION |
| | Expected behaviour |
| ensure that { when { the IUT is recontaining containing cont | eceiving a SecuredMessage { header_fields ['signer_info'] { ng signer { ning type cating 'certificate' ning certificate (CERT_TS_AT_07_02_NB) { aining validity_restrictions['region'] { ntaining region_type indicating 'rectangle' ntaining rectangular_region[0] indicating RECT_REGION_TS_AT aining signer_info.digest ferencing to a CERT_TS_AA_C |
| } } } | |
| } then { the IUT accep | pts the message |
| } | |

```
TP Id
                  TP_SEC_ITSS_RCV_CERT_07_03_BO
                  Check that the IUT discards a message when the signing certificate does not contain a region
Summary
                  validity restriction but its issuing certificate contains the rectangular region validity restriction
Reference
                  ETSI TS 103 097 [1], clause 7.4
PICS Selection
                  PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION
                                           Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_07_03_BO_AT) {
            not containing validity_restrictions['region']
            containing signer_info.digest
              referencing to a CERT_TS_C_AA
        }
      }
  } then {
    the IUT discards the message
```

```
TP Id
                  TP_SEC_ITSS_RCV_CERT_07_04_BO
                  Check that the IUT discards a message when the rectangular validity region of the message signing
Summary
                 certificate is outside of the validity region of its issuing certificate
Reference
                  ETSI TS 103 097 [1], clause 7.4
PICS Selection
                 PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION
                                           Expected behaviour
 the IUT being in the 'authorized' state
ensure that \{
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_07_04_BO_AT)
            containing validity_restrictions['region'] {
              containing region_type
                indicating 'rectangle'
              containing rectangular_region[0]
                indicating RECT_REGION_AT
            containing signer_info.digest
              referencing to a CERT_TS_07_04_BO_AA
                containing validity_restrictions['region'] {
                   containing region_type
                     indicating 'rectangle'
                   containing rectangular_region[0]
                     indicating RECT_REGION_AA_OUTSIDE
      }
    }
  } then {
    the IUT discards the message
```

```
TP Id TP_SEC_ITSS_RCV_CERT_07_05_BO

Summary Check that the IUT discards a message when the rectangular validity region of the message signing certificate is not fully covered by the validity region of the issuing certificate

Reference ETSI TS 103 097 [1], clause 7.4

PICS Selection PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION

Expected behaviour

with {
    the IUT being in the 'authorized' state
```

```
ensure that {
 when {
   the IUT is receiving a SecuredMessage {
     containing header_fields ['signer_info'] {
       containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_07_05_BO_AT) {
            containing validity_restrictions['region'] {
                containing region_type
                  indicating 'rectangle'
                containing rectangular_region[0]
                  indicating RECT_REGION_AT
            containing signer_info.digest
              referencing to a CERT_TS_07_05_BO_AA
                containing validity_restrictions['region'] {
                  containing region_type
                    indicating 'rectangle'
                  containing rectangular_region[0]
                    indicating RECT_REGION_AA_INTERSECT
     }
  } then {
   the IUT discards the message
  }
```

5.3.5.8 Check polygonal region of subordinate certificate

| TP ld | TP_SEC_ITSS_RCV_CERT_08_01_BV |
|---|---|
| Summary | Check that the IUT accepts a message when its signing certificate contains the same polygonal region validity restriction as its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4 |
| PICS Selection | PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION |
| | Expected behaviour |
| ensure that { when { | in the 'authorized' state eceiving a SecuredMessage { |
| containing | header_fields ['signer_info'] { ng signer { ning type cating 'certificate' ning certificate (CERT_TS_08_01_BV_AT) { aining validity_restrictions['region'] { ntaining region_type indicating 'polygon' ntaining polygonal_region indicating POLYGON_REGION_AA aining signer_info.digest ferencing to a CERT_TS_D_AA |

