# ETSI TS 103 096-2 V1.3.1 (2017-03)


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

Reference
RTS/ITS-00535

Keywords
ITS, security, testing, TSS&TP

***ETSI***

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

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

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

***Important notice***

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

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

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

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

***Copyright Notification***

# Contents

# Intellectual Property Rights

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

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

# Foreword

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

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

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

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

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

# Modal verbs terminology

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

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

# 1 Scope

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

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

# 2 References

## 2.1 Normative references

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

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

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

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

[1] ETSI TS 103 097 (V1.2.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".

[2] ETSI TS 103 096-1 (V1.3.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)".

[3] ETSI TS 102 871-1 (V1.3.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma".

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

[5] United Nations, Statistics Division (1996): "Standard Country or Area Codes for Statistical Use (Rev. 3), Series M: Miscellaneous Statistical Papers, No. 49", New York: United Nations.

## 2.2 Informative references

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

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

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

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

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

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

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

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

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

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

# 3 Definitions and abbreviations

## 3.1 Definitions

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

## 3.2 Abbreviations

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

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

# 4 Test Suite Structure (TSS)

## 4.1 Structure for Security tests

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

**Table 1: TSS for Security**

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

# 5 Test Purposes (TP)

## 5.1 Introduction

### 5.1.1 TP definition conventions

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

### 5.1.2 TP Identifier naming conventions

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

**Table 2: TP naming convention**

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

### 5.1.3 Rules for the behaviour description

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

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

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

### 5.1.4 Sources of TP definitions

All TPs have been specified according to ETSI TS 103 097 [1].

### 5.1.5 Mnemonics for PICS reference

To avoid an update of all TPs when the PICS document is changed, table 3 introduces mnemonics name and the correspondence with the real PICS item number. The 'PICS item' column refers to tables and items of ETSI TS 103 096-1 [2] if not stated otherwise. The 'PICS item' as defined in ETSI TS 103 096-1 [2] and ETSI TS 102 871-1 [3] shall be used to determine the test applicability.

**Table 3: Mnemonics for PICS reference**

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

# 5 ITS-S Security

## 5.1 Overview

Void.

## 5.2 Sending behaviour

### 5.2.1 Check the message protocol version

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

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

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

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

### 5.2.3 Check Signature ECC point type

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

### 5.2.4 CAM profile

#### 5.2.4.1 Check secured CAM its_aid value

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

### 5.2.4.2 Check header fields

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

### 5.2.4.3 Check that IUT sends digest as sender info

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

| TP Id | TP_SEC_ITSS_SND_CAM_05_02_BV |
|---|---|
| Summary | Check that the secured CAM contains the signer_info field of certificate when the timeout of one second has been expired after the previous CAM containing the certificate |
| Reference | ETSI TS 103 097 [1], clause 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT is configured to send more than one CAM per second
   and the IUT having sent a CAM
      containing header_fields['signer_info'].signer.type
         indicating 'certificate'
      at TIME_LAST
ensure that
   when
      the IUT is sending a CAM
         containing header_fields['generation_time']
            indicating TIME >= TIME_LAST + 1sec
   then
      this message is
         containing header_fields ['signer_info']
            containing signer
               containing type
                  indicating 'certificate'
               and containing certificate
```

### 5.2.4.4 Check that IUT sends cert to unknown ITS-S

| TP Id | 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)
      and containing header_fields['signer_info']
         containing signer
            containing type
               indicating 'certificate_digest_with_sha256'
            and containing digest
               indicating HashedId3 value
                  referencing an 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
         and containing header_fields[0]
            containing type
               indicating 'signer_info'
            and containing signer
               containing type
                  indicating 'certificate'
               and containing certificate
```

### 5.2.4.5 Check that IUT restarts the timer when the certificate has been sent

| | |
|---|---|
| **TP Id** | TP_SEC_ITSS_SND_CAM_07_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** | |

```
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
                  at TIME_2 (TIME_1 +0.3sec)
      containing header_fields['signer_info'].signer.type
         indicating 'certificate_digest_with_ecdsap256'
      and containing header_fields['signer_info'].signer.digest
         referencing an unknown certificate
   and the IUT having sent CAM at TIME_3 (TIME_3 > TIME_2)
      containing header_fields['signer_info'].signer.type
         indicating 'certificate'
ensure that
   when
      the IUT is sending the next CAM at TIME_4
         containing header_fields['signer_info'].signer.type
            indicating 'certificate'
   then
      the difference between TIME_4 and TIME_3 is about 1sec
```

### 5.2.4.6 Check that IUT sends certificate when requested

| | |
|---|---|
| **TP Id** | 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 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)
   then
      the IUT sends a SecuredMessage
         containing header_fields['signer_info']
            containing signer
               containing type
                  indicating 'certificate'
               and containing certificate
                  referenced by the requested digest
```

### 5.2.4.7 Check that IUT send certificate_chain when requested

| | |
|---|---|
| **TP Id** | 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** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT is configured to send more than one CAM per second<br>and the IUT having already sent a CAM<br>containing header_fields['signer_info'].signer.type<br>indicating 'certificate'<br>at TIME_1<br>and the IUT having received a SecuredMessage<br>containing header_fields['request_unrecognized_certificate']<br>containing digests<br>containing HashedId3 value<br>referencing to the AA certificate<br>at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec)<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>at TIME_3 (TIME_1 < TIME_2 < TIME_3 < TIME_1+1sec)<br>then<br>the IUT sends a SecuredMessage<br>and containing header_fields['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate_chain'<br>and containing certificates[last]<br>indicating the AT certificate<br>and containing certificates[last-1]<br>indicating the AA certificate | |

### 5.2.4.8 Check generation time

| | |
|---|---|
| **TP Id** | TP_SEC_ITSS_SND_CAM_10_01_BV |
| **Summary** | Check that Secured CAM generation time is inside the validity period of the signing certificate;<br>Check that message generation time value is realistic |
| **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
   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 GEN_TIME (CUR_TIME - 5min <= GEN_TIME <= CUR_TIME + 5min)
         and containing header_fields ['signer_info']
            containing signer
               containing type
                  indicating 'certificate'
               and containing certificate
                  containing validity_restrictions['time_end']
                     containing end_validity
                        indicating value > GEN_TIME
                  or containing validity_restrictions['time_start_and_end']
                     containing start_validity
                        indicating value <= GEN_TIME
                     and containing end_validity
                        indicating value > GEN_TIME
                  or containing validity_restrictions['time_start_and_duration']
                     containing start_validity (X_START_VALIDITY)
                        indicating value <= GEN_TIME
                     and containing duration
                        indicating value > GEN_TIME - X_START_VALIDITY
```

### 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 |
| **Reference** | ETSI TS 103 097 [1], clause 7.1 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT has receiving a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate_digest_with_sha256'<br>and containing digest<br>indicating HashedId3 value DIGEST_A<br>referencing an unknown certificate<br>ensure that<br>when<br>the IUT is requested to send CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['request_unrecognized_certificate']<br>containing digests<br>containing HashedId3 value<br>indicating DIGEST_A | |

### 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** | |
| with<br>the IUT being in the 'authorized' state<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>and containing payload_field<br>containing type<br>indicating 'signed'<br>and containing 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 |
|---|---|
| Summary | Check that the secured CAM contains only one TrailerField of type signature;<br>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 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate_digest_with_ecdsap256'<br>and containing digest<br>referencing the certificate<br>containing subject_info.subject_type<br>indicating 'authorization_ticket'<br>and containing subject_attributes['verification key'] (KEY)<br>or containing signer<br>containing type<br>indicating 'certificate'<br>and containing certificate<br>containing subject_info.subject_type<br>indicating 'authorization_ticket' (2)<br>and containing subject_attributes['verification key'] (KEY)<br>containing trailer_fields<br>containing single instance of type TrailerField<br>containing type<br>indicating 'signature'<br>and containing signature<br>verifiable using KEY | |

## 5.2.5 DENM profile

### 5.2.5.1 Check secured DENM its_aid value

| TP Id | TP_SEC_ITSS_SND_DENM_01_01_BV |
|---|---|
| Summary | Check that the sent Secured DENM contains a 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** | |
| with<br>the IUT being in the 'authorized' state<br>ensure that<br>when<br>the IUT is requested to send a DENM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields ['its_aid']<br>containing its_aid<br>indicating 'AID_DENM' | |

### 5.2.5.2 Check header fields

| | |
|---|---|
| **TP Id** | TP_SEC_ITSS_SND_DENM_02_01_BV |
| **Summary** | Check that the secured DENM contains exactly one element of these header fields: signer_info, generation_time, generation_location, message_type;<br>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;<br>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** | |
| with<br>the IUT being in the 'authorized' state<br>ensure that<br>when<br>the IUT is requested to send DENM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields[0]<br>containing type<br>indicating 'signer_info'<br>and containing header_fields [n].type<br>indicating value less than header_fields [n+1].type<br>and containing header_fields ['generation_time']<br>and containing header_fields ['generation_location']<br>and containing header_fields ['its_aid']<br>and not containing header_fields ['generation_time_with_confidence'] | |

### 5.2.5.3 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** | |
| with<br>the IUT being in the 'authorized' state<br>ensure that<br>when<br>the IUT is requested to send a DENM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>and containing certificate | |