| TP ld | TP_SEC_ITSS_RCV_CERT_08_02_BV |
|--|---|
| Summary | Check that the IUT accepts a message when its signing certificate contains the validity restriction with the polygonal region which is fully inside in the validity region of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4 |
| PICS Selection | PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION |
| | Expected behaviour |
| ensure that { when { the IUT is recontaining containing cont | eceiving a SecuredMessage { header_fields ['signer_info'] { ng signer { ning type cating 'certificate' ning certificate (CERT_TS_08_02_BV_AT) { aining validity_restrictions['region'] { |
| } then { | |
| <pre>the IUT accepts the message } </pre> | |

```
TP Id
                   TP_SEC_ITSS_RCV_CERT_08_03_BO
                   Check that the IUT discards a message when its signing certificate does not contain a region validity
Summary
                   restriction but its issuing certificate contains the polygonal region validity restriction
Reference
                   ETSI TS 103 097 [1], clause 7.4
                   PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION
PICS Selection
                                              Expected behaviour
with {
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
   containing header_fields ['signer_info'] {
         {\tt containing \ signer}\ \{
           containing type
             indicating 'certificate'
           containing certificate (CERT_TS_08_03_BO_AT) {
             not containing validity_restrictions['region']
             containing signer_info.digest
               referencing to a CERT_TS_D_AA
         }
      }
  } then {
    the IUT discards the message
```

| | TD 050 1700 DOV 05DT 00 04 DO | |
|----------------------------|--|--|
| TP ld | TP_SEC_ITSS_RCV_CERT_08_04_BO | |
| Summary | Check that the IUT discards a message when signing certificate contains a polygonal region validity | |
| - Cammury | restriction containing less than 3 points | |
| Reference | ETSI TS 103 097 [1], clauses 4.2.24 and 7.4 | |
| PICS Selection | PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION | |
| | Expected behaviour | |
| with { | | |
| the IUT being | in the 'authorized' state | |
| <pre>} ensure that {</pre> | | |
| when { | | |
| | eceiving a SecuredMessage { | |
| | header_fields ['signer_info'] { | |
| | ng signer { | |
| | ning type | |
| | cating 'certificate' | |
| | <pre>containing certificate (CERT_TS_08_04_BO_AT) { containing validity_restrictions['region'] {</pre> | |
| | ntaining region_type | |
| | indicating 'polygon' | |
| | ntaining polygonal region | |
| | containing length | |
| | indicating 2 | |
| } | | |
| | aining signer_info.digest | |
| re | ferencing to a CERT_TS_D_AA | |
| } | | |
| } | | |
| } | | |
| } then { | | |
| , | ards the message | |
| } | - | |
| } | | |
| | | |

```
TP Id TP_SEC_ITSS_RCV_CERT_08_05_BO

Summary Check that the IUT discards a message when the polygonal region validity restriction of the message signing certificate is outside of the validity region of the issuing certificate

Reference ETSI TS 103 097 [1], clause 7.4

PICS Selection PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION

Expected behaviour
```

```
Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage {
     containing header_fields ['signer_info'] {
       containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_08_05_BO_AT) {
            containing validity_restrictions['region'] {
              containing region_type
                indicating 'polygon'
              containing polygonal_region
                indicating POLYGON_REGION_AT
            containing signer_info.digest
              referencing to a CERT_TS_08_05_BO_AA
                containing validity_restrictions['region'] {
                  containing region_type
                    indicating 'polygon'
                  containing polygonal_region
                    indicating POLYGON_REGION_AA_OUTSIDE
     }
  } then {
   the IUT discards the message
  }
```

```
TP Id TP_SEC_ITSS_RCV_CERT_08_06_BO

Summary Check that the IUT discards a message when the polygonal validity region of the message signing certificate is not fully covered by the validity region of its issuing certificate

Reference ETSI TS 103 097 [1], clause 7.4

PICS Selection PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION

Expected behaviour
```

```
the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage {
     containing header_fields ['signer_info'] {
       containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_08_06_BO_AT) {
            containing validity_restrictions['region'] {
              containing region_type
                indicating 'polygon'
              containing polygonal_region
                indicating POLYGON_REGION_AT
            containing signer_info.digest
              referencing to a CERT_TS_08_06_BO_AA
                containing validity_restrictions['region'] {
                  containing region_type
                    indicating 'polygon'
                  containing polygonal_region
                    indicating POLYGON_REGION_AA_INTERSECT
     }
  } then {
   the IUT discards the message
  }
```

5.3.5.9 Check identified region of subordinate certificate

} then {
 the IUT accepts the message

| TP Id | TP_SEC_ITSS_RCV_CERT_09_01_BV |
|---|---|
| | Check that the IUT accepts a message when its signing certificate contains the region validity restriction with the same identified region as the issuing certificate and without local area definition |
| Reference | ETSI TS 103 097 [1], clauses 4.2.26 and 7.4 |
| PICS Selection | PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION |
| | Expected behaviour |
| } ensure that { when { the IUT is recontaining containir contairindic | in the 'authorized' state eceiving a SecuredMessage { header_fields ['signer_info'] { ng signer { ning type conting 'certificate' respectively (CRDET TO 00 01 DV NT) { |
| <pre>containing certificate (CERT_TS_09_01_BV_AT) { containing validity_restrictions['region'] { containing region_type indicating 'id' containing id_region { containing region_dictionary indicating 'iso_3166_1' (0) containing region_identifier indicating ID_REGION_AT containing local_region indicating 0 } } containing signer_info.digest referencing to a CERT_AA_E_TS } }</pre> | |

```
TP Id

TP_SEC_ITSS_RCV_CERT_09_02_BV

Check that the IUT accepts a message when its signing certificate contains the identified region validity restriction with the same identified region as in the issuing certificate but with the local area definition

Reference

ETSI TS 103 097 [1], clauses 4.2.26 and 7.4

PICS Selection

PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION

Expected behaviour

with {
the IUT being in the 'authorized' state
```

```
ensure that {
 when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
       containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_09_01_BV_AT) {
           containing validity_restrictions['region'] {
              containing region_type
                indicating 'id'
              containing id_region {
               containing region_dictionary
                  indicating 'iso_3166_1' (0)
                containing region_identifier
                  indicating ID_REGION_AT
                containing local_region
                  indicating 1
            containing signer_info.digest
              referencing to a CERT_TS_E_AA
       }
   then {
   the IUT accepts the message
```

```
TP Id TP_SEC_ITSS_RCV_CERT_09_03_BV

Check that the IUT accepts a message when its signing certificate contains the region validity restriction with the identified region which is fully covered by the identified validity region of the issuing certificate

Reference ETSI TS 103 097 [1], clauses 4.2.26 and 7.4

PICS Selection PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION

Expected behaviour
```

```
Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_09_03_BV_AT) {
            containing validity_restrictions['region'] {
              containing region_type
                indicating 'id'
              containing id_region {
                containing region_dictionary
                  indicating 'un_stats' (1)
                containing region_identifier
                  indicating ID_REGION_AT
                containing local_region
                  indicating 0
            }
            containing signer_info.digest
              referencing to a CERT_TS_09_03_BV_AA
                containing validity_restrictions['region'] {
                  containing region_type
                    indicating 'id'
                  containing id_region {
                    containing region_dictionary
                      indicating 'un_stats' (1)
                    containing region_identifier
                      indicating ID_REGION_AA_UNSTATS
                    containing local_region
                      indicating 0
                }
          }
       }
     }
  } then {
   the IUT accepts the message
```

```
TP Id
                   TP_SEC_ITSS_RCV_CERT_09_04_BO
                   Check that the IUT discards a message when signing certificate does not contain a region validity
Summary
                   restriction but the issuing certificate contains the identified region validity restriction
Reference
                   ETSI TS 103 097 [1], clauses 4.2.26 and 7.4
                   PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION
PICS Selection
                                               Expected behaviour
with {
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
   containing header_fields ['signer_info'] {
         {\tt containing \ signer}\ \{
           containing type