### 5.2.5.4 Check generation time

| TP Id | TP_SEC_ITSS_SND_DENM_04_01_BV |
|---|---|
| **Summary** | Check that Secured DENM generation time is inside the validity period of the signing certificate;<br>Check that 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 GEN_TIME (CUR_TIME - 10min <= GEN_TIME < CUR_TIME + 10min)
         containing header_fields['signer_info']
            containing signer
               containing type
                  indicating 'certificate'
               containing certificate
                  containing validity_restrictions['time_end']
                     and containing end_validity
                        indicating value > GEN_TIME
                  or containing validity_restrictions['time_start_and_end']
                     containing start_validity
                        indicating value <= GEN_TIME
                     and containing end_validity
                        indicating value > GEN_TIME
                  or containing validity_restrictions['time_start_and_duration']
                     containing start_validity (X_START_VALIDITY)
                        indicating value <= GEN_TIME
                     and containing duration
                        indicating value > GEN_TIME - X_START_VALIDITY
```

### 5.2.5.5 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_GN_SECURITY AND PICS_CERTIFICATE_SELECTION |
| **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
```

| TP Id | TP_SEC_ITSS_SND_DENM_05_02_BV |
|---|---|
| Summary | Check that the secured DENM contains exactly one HeaderField generation_location which is inside the circular region defined by the validity restriction of the certificate pointed by the signer_info field |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND 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

| 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 defined by the validity restriction of the certificate pointed by the signer_info field |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND PICS_USE_RECTANGULAR_REGION |
| **Expected behaviour** | |

with
  the IUT has been authorized with the AT certificate (CERT_IUT_C_AT)
    containing validity_restrictions ['region']
      containing region
        containing region_type
          indicating 'rectangle'
        containing rectangular_region
          containing instance of RectangularRegion
            indicating 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
          indicating value inside the REGION

| TP Id | TP_SEC_ITSS_SND_DENM_05_04_BV |
|---|---|
| Summary | Check that the secured DENM contains exactly one HeaderField generation_location which is inside the polygonal region defined by the validity restriction of the certificate pointed by the signer_info field |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND PICS_USE_POLYGONAL_REGION |
| **Expected behaviour** | |
| with<br>the IUT has been authorized with the AT certificate (CERT_IUT_D_AT)<br>containing validity_restrictions ['region']<br>containing region<br>containing region_type<br>indicating 'polygon'<br>containing polygonal_region<br>indicating REGION<br>ensure that<br>when<br>the IUT is requested to send a DENM<br>then<br>the IUT sends a SecuredMessage<br>containing exactly one header_field ['generation_location']<br>containing generation_location<br>indicating value inside the REGION | |

| 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 defined by the validity restriction of the certificate pointed by the signer_info field |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND PICS_USE_IDENTIFIED_REGION |
| **Expected behaviour** | |
| with<br>the IUT has been authorized with the AT certificate (CERT_IUT_E_AT)<br>containing validity_restrictions ['region']<br>containing region<br>containing region_type<br>indicating 'id_region'<br>containing identified_region<br>indicating REGION<br>ensure that<br>when<br>the IUT is requested to send a DENM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields<br>containing exactly one instance of HeaderField<br>containing type<br>indicating 'generation_location'<br>containing generation_location<br>indicating value inside the REGION | |

| 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_GN_SECURITY AND NOT PICS_CERTIFICATE_SELECTION |
| 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
            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
         and containing exactly one header_field ['generation_location']
            containing generation_location
               indicating location inside the REGION
```

### 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
      the IUT is requested to send a DENM
   then
      the IUT sends a SecuredMessage
         containing payload_field
            containing type
               indicating 'signed'
            and 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;<br>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<br>the IUT being in the 'authorized' state<br>ensure that<br>when<br>the IUT is requested to send DENM<br>then<br>the IUT sends a SecuredMessage<br>containing header_field ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>and containing certificate<br>containing subject_info.subject_type<br>indicating 'authorization_ticket' (2)<br>and containing subject_attributes['verification key'] (KEY)<br>and containing trailer_fields<br>containing single instance of type TrailerField<br>containing type<br>indicating 'signature'<br>and containing signature<br>verifiable using KEY | |

### 5.2.6 Generic signed message profile

#### 5.2.6.1 Check secured its_aid value

| | |
|---|---|
| **TP Id** | TP_SEC_ITSS_SND_GENMSG_01_01_BV |
| **Summary** | Check that the sent Secured Message contains HeaderField its_aid that is set to other value then AID_CAM and AID_DENM |
| **Reference** | ETSI TS 103 097 [1], clause 5.4 |
| **PICS Selection** | PICS_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>ensure that<br>when<br>the IUT is requested to send a Beacon<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields ['its_aid']<br>containing its_aid<br>indicating 'AID_BEACON' | |

### 5.2.6.2 Check header field

| | |
|---|---|
| **TP Id** | 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;<br>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 AND NOT PICS_ITS_AID_OTHER_PROFILE |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>ensure that<br>when<br>the IUT is requested to send a Beacon<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields [0].type<br>indicating 'signer_info'<br>and containing header_fields [1..n]<br>where header_fields [i].type < header_fields [i+1].type<br>and containing header_fields ['generation_time']<br>and containing header_fields ['generation_location']<br>and containing header_fields ['its_aid'] | |

### 5.2.6.3 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 AND NOT PICS_ITS_AID_OTHER_PROFILE |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>ensure that<br>when<br>the IUT is requested to send a Beacon<br>then<br>the IUT sends a SecuredMessage<br>containing exactly one header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>and containing certificate | |

### 5.2.6.4 Check generation time

| TP Id | 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 AND NOT 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 exactly one header_fields['generation_time']
            containing generation_time
               indicating GEN_TIME (CUR_TIME - 10min <= GEN_TIME < CUR_TIME + 10min)
         and containing header_fields['signer_info']
            containing signer
               containing type
                  indicating 'certificate'
               containing certificate
                  containing validity_restrictions['time_end']
                     and containing end_validity
                        indicating value > GEN_TIME
                  or containing validity_restrictions['time_start_and_end']
                     containing start_validity
                        indicating value <= GEN_TIME
                     and containing end_validity
                        indicating value > GEN_TIME
                  or containing validity_restrictions['time_start_and_duration']
                     containing start_validity (X_START_VALIDITY)
                        indicating value <= GEN_TIME
                     and containing duration
                        indicating value > GEN_TIME - X_START_VALIDITY
```

### 5.2.6.5 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_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE AND PICS_CERTIFICATE_SELECTION |
| **Expected behaviour** | |

```
with
   the IUT has been authorized with the AT certificate (CERT_AT_A)
      not containing validity_restrictions['region']
ensure that
   when
      the IUT is requested to send a Beacon
   then
      the IUT sends a SecuredMessage
         containing exactly one header_fields['generation_location']
            containing generation_location
```

| TP Id | TP_SEC_ITSS_SND_GENMSG_05_02_BV |
|---|---|
| Summary | 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 Selection | PICS_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE AND PICS_CERTIFICATE_SELECTION AND PICS_USE_CIRCULAR_REGION |
| **Expected behaviour** | |

with
  the IUT has been authorized with the AT certificate (CERT_AT_B)
    containing validity_restrictions ['region']
      containing region
        containing region_type
          indicating 'circle'
        and containing circular_region
          indicating REGION
ensure that
  when
    the IUT is requested to send a Beacon
  then
    the IUT sends a SecuredMessage
      containing exactly one header_fields['generation_location']
        containing generation_location
          indicating value inside the REGION

| TP Id | TP_SEC_ITSS_SND_GENMSG_05_03_BV |
|---|---|
| Summary | Check that the secured GeoNetworking message 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 7.3 |
| PICS Selection | PICS_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE AND PICS_CERTIFICATE_SELECTION AND PICS_USE_RECTANGULAR_REGION |
| **Expected behaviour** | |

with
  the IUT has been authorized with the AT certificate (CERT_AT_C)
    containing validity_restrictions ['region']
      containing region
        containing region_type
          indicating 'rectangle'
        containing rectangular_region
          containing instance of RectangularRegion
            indicating REGION
ensure that
  when
    the IUT is requested to send a Beacon
  then
    the IUT sends a SecuredMessage
      containing exactly one header_fields['generation_location']
        containing generation_location
          indicating value inside the REGION

| TP Id | TP_SEC_ITSS_SND_GENMSG_05_04_BV |
|---|---|
| Summary | Check that the secured GeoNetworking message 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 | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE AND PICS_CERTIFICATE_SELECTION AND 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 exactly one header_fields['generation_location']
        containing generation_location
          indicating value inside the REGION

| TP Id | TP_SEC_ITSS_SND_GENMSG_05_05_BV |
|---|---|
| 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_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE AND PICS_CERTIFICATE_SELECTION AND PICS_USE_IDENTIFIED_REGION |
| Expected behaviour | |

with
  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
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 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 Selection | PICS_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE AND NOT PICS_CERTIFICATE_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['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
         and containing exactly one header_fields['generation_location']
            containing generation_location
               indicating location inside the REGION
```

### 5.2.6.6 Check payload

| TP Id | TP_SEC_ITSS_SND_GENMSG_06_01_BV |
|---|---|
| Summary | Check that the secured message contains the Payload element of type signed, signed_external or signed_and_encrypted |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY AND NOT 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 payload_field
            containing type
               indicating 'signed' or 'signed_external' or 'signed_and_encrypted'
```

#### 5.2.6.7 Check signature

| TP Id | TP_SEC_ITSS_SND_GENMSG_07_01_BV |
|---|---|
| Summary | Check that the secured message contains only one TrailerField of type signature;<br>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 7.3 |
| PICS Selection | PICS_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>ensure that<br>when<br>the IUT is requested to send a Beacon<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>containing certificate<br>indicating CERT<br>and containing trailer_fields ['signature']<br>containing signature<br>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 7.4.1 |
| PICS Selection | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate in the SecuredMessage<br>ensure that<br>when<br>the IUT is requested to send a SecuredMessage<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating certificate<br>containing certificate<br>containing version<br>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 7.4.1 |
| PICS Selection | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate chain in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate_chain'<br>and containing certificates<br>indicating length N > 0<br>and containing certificates [n] (0..N)<br>containing version<br>indicating '2' | |