             indicating 'certificate'
           containing certificate (CERT_TS_09_04_BO_AT) {
             not containing validity_restrictions['region']
             containing signer_info.digest
                referencing to a CERT_TS_E_AA
         }
      }
  } then {
    the IUT discards the message
```

```
TP Id TP_SEC_ITSS_RCV_CERT_09_05_BO

Summary Check that the IUT discards a message when the identified region of the validity restriction of the signing certificate is different from the one in the issuing certificate

Reference ETSI TS 103 097 [1], clauses 4.2.26 and 7.4

PICS Selection PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION

Expected behaviour
```

```
Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT TS 09 05 BO AT) {
            containing validity_restrictions['region'] {
              containing region_type
                indicating 'id'
              containing id_region {
                containing region_dictionary
                  indicating 'iso_3166_1' (0)
                containing region_identifier
                 indicating ID_REGION_AT
                containing local_region
                  indicating 0
            containing signer_info.digest
              referencing to a CERT_TS_09_05_BO_AA
                containing validity_restrictions['region'] {
                  containing region_type
                    indicating 'id'
                  containing id_region {
                    containing region_dictionary
                      indicating 'iso_3166_1' (0)
                    containing region_identifier
                      indicating ID_REGION_AA_OTHER
                    containing local_region
                      indicating 0
               }
         }
       }
     }
  } then {
   the IUT discards the message
```

```
the IUT is receiving a SecuredMessage {
   containing header_fields ['signer_info'] {
     containing signer {
       containing type
          indicating 'certificate'
        containing certificate (CERT_TS_09_06_BO_AT) {
         containing validity_restrictions['region'] {
            containing region_type
              indicating 'id'
            containing id_region {
              containing region_dictionary
                indicating 'iso_3166_1' (0)
              containing region_identifier
                indicating ID_REGION_AA
              containing local_region
                indicating 1
          }
          containing signer_info.digest
            referencing to a CERT_TS_09_06_BO_AA
              containing validity_restrictions['region'] {
                containing region_type
                  indicating 'id'
                containing id_region {
                  containing region_dictionary
                    indicating 'iso_3166_1' (0)
                  containing region_identifier
                    indicating ID_REGION_AA
                  containing local_region
                    indicating 2
              }
       }
     }
   }
} then {
 the IUT discards the message
```

```
TP Id TP_SEC_ITSS_RCV_CERT_09_07_BO

Summary Check that the IUT discards a message when the identified region validity restriction of the signing certificate contains unknown area code

Reference ETSI TS 103 097 [1], clauses 4.2.26 and 7.4

PICS Selection PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION

Expected behaviour
```

```
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
   the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_09_07_B0_AT) {
            containing validity_restrictions['region'] {
              containing region_type
                indicating 'id'
              containing id_region {
                containing region_dictionary
                  indicating 'iso_3166_1' (0)
                containing region_identifier
                 indicating ID_REGION_UNKNOWN
                containing local_region
                  indicating 0
            containing signer_info.digest
              referencing to a CERT_TS_09_07_BO_AA
                containing validity_restrictions['region'] {
                  containing region_type
                    indicating 'id'
                  containing id_region {
                    containing region_dictionary
                      indicating 'iso_3166_1' (0)
                    containing region_identifier
                      indicating ID_REGION_UNKNOWN
                    containing local_region
                      indicating 0
               }
         }
       }
     }
  } then {
   the IUT discards the message
```

5.3.5.10 Check time validity restriction presence

| TP Id | TP_SEC_ITSS_RCV_CERT_10_01_BO |
|--|--|
| Summary | Check that the IUT discards a message when its signing certificate does not contain the time validity restriction |
| Reference | ETSI TS 103 097 [1], clauses 7.4 and 7.4.1 |
| PICS Selection | PICS_GN_SECURITY |
| | Expected behaviour |
| <pre>} ensure that { when { the IUT is recontaining containing contail indiction contail contail indiction contail contail</pre> | eceiving a SecuredMessage { header_fields ['signer_info'] { ng signer { ning type cating 'certificate' ning certificate (CERT_TS_10_01_BO_AT) containing validity_restrictions['time_start_and_end'] ards the message |

| TP ld | TP_SEC_ITSS_RCV_CERT_10_02_BO | | | | |
|---|---|--|--|--|--|
| Summary | Check that the IUT discards a message when its signing certificate contains 'time_end' validity restriction | | | | |
| Reference | ETSI TS 103 097 [1], clauses 7.4 and 7.4.1 | | | | |
| PICS Selection | PICS_GN_SECURITY | | | | |
| | Expected behaviour | | | | |
| <pre>with { the IUT being in the 'authorized' state } ensure that { when { the IUT is receiving a SecuredMessage { containing header_fields ['signer_info'] { containing signer { containing type</pre> | | | | | |

```
TP Id
                   TP_SEC_ITSS_RCV_CERT_10_03_BO
                   Check that the IUT discards a message when its signing certificate contains
Summary
                   'time_start_and_duration' validity restriction
Reference
                   ETSI TS 103 097 [1], clauses 7.4 and 7.4.1
PICS Selection
                   PICS_GN_SECURITY
                                               Expected behaviour
with {
  the IUT being in the 'authorized' state
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
   containing header_fields ['signer_info'] {
         {\tt containing \ signer}\ \{
           containing type
             indicating 'certificate'
           containing certificate (CERT_TS_10_03_BO_AT) {
             containing validity_restrictions['time_start_and_duration']
      }
  } then {
    the IUT discards the message
```

5.3.5.11 Check time validity restriction conforming to the issuing certificate

| TP ld | TP_SEC_ITSS_RCV_CERT_11_01_BO | | | |
|---|--|--|--|--|
| Summary | Check that the IUT discards a message when the validity period of the signing certificate ends after the period of its issuing certificate | | | |
| Reference | ETSI TS 103 097 [1], clause 7.4 | | | |
| PICS Selection | PICS_GN_SECURITY | | | |
| | Expected behaviour | | | |
| <pre>with { the IUT being in the 'authorized' state } ensure that { when { the IUT is receiving a SecuredMessage { containing header_fields ['signer_info'].signer.certificate (CERT_TS_11_01_BO_AT) containing signer_info.digest referencing to CERT_TS_A_AA containing validity_restrictions['time_start_and_end'] { containing start_validity</pre> | | | | |

```
TP Id
                 TP_SEC_ITSS_RCV_CERT_11_02_BO
                 Check that the IUT discards a message when its signing certificate starts before its issuing
Summary
                 certificate
Reference
                 ETSI TS 103 097 [1], clause 7.4
                 PICS_GN_SECURITY
PICS Selection
                                          Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'].signer.certificate (CERT_TS_11_02_BO_AT)
        containing signer_info.digest
          referencing to CERT_TS_A_AA
            containing validity_restrictions['time_start_and_end'] {
              containing start_validity
                indicating START_VALIDITY_AA
              containing end_validity
                indicating END_VALIDITY_AA
        containing validity_restrictions['time_start_and_end'] {
          containing start_validity
            indicating START_VALIDITY_AA - 1d
          containing end_validity
            indicating END_VALIDITY_AA
     }
  } then {
    the IUT discards the message
```

| TP ld | TP_SEC_ITSS_RCV_CERT_11_03_BO | | |
|---|--|--|--|
| Summary | Check that the IUT discards a message when the issuing certificate of signing certificate is expired | | |
| Reference | ETSI TS 103 097 [1], clause 7.4 | | |
| PICS Selection | PICS_GN_SECURITY | | |
| | Expected behaviour | | |
| <pre>ensure that { when { the IUT is r containing containin refered containin containin</pre> | eceiving a SecuredMessage { header_fields ['signer_info'].signer.certificate (CERT_TS_11_03_BO_AT) ng signer_info.digest ncing to CERT_TS_11_03_BO_AA aining validity_restrictions['time_start_and_end'] { ntaining start_validity indicating START_VALIDITY_AA - 365d ntaining end_validity indicating START_VALIDITY_AA - 1d ng validity_restrictions['time_start_and_end'] { ning start_validity cating START_VALIDITY_AA - 365d ning start_validity cating START_VALIDITY_AA - 365d ning end_validity cating END_VALIDITY_AA ards the message | | |

```
TP Id
                 TP_SEC_ITSS_RCV_CERT_11_04_BO
                 Check that the IUT discards a message when the validity period of the issuing certificate of signing
Summary
                 certificate is not started yet
Reference
                 ETSI TS 103 097 [1], clause 7.4
                 PICS_GN_SECURITY
PICS Selection
                                          Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'].signer.certificate (CERT_TS_11_04_BO_AT)
        containing signer_info.digest
          referencing to CERT_TS_11_04_BO_AA
            containing validity_restrictions['time_start_and_end'] {
              containing start_validity
                indicating END_VALIDITY_AA
              containing end_validity
                indicating END_VALIDITY_AA + 365d
        containing validity_restrictions['time_start_and_end'] {
          containing start_validity
            indicating START_VALIDITY_AA
          containing end_validity
            indicating END_VALIDITY_AA +365d
      }
  } then {
    the IUT discards the message
```