### 5.2.7.2 Check the certificate chain consistence

| TP Id | TP_SEC_ITSS_SND_CERT_02_01_BV |
|---|---|
| Summary | Check that the references in the certificate chain are valid<br>Check that signer_info type of all certificates in the chain are 'certificate_digest_with_sha256', 'certificate_digest_with_other_algorithm'or 'self' |
| Reference | ETSI TS 103 097 [1], clauses 4.2.10, 6.1 and 7.4.1 |
| PICS Selection | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate chain in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate_chain'<br>and containing certificates<br>indicating length N > 1<br>and containing certificates[0]<br>containing signer_info<br>containing type<br>indicating 'certificate_digest_with_sha256'<br>or indicating 'certificate_digest_with_other_algorythm'<br>and containing digest<br>referencing the trusted certificate<br>or containing signer_info<br>containing type<br>indicating 'self'<br>and containing certificates[n] (1..N)<br>containing signer_info<br>containing type<br>indicating 'certificate_digest_with_sha256'<br>or indicating 'certificate_digest_with_other_algorythm'<br>and containing digest<br>referencing the certificates[n-1] | |

### 5.2.7.3 Check rectangular region validity restriction

| | |
|---|---|
| **TP Id** | TP_SEC_ITSS_SND_CERT_04_01_BV |
| **Summary** | Check that the rectangular region validity restriction of the message signing certificate contains not more than six valid rectangles;<br>Check that the rectangular region validity restriction of the message signing certificate 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_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND PICS_USE_RECTANGULAR_REGION |
| **Expected behaviour** | |

with<br>
the IUT being in the 'authorized' state<br>
the IUT being requested to include certificate in the next CAM<br>
ensure that<br>
when<br>
the IUT is requested to send a CAM<br>
then<br>
the IUT sends a SecuredMessage<br>
containing header_fields['signer_info'].signer<br>
containing type<br>
indicating 'certificate'<br>
containing certificate<br>
containing validity_restrictions['region']<br>
containing region<br>
containing region_type<br>
indicating 'rectangle'<br>
and containing rectangular_region<br>
indicating length <= 6<br>
and containing elements of type RectangularRegion<br>
indicating continuous region without holes<br>
and containing northwest and southeast<br>
indicating northwest is on the north from southeast

| TP Id | TP_SEC_ITSS_SND_CERT_04_02_BV |
|---|---|
| Summary | Check that the rectangular region validity restriction of all certificates contains not more than six valid rectangles;<br>Check that the rectangular region validity restriction of the AT certificate is continuous and does not contain any holes<br>Check that the rectangular certificate validity region of the subordinate certificate is well formed and inside the validity region of the issuing certificate |
| Reference | ETSI TS 103 097 [1], clauses 4.2.20 and 4.2.23 |
| PICS Selection | PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND 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 length N > 0
               and containing certificates [n] (0..N)
                  containing validity_restrictions['region']
                     containing region
                        containing region_type
                           indicating 'rectangle'
                        and 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
```

### 5.2.7.4 Check polygonal region validity restriction

| TP Id | 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;<br>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_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND 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
   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
                     containing region_type
                        indicating 'polygon'
                     and containing polygonal_region
                        indicating length >=3 and <=12
                        and indicating continuous region without holes and intersections
```

| TP Id | TP_SEC_ITSS_SND_CERT_05_02_BV |
|---|---|
| Summary | Check that the polygonal certificate validity region is inside the validity region of the issuing certificate;<br>Check that the issuing polygonal certificate validity region contains at least three and no more than 12 points;<br>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_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND 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'
and containing certificates
indicating length N > 0
and containing certificates [n] (0..N)
containing validity_restrictions['region']
containing region
containing region_type
indicating 'polygon'
and containing polygonal_region
indicating length >=3 and <=12
and indicating continuous region without holes and intersections

### 5.2.7.5 Check identified region validity restriction

| | |
|---|---|
| **TP Id** | 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 [4] or defined by United Nations Statistics Division [5] |
| **Reference** | ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1 |
| **PICS Selection** | PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND 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'
            and containing certificate
               containing validity_restrictions['region']
                  containing region
                     containing region_type
                        indicating 'id'
                     and containing id_region
                        containing region_dictionary
                           indicating 'iso_3166_1'
                        and containing region_identifier
                           indicating valid value according to ISO-3166-1
                        and containing local_region
                     or containing id_region
                        containing region_dictionary
                           indicating 'un_stats'
                        and containing region_identifier
                           indicating valid value according to UN STATS
                        and containing local_region
```

| TP Id | TP_SEC_ITSS_SND_CERT_06_02_BV |
|---|---|
| Summary | Check that the identified certificate validity region contains values that correspond to numeric country codes as defined in ISO 3166-1 [4] or defined by United Nations Statistics Division [5];<br>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], clauses 4.2.26 and 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND 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'
and containing certificates
indicating length N > 1
and containing certificates[n](0..N)
containing validity_restrictions['region']
containing region
containing region_type
indicating 'id'
and containing id_region
containing region_dictionary
indicating 'iso_3166_1'
and containing region_identifier
indicating valid value according to ISO_3166-1 dictionary
and containing local_region
or containing region
containing region_type
indicating 'id'
and containing id_region
containing region_dictionary
indicating 'un_stats'
and containing region_identifier
indicating valid value according to UN STATS dictionary
and containing local_region

### 5.2.7.6 Check region validity restrictions in the chain

| **TP Id** | TP_SEC_ITSS_SND_CERT_07_01_BV |
|---|---|
| **Summary** | Check that the region of the subordinate certificate validity restriction is inside the region of the issuing certificate validity restriction |
| **Reference** | ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1 |
| **PICS Selection** | PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION |

**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'
            and containing certificates
               indicating length N > 1
               and containing certificates[n](0..N)
                  indicating certificate
                     not containing validity_restrictions['region']
                     and containing signer_info
                        containing digest
                           referencing the certificate
                              not containing validity_restrictions['region']
                  or indicating certificate
                     containing validity_restrictions['region']
                        containing region.region_type
                           indicating 'none'
                     and containing signer_info
                        containing digest
                           referencing the certificate
                              not containing validity_restrictions['region']
                              or containing validity_restrictions['region']
                                 containing region.region_type
                                    indicating 'none'
                  or indicating certificate
                     containing validity_restrictions['region']
                        containing region.region_type
                           indicated 'circle'
                           or indicated 'rectangle'
                           or indicated 'polygon'
                           or indicated 'id'
                        and containing region (X_CERT__REGION)
                     and containing signer_info
                        containing digest
                           referencing the certificate
                              not containing validity_restrictions['region']
                              or containing validity_restrictions['region']
                                 containing region.region_type
                                    indicating 'none'
                              or containing validity_restrictions['region']
                                 containing region
                                    indicating region fully covering the X_CERT_REGION
```

| TP Id | TP_SEC_ITSS_SND_CERT_07_02_BV |
|---|---|
| Summary | Check that the identified region validity restriction of the subordinate certificate is included in the identified region validity restriction of the issuing certificate |
| Reference | ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND PICS_USE_IDENTIFIED_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   the IUT is using both AA and AT certificates with identified region validity restriction
   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 length > 1
               and containing certificates [n] (0..N)
                  containing validity_restrictions['region']
                     containing region
                        containing region_type
                           indicating 'id'
                        containing id_region
                           containing region_dictionary
                              indicating 'iso_3166_1'
                              or indicating 'un_stats'
                           containing region_identifier (X_CERT_REGION_ID)
                              indicating valid value according to ISO_3166-1 or UN STATS dictionary
                           containing local_region (X_CERT_LOCAL_REGION)
               and containing signer_info
                  containing digest
                     referencing the certificate
                        containing validity_restrictions['region']
                           containing region
                              containing region_type
                                 indicating 'id'
                              containing id_region
                                 containing region_dictionary
                                    indicating 'iso_3166_1'
                                    or indicating 'un_stats'
                                 and containing region_identifier
                                    indicating value == X_CERT_REGION_ID
                                 and containing local_region
                                    indicating value == X_CERT_LOCAL_REGION
                                    or indicating 0
                              or containing id_region
                                 containing region_dictionary
                                    indicating 'un_stats'
                                 and containing region_identifier
                                    indicating value fully covering the X_CERT_REGION_ID
```

### 5.2.7.7 Check time validity restriction in the chain

| | |
|---|---|
| **TP Id** | TP_SEC_ITSS_SND_CERT_08_01_BV |
| **Summary** | Check the certificate chain to ensure that the time validity restriction of the subordinate certificate is inside the time validity restriction of the issuing certificate |
| **Reference** | ETSI TS 103 097 [1], clause 7.4.4 |
| **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 length N > 1
               and containing certificates[n] (0..N)
                  containing validity_restrictions
                     containing validity_restrictions['time_end']
                        containing end_validity
                           indicating X_END_VALIDITY_AT
                     or containing validity_restrictions['time_start_and_end']
                        containing start_validity
                           indicating X_START_VALIDITY_AT
                        and containing end_validity
                           indicating X_END_VALIDITY_AT >X_START_VALIDITY_AT
                     or containing validity_restrictions['time_start_and_duration']
                        containing start_validity
                           indicating X_START_VALIDITY_AT
                        and containing end_validity
                           indicating X_DURATION_AT > 0
                  and containing signer_info
                     containing digest
                        referencing the certificate
                           containing validity_restrictions['time_end']
                              containing end_validity
                                 indicating value >= X_END_VALIDITY_AT if defined
                                 or indicating value >= X_START_VALIDITY_AT + X_DURATION_AT
                           or containing validity_restrictions['time_start_and_end']
                              containing start_validity
                                 indicating value <= X_START_VALIDITY_AT if defined
                                 or indicating value <= CURRENT_TIME
                              and containing end_validity
                                 indicating value >= X_END_VALIDITY_AT if defined
                                 or indicating value >= X_START_VALIDITY_AT + X_DURATION_AT
                           or containing validity_restrictions['time_start_and_duration']
                              containing start_validity
                                 indicating X_START_VALIDITY_AA <= X_START_VALIDITY_AT if defined
                                 or indicating X_START_VALIDITY_AA <= CURRENT_TIME
                              and containing duration
                                 indicating value >= X_END_VALIDITY_AT - X_START_VALIDITY_AA if defined
                                 or indicating value >= X_START_VALIDITY_AT + X_DURATION_AT -
                                          X_START_VALIDITY_AA
```