5.3.5.12 Check AID subject attribute presence

| TP ld | TP_SEC_ITSS_RCV_CERT_12_01_BO | | | |
|------------------------|---|--|--|--|
| Summary | Check that the IUT discards a message when its signing certificate does not contain the SSP-AID | | | |
| | subject attribute | | | |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 | | | |
| PICS Selection | PICS_GN_SECURITY | | | |
| | Expected behaviour | | | |
| with { | | | | |
| the IUT being | in the 'authorized' state | | | |
| } | | | | |
| ensure that { when { | | | | |
| | eceiving a SecuredMessage { | | | |
| | header_fields ['signer_info'] { | | | |
| _ | ng signer { | | | |
| | ning type | | | |
| | cating 'certificate' | | | |
| contai | ning certificate (CERT_TS_12_01_BO_AT) | | | |
| not | containing subject_attributes['its_aid_ssp_list'] | | | |
| } | | | | |
| } | | | | |
| } | | | | |
| } then { | | | | |
| the IUT disc | the IUT discards the message | | | |
| } | | | | |
| } | | | | |

```
TP Id
                 TP_SEC_ITSS_RCV_CERT_12_02_BO
                 Check that the IUT discards a Secured CAM when its signing certificate does not contain a record
Summary
                 with AID_CAM in the its_aid_ssp_list subject attribute
Reference
                 ETSI TS 103 097 [1], clause 7.4.1
                 PICS_GN_SECURITY
PICS Selection
                                          Expected behaviour
with {
 the IUT being in the 'authorized' state
ensure that {
 when {
    the IUT is receiving a Secured CAM {
      containing header_fields ['its_aid'] {
        containing its_aid
          indicating 'AID_CAM' (16512)
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_12_02_BO_AT) {
            containing subject_attributes['its_aid_ssp_list']
              not containing an item
                containing its_aid
                  indicating 'AID_CAM' (16512)
        }
      }
  } then {
    the IUT discards the message
```