### 5.2.7.8 Check ECC point type of the certificate signature

| **TP Id** | TP_SEC_ITSS_SND_CERT_09_01_BV |
|---|---|
| **Summary** | Check that the certificate signature contains ECC point of type set to either compressed_lsb_y_0, compressed_lsb_y_1 or x_coordinate_only |
| **Reference** | ETSI TS 103 097 [1], clause 4.2.9 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate'<br>containing certificate<br>containing signature.ecdsa_signature<br>containing R.type<br>indicating compressed_lsb_y_0<br>or indicating compressed_lsb_y_1<br>or indicating x_coordinate_only | |

| **TP Id** | TP_SEC_ITSS_SND_CERT_09_02_BV |
|---|---|
| **Summary** | Check that the all certificates in a chain have signatures contains ECC point of type set to either compressed_lsb_y_0, compressed_lsb_y_1 or x_coordinate_only |
| **Reference** | ETSI TS 103 097 [1], clause 4.2.9 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate_chain'<br>containing certificates<br>indicating length N > 1<br>and containing certificates[n](0..N)<br>containing signature.ecdsa_signature<br>containing R.type<br>indicating compressed_lsb_y_0<br>or indicating compressed_lsb_y_1<br>or indicating x_coordinate_only | |

### 5.2.7.9 Check ECC point type of the certificate verification key

| **TP Id** | TP_SEC_ITSS_SND_CERT_10_01_BV |
|---|---|
| **Summary** | Check that the certificate verification key contains ECC point of type set to either compressed_lsb_y_0, compressed_lsb_y_1 or uncompressed |
| **Reference** | ETSI TS 103 097 [1], clause 4.2.4 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate'<br>and containing certificate<br>containing subject_attributes['verification_key']<br>containing key.public_key.type<br>indicating compressed_lsb_y_0<br>or indicating compressed_lsb_y_1<br>or indicating uncompressed | |

| **TP Id** | TP_SEC_ITSS_SND_CERT_10_02_BV |
|---|---|
| **Summary** | Check that all certificate in a chain have verification keys contains ECC point of type set to either compressed_lsb_y_0, compressed_lsb_y_1 or uncompressed |
| **Reference** | ETSI TS 103 097 [1], clause 4.2.4 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate_chain'<br>and containing certificates<br>indicating length N > 0<br>containing certificates [n] (0..N)<br>containing subject_attributes['verification_key']<br>containing key.public_key.type<br>indicating compressed_lsb_y_0<br>or indicating compressed_lsb_y_1<br>or indicating uncompressed | |

### 5.2.7.10 Verify certificates signatures

| **TP Id** | TP_SEC_ITSS_SND_CERT_11_01_BV |
|---|---|
| **Summary** | Check the certificate signature |
| **Reference** | ETSI TS 103 097 [1], clauses 6.1 and 7.4.1 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate'<br>and containing certificate<br>containing signer_info<br>containing type<br>indicating 'certificate_digest_with_sha256'<br>and containing digest<br>referencing the certificate CERT<br>and containing signature<br>verifiable using CERT.subject_attributes['verification_key'].key | |

| **TP Id** | TP_SEC_ITSS_SND_CERT_11_02_BV |
|---|---|
| **Summary** | Check the validity of signatures of all certificates in the chain |
| **Reference** | ETSI TS 103 097 [1], clauses 6.1 and 7.4.1 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate chain in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate_chain'<br>and containing certificates<br>indicating length N > 1<br>and containing certificates[0]<br>containing signer_info<br>containing type<br>indicating 'certificate_digest_with_sha256'<br>and containing digest<br>referencing the trusted certificate (CERT_ROOT)<br>and containing signature<br>verifiable using CERT_ROOT<br>.subject_attributes['verification_key'].key<br>and containing certificates[n] (1..N)<br>containing signer_info<br>containing type<br>indicating 'certificate_digest_with_sha256'<br>and containing digest<br>referencing the certificates[n-1]<br>and containing signature<br>verifiable using certificates[n-1]<br>.subject_attributes['verification_key'].key | |

### 5.2.7.11 Check certificate assurance level in the chain

| | |
|---|---|
| **TP Id** | TP_SEC_ITSS_SND_CERT_12_01_BV |
| **Summary** | Check that the assurance level of the subordinate certificate is equal to or less than the assurance level of the issuing certificate |
| **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
               indicating length N > 1
               and containing certificates[n](0..N)
                  containing subject_attributes ['assurance_level']
                     containing assurance_level
                        containing bits [5-7]
                           indicating assurance level CERT_AL
               and containing signer_info
                  containing digest
                     referencing the certificate
                        containing subject_attributes ['assurance_level']
                           containing assurance_level
                              containing bits [5-7]
                                 indicating value <= CERT_AL
```

### 5.2.7.12 AA certificate profile

#### 5.2.7.12.1 Check AA certificate subject type

| | |
|---|---|
| **TP Id** | 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 7.4.4 |
| **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'
            and containing certificates
               containing certificates[last-1]
                  containing subject_info.subject_type
                     indicating 'authorization_authority'
```

### 5.2.7.12.2 Check AA certificate subject name

| **TP Id** | TP_SEC_ITSS_SND_CERT_AA_02_01_BV |
|---|---|
| **Summary** | Check that the AA certificsate subject_name variable-length vector contains 32 bytes maximum |
| **Reference** | ETSI TS 103 097 [1], clause 6.2 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate chain in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate_chain'<br>and containing certificates<br>containing certificates[last-1]<br>containing subject_info.subject_name<br>indicating length <= 32 bytes | |

### 5.2.7.12.3 Check that signer info of AA certificate is a digest

| **TP Id** | TP_SEC_ITSS_SND_CERT_AA_03_01_BV |
|---|---|
| **Summary** | Check that signer_info type of AA certificates is set to 'certificate_digest_with_sha256' |
| **Reference** | ETSI TS 103 097 [1], clause 7.4.4 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate chain in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate_chain'<br>and containing certificates<br>containing certificates[last-1]<br>containing signer_info<br>containing type<br>indicating 'certificate_digest_with_sha256' | |

#### 5.2.7.12.4 Check that AA cert is signed by Root cert

| **TP Id** | TP_SEC_ITSS_SND_CERT_AA_04_01_BV |
|---|---|
| **Summary** | Check that AA certificate is signed by Root CA or other authority.<br>NOTE: There is no clear specification that AA cert shall be signed by the Root CA only. |
| **Reference** | ETSI TS 103 097 [1], clause 6.3 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate chain in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate_chain'<br>and containing certificates<br>containing certificates[last-1]<br>containing signer_info<br>containing type<br>indicating 'certificate_digest_with_ecdsap256'<br>and containing digest<br>referencing to the trusted certificate<br>containing subject_info.subject_type<br>indicating 'root_ca'<br>or indicating 'authorisation_authority' | |

#### 5.2.7.12.5 Check AA ceretificate subject attributes presence and order

| **TP Id** | 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, 7.4.1 and 7.4.4 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate chain in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate_chain'<br>and containing certificates<br>containing certificates[last-1]<br>containing subject_attributes [0..N]<br>indicating subject_attributes[n].type<br>< subject_attributes[n+1].type<br>and containing subject_attributes['verification_key']<br>and containing subject_attributes['assurance_level']<br>and containing subject_attributes['its_aid_list'] | |

#### 5.2.7.12.6 Check ITS-AID list of AA certificate

| **TP Id** | TP_SEC_ITSS_SND_CERT_AA_08_01_BV |
|---|---|
| **Summary** | Check that all AIDs containing in the its_aid_list in AA certificate are unique<br>Check that AID list contains not more than 31 items |
| **Reference** | ETSI TS 103 097 [1], clause 7.4.4 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate chain in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate_chain'<br>and containing certificates<br>containing certificates[last-1]<br>containing subject_attributes['its_aid_list']<br>containing its_aid_list<br>containing not more than 31 unique items | |

#### 5.2.7.12.7 Check AA certificate validity restriction presence and order

| **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], clauses 6.1, 6.7 and 7.4.1 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate chain in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate_chain'<br>and containing certificates<br>containing certificates[last-1]<br>containing validity_restrictions[0..N]<br>indicating validity_restrictions[n].type<br>< validity_restrictions[n+1].type<br>and containing validity_restrictions['time_start_and_end']<br>and not containing validity_restrictions['time_end']<br>and not containing validity_restrictions['time_start_and_duration'] | |

#### 5.2.7.12.8 Check the AA certificate time_start_and_end validity restriction

| | |
|---|---|
| **TP Id** | TP_SEC_ITSS_SND_CERT_AA_11_01_BV |
| **Summary** | Check that time_start_and_end is included in the AA certificate validation restrictions;<br>Check that end_validity is greater than start_validity;<br>Check that validity restriction of AA certificate is inside the validity restriction of its issuing certificate |
| **Reference** | ETSI TS 103 097 [1], clause 7.4.4 |
| **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
               containing certificates[last-1]
                  containing validity_restrictions
                     containing validity_restrictions['time_start_and_end']
                        containing start_validity
                           indicating START_VALIDITY_AA
                        containing end_validity
                           indicating END_VALIDITY_AA >=START_VALIDITY_AA
                  and containing signer_info
                     containing digest
                        referencing the trusted certificate
                           containing validity_restrictions['time_end']
                              containing end_validity
                                 indicating value > END_VALIDITY_AA
                           or containing validity_restrictions['time_start_and_end']
                              containing start_validity
                                 indicating value <= START_VALIDITY_AA
                              and containing end_validity
                                 indicating value > END_VALIDITY_AA
                           or containing validity_restrictions['time_start_and_duration']
                              containing start_validity
                                 indicating X_START_VALIDITY <= START_VALIDITY_AA
                              and containing duration
                                 indicating value > END_VALIDITY_AA - X_START_VALIDITY
```

### 5.2.7.13 AT certificate profile

#### 5.2.7.13.1 Check AT certificate subject type

| | |
|---|---|
| **TP Id** | TP_SEC_ITSS_SND_CERT_AT_01_01_BV |
| **Summary** | Check that the subject_type of the AT certificate is set to 'authorization_ticket' |
| **Reference** | ETSI TS 103 097 [1], clause 7.4.2 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate'<br>and containing certificate<br>containing subject_info.subject_type<br>indicating 'authorization_ticket' | |

#### 5.2.7.13.2 Check AT certificate subject name

| | |
|---|---|
| **TP Id** | TP_SEC_ITSS_SND_CERT_AT_02_01_BV |
| **Summary** | Check that the subject_name variable-length vector is empty for AT certificates |
| **Reference** | ETSI TS 103 097 [1], clause 7.4.2 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate'<br>and containing certificate<br>containing subject_info.subject_name<br>indicating length = 0 | |

#### 5.2.7.13.3 Check that signer info of AT certificate is a digest

| **TP Id** | TP_SEC_ITSS_SND_CERT_AT_03_01_BV |
|---|---|
| **Summary** | Check that signer_info type of AT certificates is set to 'certificate_digest_with_sha256' |
| **Reference** | ETSI TS 103 097 [1], clause 7.4.2 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate'<br>and containing certificate<br>containing signer_info.<br>containing type<br>indicating 'certificate_digest_with_sha256' | |

#### 5.2.7.13.4 Check AT ceretificate subject attributes presence and order

| **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 7.4.1 and 7.4.2 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate'<br>containing certificate<br>containing subject_attributes [0..N]<br>indicating subject_attributes[n].type<br>< subject_attributes[n+1].type<br>containing subject_attributes['verification_key']<br>containing subject_attributes['assurance_level']<br>containing subject_attributes['its_aid_ssp_list'] | |

#### 5.2.7.13.5 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;<br>Check that time_start_and_end is inside the AA certificate time restrictions<br>Check that validity restriction of AT certificate is inside the validity restriction of its issuing certificate |
| **Reference** | ETSI TS 103 097 [1], clause 7.4.2 |
| **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]
containing subject_info.subject_type
indicating 'authorization_ticket'
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_VALIDITY_AT
containing end_validity
indicating END_VALIDITY_AT
containing certificates[last-1]
containing validity_restrictions['time_end']
containing end_validity
indicating value > END_VALIDITY_AT
or containing validity_restrictions['time_start_and_end']
containing start_validity
indicating value <= START_VALIDITY_AT
and containing end_validity
indicating value > END_VALIDITY_AT
or containing validity_restrictions['time_start_and_duration']
containing start_validity
indicating X_START_VALIDITY <= START_VALIDITY_AT
and containing duration
indicating value > END_VALIDITY_AT - X_START_VALIDITY

### 5.2.7.13.6 Check ITS-AID-SSP

| | |
|---|---|
| **TP Id** | 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;<br>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;<br>Check that the length of SSP of each AID is 31 octets maximum |
| **Reference** | ETSI TS 103 097 [1], clauses 6.9 and 7.4.2 |
| **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'
          and containing subject_attributes['its_aid_list']
            containing its_aid_list[0..N]
              indicating ITS_AID_LIST_AA
        and containing certificates[last]
          containing subject_info.subject_type
            indicating 'authorization_ticket'
          and 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
                and containing service_specific_permissions
                  indicating length <= 31 octet

#### 5.2.7.13.7 Check that AT certificate is signed by AA cert

| **TP Id** | 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** | |
| with<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate chain in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating certificate_chain<br>containing certificates[last-1] (CERT_AA)<br>containing subject_info.subject_type<br>indicating 'authorization_authority'<br>and containing subject_attributes['verification key'] (KEY)<br>containing certificates[last]<br>containing subject_info.subject_type<br>indicating 'authorization_ticket'<br>and containing signer_info<br>containing type<br>indicating 'certificate_digest_with_ecdsap256'<br>and containing digest<br>referencing to CERT_AA<br>and containing signature<br>verifiable using KEY | |

#### 5.2.7.13.8 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<br>the IUT being in the 'authorized' state<br>the IUT being requested to include certificate in the next CAM<br>ensure that<br>when<br>the IUT is requested to send a CAM<br>then<br>the IUT sends a SecuredMessage<br>containing header_fields['signer_info'].signer<br>containing type<br>indicating 'certificate'<br>containing certificate<br>containing validity_restrictions<br>indicating validity_restrictions[n].type < validity_restrictions[n+1].type<br>and containing validity_restrictions['time_start_and_end']<br>and not containing validity_restrictions['time_end']<br>and not containing validity_restrictions['time_start_and_duration'] | |

# 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<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage<br>containing protocol_version<br>indicating value '2'<br>and containing header_fields[0]<br>containing type<br>indicating 'signer_info'<br>and containing signer<br>containing type<br>indicating 'certificate'<br>and containing certificate (CERT_TS_A_AT)<br>containing subject_info.subject_type<br>indicating 'authorization_ticket'<br>and containing subject_attributes['verification key'] (KEY)<br>and containing header_fields [1]<br>containing type<br>indicating 'generation_time'<br>and containing generation_time<br>indicating CURRENT_TIME<br>and containing header_fields[2]<br>containing type<br>indicating 'its_aid'<br>and containing its_aid<br>indicating 'AID_CAM'<br>and containing payload_field<br>containing type<br>indicating 'signed'<br>and containing data<br>indicating length > 0<br>containing CAM payload<br>and containing trailer_fields<br>containing trailer_fields[0]<br>containing type<br>indicating 'signature'<br>containing signature<br>verifiable using KEY<br>then<br>the IUT accepts the message | |
| NOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name 'MSG_SEC_RCV_CAM_01'. Only differences to this snippet are mentioned in subsequent test purposes. | |

| **TP Id** | 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<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>and the IUT already received a Secured message containing certificate (CERT_TS_A_AT)<br>containing subject_info.subject_type<br>indicating 'authorization_ticket'<br>and containing subject_attributes['verification key'] (KEY)<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage<br>containing protocol_version<br>indicating value '2'<br>and containing header_fields[0]<br>containing type<br>indicating 'signer_info'<br>and containing signer<br>containing type<br>indicating 'certificate_digest_with_sha256'<br>and containing digest<br>referencing to certificate (CERT_TS_A_AT)<br>and containing header_fields [1]<br>containing type<br>indicating 'generation_time'<br>and containing generation_time<br>indicating CURRENT_TIME<br>and containing header_fields[2]<br>containing type<br>indicating 'its_aid'<br>and containing its_aid<br>indicating 'AID_CAM'<br>and containing payload_field<br>containing type<br>indicating 'signed'<br>and containing data<br>indicating length > 0<br>containing CAM payload<br>and containing trailer_fields<br>containing trailer_fields[0]<br>containing type<br>indicating 'signature'<br>containing signature<br>verifiable using KEY<br>then<br>the IUT accepts the message | |
| NOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name 'MSG_SEC_RCV_CAM_02'. Only differences to this snippet are mentioned in subsequent test purposes. | |

| **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**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
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 certificates[0] (CERT_TS_A_AA)
                     containing subject_info.subject_type
                        indicating 'authorization_authority'
                     and containing subject_attributes['verification key'] (KEY_TS_AA)
                  and containing certificates[1] (CERT_TS_A_AT)
                     containing subject_info.subject_type
                        indicating 'authorization_ticket'
                     and containing signer_info
                        containing type
                           indicating 'certificate_digest_with_sha256'
                        and containing digest
                           referencing to the CERT_TS_A_AA
                     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'
            and containing generation_time
               indicating CURRENT_TIME
         and containing header_fields[2]
            containing type
               indicating 'its_aid'
            and containing its_aid
               indicating 'AID_CAM'
         and containing payload_field
            containing type
               indicating 'signed'
            and containing data
               indicating length > 0
               containing CAM payload
         and containing trailer_fields
            containing trailer_fields[0]
               containing type
                  indicating 'signature'
               and containing signature
                  verifiable using KEY_TC_AT
   then
      the IUT accepts the message
```

NOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name 'MSG_SEC_RCV_CAM_03'. Only differences to this snippet are mentioned in subsequent test purposes.