| Check that the IUT discards a Secured DENM when its signing certificate does not contain a reconverted with AID_DENM in the its_aid_ssp_list subject attribute Reference | | | | |
|---|-----------------|---|--|--|
| with AID_DENM in the its_aid_ssp_list subject attribute Reference | TP Id | TP_SEC_ITSS_RCV_CERT_12_03_BO | | |
| Reference ETSLTS 103 097 [1], clause 7.4.1 PICS Selection PICS_GN_SECURITY Expected behaviour with { the IUT being in the 'authorized' state } ensure that { when { the IUT is receiving a Secured DENM { containing its_aid indicating 'AID_DENM' (16513) containing signer { containing type indicating 'certificate' containing certificate (CERT_TS_12_03_BO_AT) { containing subject_attributes['its_aid_ssp_list'] not containing an item containing its_aid indicating 'AID_DENM' (16513) recontaining subject_attributes['its_aid_ssp_list'] | Summary | Check that the IUT discards a Secured DENM when its signing certificate does not contain a record | | |
| Expected behaviour with { the IUT being in the 'authorized' state } ensure that { when { the IUT is receiving a Secured DENM { containing header_fields ['its_aid'] { containing its_aid indicating 'AID_DENM' (16513) containing signer { containing signer { containing certificate' containing retrificate (CERT_TS_12_03_B0_AT) { containing subject_attributes['its_aid_ssp_list'] not containing an item containing its_aid indicating 'AID_DENM' (16513) | Outilinal y | with AID_DENM in the its_aid_ssp_list subject attribute | | |
| <pre>interest</pre> | Reference | ETSI TS 103 097 [1], clause 7.4.1 | | |
| with { the IUT being in the 'authorized' state } ensure that { when { the IUT is receiving a Secured DENM { containing header_fields ['its_aid'] { containing its_aid | PICS Selection | PICS_GN_SECURITY | | |
| <pre>the IUT being in the 'authorized' state } ensure that { when { the IUT is receiving a Secured DENM { containing header_fields ['its_aid'] { containing its_aid indicating 'AID_DENM' (16513) containing header_fields ['signer_info'] { containing signer { containing type indicating 'certificate' containing certificate (CERT_TS_12_03_BO_AT) { containing subject_attributes['its_aid_ssp_list'] not containing an item</pre> | | Expected behaviour | | |
| <pre>Pensure that { when { the IUT is receiving a Secured DENM { containing header_fields ['its_aid'] { containing its_aid indicating 'AID_DENM' (16513) containing header_fields ['signer_info'] { containing signer { containing type indicating 'certificate' containing certificate (CERT_TS_12_03_BO_AT) { containing subject_attributes['its_aid_ssp_list']</pre> | with { | | | |
| <pre>when { the IUT is receiving a Secured DENM { containing header_fields ['its_aid'] { containing its_aid indicating 'AID_DENM' (16513) containing header_fields ['signer_info'] { containing signer { containing type indicating 'certificate' containing certificate (CERT_TS_12_03_BO_AT) { containing subject_attributes['its_aid_ssp_list'] not containing an item containing its_aid indicating 'AID_DENM' (16513) } } } } then {</pre> | the IUT being : | in the 'authorized' state | | |
| <pre>when { the IUT is receiving a Secured DENM { containing header_fields ['its_aid'] { containing its_aid indicating 'AID_DENM' (16513) containing header_fields ['signer_info'] { containing signer { containing type indicating 'certificate' containing certificate (CERT_TS_12_03_BO_AT) { containing subject_attributes['its_aid_ssp_list'] not containing an item containing its_aid indicating 'AID_DENM' (16513) } } } } then {</pre> | } | | | |
| <pre>the IUT is receiving a Secured DENM { containing header_fields ['its_aid'] { containing its_aid indicating 'AID_DENM' (16513) containing header_fields ['signer_info'] { containing signer { containing type indicating 'certificate' containing certificate (CERT_TS_12_03_BO_AT) { containing subject_attributes['its_aid_ssp_list'] not containing an item containing its_aid indicating 'AID_DENM' (16513) } } } } then {</pre> | , | | | |
| <pre>containing header_fields ['its_aid'] { containing its_aid indicating 'AID_DENM' (16513) containing header_fields ['signer_info'] { containing signer { containing type indicating 'certificate' containing certificate (CERT_TS_12_03_BO_AT) { containing subject_attributes['its_aid_ssp_list'] not containing an item containing its_aid</pre> | | ogaining a Cogured DENM | | |
| <pre>containing its_aid indicating 'AID_DENM' (16513) containing header_fields ['signer_info'] { containing signer { containing type indicating 'certificate' containing certificate (CERT_TS_12_03_BO_AT) { containing subject_attributes['its_aid_ssp_list'] not containing an item containing its_aid indicating 'AID_DENM' (16513) } } then {</pre> | | · · · · · · · · · · · · · · · · · · · | | |
| <pre>indicating 'AID_DENM' (16513) containing header_fields ['signer_info'] { containing signer { containing type indicating 'certificate' containing certificate (CERT_TS_12_03_BO_AT) { containing subject_attributes['its_aid_ssp_list'] not containing an item containing its_aid indicating 'AID_DENM' (16513) } } } then {</pre> | | | | |
| <pre>containing header_fields ['signer_info'] { containing signer { containing type indicating 'certificate' containing certificate (CERT_TS_12_03_BO_AT) { containing subject_attributes['its_aid_ssp_list'] not containing an item containing its_aid indicating 'AID_DENM' (16513) } } } then {</pre> | | | | |
| <pre>containing type indicating 'certificate' containing certificate (CERT_TS_12_03_BO_AT) { containing subject_attributes['its_aid_ssp_list'] not containing an item</pre> | | | | |
| <pre>indicating 'certificate' containing certificate (CERT_TS_12_03_BO_AT) { containing subject_attributes['its_aid_ssp_list'] not containing an item containing its_aid indicating 'AID_DENM' (16513) } } then {</pre> | containin | ng signer { | | |
| <pre>containing certificate (CERT_TS_12_03_BO_AT) { containing subject_attributes['its_aid_ssp_list'] not containing an item containing its_aid indicating 'AID_DENM' (16513) } } then {</pre> | contain | ning type | | |
| <pre>containing subject_attributes['its_aid_ssp_list'] not containing an item</pre> | | | | |
| <pre>not containing an item</pre> | | | | |
| <pre>containing its_aid</pre> | | | | |
| indicating 'AID_DENM' (16513) } } then { | | - | | |
| } } then { | | 9 = | | |
| | 1 | indicating 'AID_DENM' (16513) | | |
| | } | | | |
| | 1 | | | |
| | } | | | |
| | } then { | | | |
| } | | | | |
| | } | | | |
| } | } | | | |