### 5.3.2.2 Check the message protocol version

| **TP Id** | 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 5.1 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing protocol_version<br>indicating 1<br>then<br>the IUT discards 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 5.1 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing protocol_version<br>indicating 3<br>then<br>the IUT discards a SecuredMessage | |

### 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 header field 'signer_info' |
| **Reference** | ETSI TS 103 097 [1], clause 7.1 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing header_fields[0].type<br>indicating 'signer_info'<br>and containing header_fields[1].type<br>indicating 'signer_info'<br>and containing header_fields [2].type<br>indicating 'generation_time'<br>and containing header_fields[3].type<br>indicating 'its_aid'<br>and not containing other header fields<br>then<br>the IUT discards a SecuredMessage | |

| TP Id | TP_SEC_ITSS_RCV_CAM_04_02_BO |
|---|---|
| Summary | Check that IUT discards a secured CAM if the header_fields does not contain the header '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
  and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
  when
    the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)
      containing header_fields[0].type
        indicating 'generation_time'
      and containing header_fields[1].type
        indicating 'its_aid'
      and not containing other header fields
  then
    the IUT discards a SecuredMessage

| TP Id | TP_SEC_ITSS_RCV_CAM_04_03_BO |
|---|---|
| Summary | Check that IUT is able to receive a secured CAM where the header fields 'signer_info' 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
  and the IUT current time is inside the time validity period of CERT_TS_A_AT
  and the IUT is sending CAMs
ensure that
  when
    the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)
      containing header_fields[0].type
        indicating 'generation_time'
      and containing header_fields[1].type
        indicating 'its_aid'
      and containing header_fields[2].type
        indicating 'signer_info'
      and not containing other header fields
  then
    the IUT discards the SecuredMessage

| TP Id | TP_SEC_ITSS_RCV_CAM_04_04_BO |
|---|---|
| Summary | Check that IUT discards a secured CAM if the header_fields contains more than one header field 'generation_time' |
| Reference | ETSI TS 103 097 [1], clause 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing header_fields[0].type<br>indicating 'signer_info'<br>and containing header_fields[1].type<br>indicating 'generation_time'<br>and containing header_fields[2].type<br>indicating 'generation_time'<br>and containing header_fields[3].type<br>indicating 'its_aid'<br>and not containing other header fields<br>then<br>the IUT discards a SecuredMessage | |

| TP Id | TP_SEC_ITSS_RCV_CAM_04_05_BO |
|---|---|
| Summary | Check that IUT discards a secured CAM if the header_fields does not contain the header field 'generation_time' |
| Reference | ETSI TS 103 097 [1], clause 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing header_fields[0].type<br>indicating 'signer_info'<br>and containing header_fields[1].type<br>indicating 'its_aid'<br>and not containing other header fields<br>then<br>the IUT discards a SecuredMessage | |

| TP Id | 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 header field '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
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)
         containing header_fields[0].type
            indicating 'signer_info'
         and containing header_fields[1].type
            indicating 'generation_time'
         and containing header_fields[2]
            containing type
               indicating 'its_aid'
            and containing its_aid
               indicating 'AID_CAM'
         and containing header_fields[3]
            containing type
               indicating 'its_aid'
            and containing its_aid
               indicating 'AID_DENM'
         and not containing other header fields
   then
      the IUT discards a SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_CAM_04_06a_BO |
|---|---|
| Summary | Check that IUT discards a secured CAM if the header_fields does not contain the header field '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
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)
         containing header_fields[0].type
            indicating 'signer_info'
         and containing header_fields[1].type
            indicating 'generation_time'
         and not containing other header fields
   then
      the IUT discards a SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_CAM_04_07_BO |
|---|---|
| Summary | Check that IUT discards a secured CAM if the header fields are not in the ascending order according to the numbering of the enumeration. |
| Reference | ETSI TS 103 097 [1], clause 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing header_fields[0].type<br>indicating 'signer_info'<br>and containing header_fields[1].type<br>indicating 'its_aid'<br>and containing header_fields[2].type<br>indicating 'generation_time'<br>and not containing other header fields<br>then<br>the IUT discards the SecuredMessage | |

| TP Id | TP_SEC_ITSS_RCV_CAM_04_08_BO |
|---|---|
| Summary | Check that IUT discards the Secured CAM containing the header field 'generation_time_standard_deviation'. |
| Reference | ETSI TS 103 097 [1], clause 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing header_fields[0].type<br>indicating 'signer_info'<br>and containing header_fields[1]<br>containing type<br>indicating 'generation_time'<br>and containing generation_time<br>indicating GEN_TIME inside the validity period of the signer certificate<br>and containing header_fields[2]<br>containing type<br>indicating 'generation_time_with_standard_deviation'<br>and containing generation_time_with_standard_deviation<br>indicating GEN_TIME inside the validity period of the signer certificate<br>and containing header_fields[3].type<br>indicating 'its_aid'<br>and not containing other header fields<br>then<br>the IUT discards the SecuredMessage | |

| TP Id | TP_SEC_ITSS_RCV_CAM_04_10_BO |
|---|---|
| Summary | Check that IUT discards the Secured CAM containing the header field 'expiry_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
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)
         containing header_fields[0].type
            indicating 'signer_info'
         and containing header_fields[1]
            containing type
               indicating 'generation_time'
            containing generation_time
               indicating CURRENT_TIME
         and containing header_fields[2]
            containing type
               indicating 'expiration'
            and containing expiry_time
               indicating CURRENT_TIME + 1h
         and containing header_fields[3].type
            indicating 'its_aid'
         and not containing other header fields
   then
      the IUT discards the SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_CAM_04_11_BO |
|---|---|
| Summary | Check that IUT discards the Secured CAM containing the header field 'generation_location' |
| 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 current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)
         containing header_fields[0]
            containing type
               indicating 'signer_info'
            and containing signer
               containing type
                  indicating certificate
               and containing certificate (CERT_TS_B_AT)
                  containing validity_restrictions['region']
                     containing region (X_CERT_REGION)
         and containing header_fields[1].type
            indicating 'generation_time'
         and containing header_fields[2]
            containing type
               indicating 'generation_location'
            and containing generation_location
               indicating position outside of the validity restriction of X_CERT_REGION
         and containing header_fields[3].type
            indicating 'its_aid'
         and not containing other header fields
   then
      the IUT discards the SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_CAM_04_12_BV |
|---|---|
| Summary | Check that IUT accepts the Secured CAM containing additional non-standard HeaderField |
| 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 current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)
         containing header_fields[0].type
            indicating 'signer_info'
         and containing header_fields[1].type
            indicating 'generation_time'
         and containing header_fields[2].type
            indicating 'its_aid'
         and containing header_fields[3]
            containing type
               indicating non-standard header field type (1000)
            and containing other_header
               indicating non-empty data
         and not containing other header fields
   then
      the IUT accepts the SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_CAM_04_13_BO |
|---|---|
| Summary | Check that IUT discards the Secured CAM containing the header field 'encryption_parameter' and 'recipient_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 with CERT_IUT_A_AT
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)
         containing header_fields[0].type
            indicating 'signer_info'
         and containing header_fields[1].type
            indicating 'generation_time'
         and containing header_fields[2].type
            indicating 'its_aid'
         and containing header_fields[3]
            containing type
               indicating 'encryption_parameters'
            and containing enc_params
               containing symm_algorithm
                  indicating 'aes_128_ccm'
               and containing nonce
         and containing header_fields[4]
            containing type
               indicating 'recipient_info'
            and containing recipients
               containing recipients[0]
                  containing cert_id
                     referencing to CERT_IUT_A_AT
                  and containing pk_encryption
                     indicating 'ecies_nistp256'
                  and containing enc_key
         and not containing other header fields
   then
      the IUT discards the SecuredMessage
```

### 5.3.2.4 Check signer info

| 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** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing header_fields['signer_info']<br>containing signer.type<br>indicating 'self'<br>then<br>the IUT discards a SecuredMessage | |

| TP Id | TP_SEC_ITSS_RCV_CAM_05_02_BO |
|---|---|
| Summary | Check that IUT discards a secured CAM if the header_fields contains a signer of type certificate_digest_with_other_algorithm |
| Reference | ETSI TS 103 097 [1], clause 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_02)<br>containing header_fields['signer_info']<br>containing signer.type<br>indicating 'certificate_digest_with_other_algorithm'<br>then<br>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** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_03)<br>containing header_fields['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate_chain'<br>and containing certificates<br>indicating length = 0<br>then<br>the IUT discards a SecuredMessage | |

| TP Id | TP_SEC_ITSS_RCV_CAM_05_04_BO |
|---|---|
| Summary | Check that IUT discards a secured CAM if the header_fields contains a signer of type certificate_chain and the chain contains only one certificate |
| Reference | ETSI TS 103 097 [1], clause 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_03))<br>containing header_fields['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate_chain'<br>and containing certificates<br>indicating length = 1<br>then<br>the IUT discards a SecuredMessage | |

| TP Id | TP_SEC_ITSS_RCV_CAM_05_05_BO |
|---|---|
| Summary | Check that IUT discards a secured CAM if the header_fields contains a signer info of unknown or reserved type |
| Reference | ETSI TS 103 097 [1], clause 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_02)<br>containing header_fields['signer_info']<br>containing signer.type<br>indicating X_UNKNOWN_SIGNERINFO_TYPE<br>then<br>the IUT discards a SecuredMessage | |
| NOTE: Values to be used as X_UNKNOWN_SIGNERINFO_TYPE are 5, 239, 240 and 255. | |

### 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** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing header_fields['signer_info'].signer<br>containing certificate (CERT_TS_MSG_06_01_BO_AT)<br>containing validity_restrictions['time_start_and_end']<br>containing start_validity<br>indicating START_VALIDITY_AT<br>and containing end_validity<br>indicating END_VALIDITY_AT<br>and containing header_fields ['generation_time']<br>containing generation_time<br>indicating GEN_TIME < START_VALIDITY_AT<br>then<br>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<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing header_fields['signer_info'].signer<br>containing certificate (CERT_TS_MSG_06_02_BO_AT)<br>containing validity_restrictions['time_start_and_end']<br>containing start_validity<br>indicating START_VALIDITY_AT<br>and containing end_validity<br>indicating END_VALIDITY_AT<br>and containing header_fields ['generation_time']<br>containing generation_time<br>indicating GEN_TIME > END_VALIDITY_AT<br>then<br>the IUT discards the message | |

### 5.3.2.6 Check its_aid

| **TP Id** | TP_SEC_ITSS_RCV_CAM_07_01_BO |
|---|---|
| **Summary** | Check that IUT discards secured CAM when its_aid value is defined but not the AID_CAM |
| **Reference** | ETSI TS 103 097 [1], clause 7.1 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing header_fields['its_aid']<br>indicating 'AID_DENM'<br>and containing payload_field<br>containing type<br>indicating 'signed'<br>and containing data<br>containing CAM payload<br>then<br>the IUT discards the message | |

| **TP Id** | TP_SEC_ITSS_RCV_CAM_07_02_BO |
|---|---|
| **Summary** | Check that IUT discards secured CAM when its_aid value is undefined |
| **Reference** | ETSI TS 103 097 [1], clause 7.1 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing header_fields['its_aid']<br>indicating 'AID_UNDEFINED'<br>and containing payload_field<br>containing type<br>indicating 'signed'<br>and containing data<br>containing CAM payload<br>then<br>the IUT discards the message | |

### 5.3.2.7 Check payload

| TP Id | 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 | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing payload_field<br>containing type<br>indicating 'signed'<br>and containing data<br>indicating length 0<br>then<br>the IUT discards the message | |

| 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<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing payload_field<br>containing type<br>indicating 'unsecured'<br>and containing data<br>indicating length > 0<br>then<br>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 | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing payload_field<br>containing type<br>indicating 'encrypted'<br>and containing data<br>indicating length > 0<br>then<br>the IUT discards the message | |

| TP Id | 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<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing payload_field<br>containing type<br>indicating 'signed_external'<br>and containing data<br>indicating length > 0<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_CAM_09_06_BO |
|---|---|
| Summary | Check that IUT discards the Secured CAM containing non-empty payload of type 'signed_and_encrypted' |
| Reference | ETSI TS 103 097 [1], clause 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing payload_field<br>containing type<br>indicating 'signed_and_encrypted'<br>and containing data<br>indicating length > 0<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_CAM_09_07_BO |
|---|---|
| Summary | Check that IUT discards the Secured CAM containing non-empty payload of unknown type |
| Reference | ETSI TS 103 097 [1], clause 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing payload_field<br>containing type<br>indicating X_UNKNOWN_PAYLOAD_TYPE<br>and containing data<br>indicating length > 0<br>then<br>the IUT discards the message | |
| NOTE: Proposed values to be used as X_UNKNOWN_PAYLOAD_TYPE are 5 and 255. | |

### 5.3.2.8 Check presence of trailer field

| TP Id | 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<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing trailer_fields<br>not containing any instance of type TrailerField<br>containing type<br>indicating 'signature'<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_CAM_10_02_BO |
|---|---|
| Summary | Check that IUT discards the Secured CAM containing more than one instance of TrailerField of type 'signature' |
| Reference | ETSI TS 103 097 [1], clause 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing trailer_fields[0]<br>containing type<br>indicating 'signature'<br>and containing trailer_fields[1]<br>containing type<br>indicating 'signature'<br>then<br>the IUT discards the message | |

### 5.3.2.9 Check signature

| TP Id | TP_SEC_ITSS_RCV_CAM_11_01_BO |
|---|---|
| Summary | Check that the IUT discards Secured 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], clauses 4.2.2 and 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| **Expected behaviour** | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)
         containing header_fields ['signer_info'].signer
            containing certificate
               containing subject_attributes['verification key']
                  containing key (KEY)
         and containing trailer_fields[0]
            containing type
               indicating 'signature'
            and containing signature
               NOT verifiable using KEY
   then
      the IUT discards the message
```

| 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], clauses 4.2.2 and 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| **Expected behaviour** | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_02)
         containing header_fields ['signer_info'].signer
            containing digest
               referencing to the certificate (CERT_TS_A_AT)
                  containing subject_attributes['verification key']
                     containing key (KEY)
         and containing trailer_fields[0]
            containing type
               indicating 'signature'
            and containing signature
               NOT verifiable using KEY
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_CAM_11_03_BO |
|---|---|
| Summary | Check that IUT discards the Secured CAM if the message contains trailer field of type 'signature' with reserved public key algorythms |
| Reference | ETSI TS 103 097 [1], clauses 4.2.2 and 7.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing trailer_fields<br>containing an instance of type TrailerField<br>containing type<br>indicating 'signature'<br>and containing signature.algorithm<br>indicating X_RESERVED_PK_ALGORYTHM<br>then<br>the IUT discards the message | |
| NOTE: Values to be provided as X_RESERVED_PK_ALGORYTHM are: 240, 255. | |

### 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], clause 6.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>containing certificate (CERT_TS_A_EC)<br>containing subject_info.subject_type<br>indicating 'enrolment_credentials'<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_CAM_12_02_BO |
|---|---|
| Summary | Check that IUT discards a Secured CAM if the signer certificate of the message contains the subject type 'authorization_authority' |
| 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 current time is inside the time validity period of CERT_TS_A_AT
ensure that
  when
    the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)
      containing header_fields ['signer_info']
        containing signer
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_A_AA)
            containing subject_info.subject_type
              indicating 'authorization_authority'
  then
    the IUT discards the message

| TP Id | TP_SEC_ITSS_RCV_CAM_12_03_BO |
|---|---|
| Summary | Check that IUT discards a Secured CAM if the signer certificate of the message contains the subject type 'enrolment_authority' |
| 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 current time is inside the time validity period of CERT_TS_A_AT
ensure that
  when
    the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)
      containing header_fields ['signer_info']
        containing signer
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_A_EA)
            containing subject_info.subject_type
              indicating 'enrolment_authority'
  then
    the IUT discards the message

| TP Id | TP_SEC_ITSS_RCV_CAM_12_04_BO |
|---|---|
| Summary | Check that IUT discards a Secured CAM if the signer certificate of the message contains the subject type 'root_ca' |
| Reference | ETSI TS 103 097 [1], clause 6.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>containing certificate (CERT_TS_ROOT)<br>containing subject_info.subject_type<br>indicating 'root_ca'<br>then<br>the IUT discards the message | |

### 5.3.2.11 Check certificate validity

| TP Id | TP_SEC_ITSS_RCV_CAM_13_01_BO |
|---|---|
| Summary | Check that IUT discards secured CAM signed with the not yet valid certificate |
| Reference | ETSI TS 103 097 [1], clause 6.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is before the time validity period of CERT_TS_MSG_13_01_BO_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)<br>containing header_fields['signer_info'].signer<br>containing certificate (CERT_TS_MSG_13_01_BO_AT)<br>containing validity_restrictions['time_start_and_end']<br>containing start_validity<br>indicating START_VALIDITY_AT > CURRENT_TIME<br>and containing end_validity<br>indicating END_VALIDITY_AT > START_VALIDITY_AT<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_CAM_13_02_BO |
|---|---|
| Summary | Check that IUT discards secured CAM signed with the expired certificate |
| Reference | ETSI TS 103 097 [1], clause 6.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is before the time validity period of CERT_TS_MSG_13_02_BO_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)
         containing header_fields['signer_info'].signer
            containing certificate (CERT_TS_MSG_13_02_BO_AT)
               containing validity_restrictions['time_start_and_end']
                  containing start_validity
                     indicating START_VALIDITY_AT < CURRENT_TIME
                  and containing end_validity
                     indicating END_VALIDITY_AT < CURRENT_TIME
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_CAM_13_03_BO |
|---|---|
| Summary | Check that IUT discards secured CAM when IUT location is outside the circular validity restriction of the signing certificate |
| Reference | ETSI TS 103 097 [1], clause 6.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the validity period of CERT_TS_MSG_13_03_BO_AT
   and the IUT current location is set to CURRENT_IUT_LOCATION
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)
         containing header_fields['signer_info'].signer
            containing certificate (CERT_TS_MSG_13_03_BO_AT)
               containing validity_restrictions['region']
                  containing region
                     containing region_type
                        indicating 'circle'
                     and containing circular_region
                        indicating REGION
                           not containing the CURRENT_IUT_LOCATION
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_CAM_13_04_BO |
|---|---|
| Summary | Check that IUT discards secured CAM when IUT location is outside the rectangular validity restriction of the signing certificate |
| Reference | ETSI TS 103 097 [1], clause 6.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

with
the IUT being in the 'authorized' state
and the IUT current time is inside the validity period of CERT_TS_MSG_13_04_BO_AT
and the IUT current location is set to CURRENT_IUT_LOCATION
ensure that
when
the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)
containing header_fields['signer_info'].signer
containing certificate (CERT_TS_MSG_13_04_BO_AT)
containing validity_restrictions['region']
containing region
containing region_type
indicating 'rectangle'
and containing rectangular_regions
indicating REGION
not containing the CURRENT_IUT_LOCATION
then
the IUT discards the message

| TP Id | TP_SEC_ITSS_RCV_CAM_13_05_BO |
|---|---|
| Summary | Check that IUT discards secured CAM when IUT location is outside the polygonal validity restriction of the signing certificate |
| Reference | ETSI TS 103 097 [1], clause 6.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

with
the IUT being in the 'authorized' state
and the IUT current time is inside the validity period of CERT_TS_MSG_13_05_BO_AT
and the IUT current location is set to CURRENT_IUT_LOCATION
ensure that
when
the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)
containing header_fields['signer_info'].signer
containing certificate (CERT_TS_MSG_13_05_BO_AT)
containing validity_restrictions['region']
containing region
containing region_type
indicating 'polygon'
and containing polygonal_region
indicating REGION
not containing the CURRENT_IUT_LOCATION
then
the IUT discards the message

| TP Id | TP_SEC_ITSS_RCV_CAM_13_06_BO |
|---|---|
| Summary | Check that IUT discards secured CAM when IUT location is outside the identified validity restriction of the signing certificate |
| Reference | ETSI TS 103 097 [1], clause 6.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

with
the IUT being in the 'authorized' state
and the IUT current time is inside the validity period of CERT_TS_MSG_13_06_BO_AT
and the IUT current location is set to CURRENT_IUT_LOCATION
ensure that
when
the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)
containing header_fields['signer_info'].signer
containing certificate (CERT_TS_MSG_13_06_BO_AT)
containing validity_restrictions['region']
containing region
containing region_type
indicating 'id'
and containing id_region
indicating REGION
not containing the CURRENT_IUT_LOCATION
then
the IUT discards the message

## 5.3.3 DENM Profile

### 5.3.3.1 Check that IUT accepts well-formed Secured DENM

| **TP Id** | TP_SEC_ITSS_RCV_DENM_01_01_BV |
|---|---|
| **Summary** | Check that IUT accepts a well-formed Secured DENM signed with the certificate without 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
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
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_A_AT)
                  containing subject_info.subject_type
                     indicating 'authorization_ticket'
                  and containing subject_attributes['verification key']
                     containing key (KEY)
                  and not containing validity_restrictions['region']
         and containing header_fields [1]
            containing type
               indicating 'generation_time'
            and containing generation_time
               indicating CURRENT_TIME
         and containing header_fields [2]
            containing type
               indicating 'generation_location'
            and containing generation_location
         and containing header_fields[3]
            containing type
               indicating 'its_aid'
            and containing its_aid
               indicating 'AID_DENM'
         and containing payload_field
            containing type
               indicating 'signed'
            and containing data
               indicating length > 0
               and containing DENM payload
         and containing trailer_fields
            containing single instance of type TrailerField
               containing type
                  indicating 'signature'
               and containing signature
                  verifiable using KEY
   then
      the IUT accepts the message
```

NOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name 'MSG_SEC_RCV_DENM_A'. Only differences to this snippet are mentioned in subsequent test purposes.

| **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
   and the IUT current time is inside the time validity period of CERT_TS_B_AT
   and the IUT current location is inside the region validity period of CERT_TS_B_AT
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_TS_B_AT)
                  containing subject_info.subject_type
                     indicating 'authorization_ticket'
                  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'
            and containing generation_time
               indicating CURRENT_TIME
         and containing header_fields [2]
            containing type
               indicating 'generation_location'
            and containing generation_location
               indicating position inside the REGION
         and containing header_fields[3]
            containing type
               indicating 'its_aid'
            and containing its_aid
               indicating 'AID_DENM'
         and not containing any other header_fields
         and containing payload_fields
            containing type
               indicating 'signed'
            and containing data
               indicating length > 0
               and containing DENM payload
         and containing trailer_fields
            containing single instance of type TrailerField
               containing type
                  indicating 'signature'
               and containing signature
                  verifiable using KEY
   then
      the IUT accepts the message
```

NOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name 'MSG_SEC_RCV_DENM_B'. Only differences to this snippet are mentioned in subsequent test purposes.

| 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
   and the IUT current time is inside the time validity period of CERT_TS_C_AT
   and the IUT current location is inside the region validity period of CERT_TS_C_AT
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_C_AT)
                  containing subject_info.subject_type
                     indicating 'authorization_ticket'
                  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'
            and containing generation_time
               indicating CURRENT_TIME
         and containing header_fields [2]
            containing type
               indicating 'generation_location'
            and containing generation_location
               indicating position inside the REGION
         and containing header_fields[3]
            containing type
               indicating 'its_aid'
            and containing its_aid
               indicating 'AID_DENM'
         and not containing any other header_fields
         and containing payload_field
            containing type
               indicating 'signed'
            and containing data
               indicating length > 0
               and containing DENM payload
         and containing trailer_fields
            containing single instance of type TrailerField
               containing type
                  indicating 'signature'
               and containing signature
                  verifiable using KEY
   then
      the IUT accepts the message
```

NOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name 'MSG_SEC_RCV_DENM_C'. Only differences to this snippet are mentioned in subsequent test purposes.

| 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
   and the IUT current time is inside the time validity period of CERT_TS_D_AT
   and the IUT current location is inside the region validity period of CERT_TS_D_AT
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_D_AT)
                  containing subject_info.subject_type
                     indicating 'authorization_ticket'
                  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'
            and containing generation_time
               indicating CURRENT_TIME
         and containing header_fields [2]
            containing type
               indicating 'generation_location'
            and containing generation_location
               indicating position inside the REGION
         and containing header_fields[3]
            containing type
               indicating 'its_aid'
            and containing its_aid
               indicating 'AID_DENM'
         and not containing any other header_fields
         and containing payload_field
            containing type
               indicating 'signed'
            and containing data
               indicating length > 0
               and containing DENM payload
         and containing trailer_fields
            containing single instance of type TrailerField
               containing type
                  indicating 'signature'
               and containing signature
                  verifiable using KEY
   then
      the IUT accepts the message
```

NOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name 'MSG_SEC_RCV_DENM_D'. Only differences to this snippet are mentioned in subsequent test purposes.

| **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
   and the IUT current time is inside the time validity period of CERT_TS_E_AT
   and the IUT current location is inside the region validity period of CERT_TS_E_AT
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_E_AT)
                  containing subject_info.subject_type
                     indicating 'authorization_ticket'
                  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'
            and containing generation_time
               indicating CURRENT_TIME
         and containing header_fields [2]
            containing type
               indicating 'generation_location'
            and containing generation_location
               indicating position inside the REGION
         and containing header_fields[3]
            containing type
               indicating 'its_aid'
            and containing its_aid
               indicating 'AID_DENM'
         and not containing any other header_fields
         and containing payload_field
            containing type
               indicating 'signed'
            and containing data
               indicating length > 0
               and containing DENM payload
         and containing trailer_fields
            containing single instance of type TrailerField
               containing type
                  indicating 'signature'
               and containing signature
                  verifiable using KEY
   then
      the IUT accepts the message
```

NOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name 'MSG_SEC_RCV_DENM_E'. Only differences to this snippet are mentioned in subsequent test purposes.

### 5.3.3.2 Check the message protocol version

| TP Id | 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 5.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing protocol_version<br>indicating 1<br>then<br>the IUT discards a SecuredMessage | |

| TP Id | 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 5.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing protocol_version<br>indicating 3<br>then<br>the IUT discards a SecuredMessage | |

### 5.3.3.3 Check header fields

| TP Id | TP_SEC_ITSS_RCV_DENM_04_01_BO |
|---|---|
| Summary | Check that IUT discards a secured DENM if the message contains more than one header field of type 'signer_info' |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing header_fields[0].type<br>indicating 'signer_info'<br>and containing header_fields[1].type<br>indicating 'signer_info'<br>and containing header_fields[2].type<br>indicating 'generation_time'<br>and containing header_fields[3].type<br>indicating 'generation_location'<br>and containing header_fields[4].type<br>indicating 'its_aid'<br>and not containing other header fields<br>then<br>the IUT discards the SecuredMessage | |

| TP Id | TP_SEC_ITSS_RCV_DENM_04_02_BO |
|---|---|
| Summary | Check that IUT discards a secured DENM if the message does not contain the header field of 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
  and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
  when
    the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)
      containing header_fields[0].type
        indicating 'generation_time'
      and containing header_fields[1].type
        indicating 'generation_location'
      and containing header_fields[2].type
        indicating 'its_aid'
      and not containing other header fields
  then
    the IUT discards a SecuredMessage

| TP Id | TP_SEC_ITSS_RCV_DENM_04_03_BO |
|---|---|
| Summary | Check that IUT discards the Secured DENM if the signer_info header field is not encoded first |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

with
  the IUT being in the 'authorized' state
  and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
  when
    the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)
      containing header_fields[0].type
        indicating 'generation_time'
      and containing header_fields[1].type
        indicating 'generation_location'
      and containing header_fields[2].type
        indicating 'its_aid'
      and containing header_fields[3].type
        indicating 'signer_info'
      and not containing other header fields
  then
    the IUT discards the SecuredMessage

| TP Id | TP_SEC_ITSS_RCV_DENM_04_04_BO |
|---|---|
| Summary | Check that IUT discards a secured DENM if the message contains more than one header field of type '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
  and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
  when
    the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)
      