5.3.5.13 Check AID-SSP subject attribute value conforming to the issuing certificate

```
TP Id
                 TP_SEC_ITSS_RCV_CERT_13_01_BO
                 Check that the IUT discards a message when the signing AT certificate contains a CAM AID-SSP
Summary
                 record whereas the issuing AA certificate does not contain the record with AID_CAM
Reference
                 ETSI TS 103 097 [1], clause 7.4.1
PICS Selection
                 PICS_GN_SECURITY
                                          Expected behaviour
 the IUT being in the 'authorized' state
ensure that {
 when {
    the IUT is receiving a Secured CAM {
      containing header_fields ['signer_info'].signer.certificate (CERT_TS_13_01_BO_AT) {
        containing signer_info.digest
          referencing to CERT_TS_13_01_BO_AA
            containing subject_attributes['its_aid_list']
              not containing AID_CAM
        containing subject_attributes['its_aid_ssp_list']
          containing a record
            containing its_aid
              indicating AID_CAM
      }
  } then {
    the IUT discards the message
```

| TP ld | TP_SEC_ITSS_RCV_CERT_13_02_BO | | | | |
|--|--|--|--|--|--|
| Summary | Check that the IUT discards a message when the signing AT certificate contains a DENM AID-SS record whereas the issuing AA certificate does not contain the record with AID_DENM | | | | |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 | | | | |
| PICS Selection | PICS_GN_SECURITY | | | | |
| | Expected behaviour | | | | |
| ensure that { when { the IUT is notaining containing c | in the 'authorized' state receiving a Secured DENM { g header_fields ['signer_info'].signer.certificate (CERT_TS_13_02_B0_AT) { Ing signer_info.digest encing to CERT_TS_13_02_B0_AA raining subject_attributes['its_aid_list'] but containing AID_DENM Ing subject_attributes['its_aid_ssp_list'] Ining a record raining its_aid indicating AID_DENM | | | | |
| } then { the IUT disc } } | cards the message | | | | |

Annex A (informative): Bibliography

• ETSI TS 102 894-2 (V1.2.1): "Intelligent Transport Systems (ITS); Users and applications requirements; Part 2: Applications and facilities layer common data dictionary".

History

| Document history | | | | | | |
|------------------|----------------|-------------|--|--|--|--|
| V1.1.1 | July 2013 | Publication | | | | |
| V1.2.1 | September 2015 | Publication | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |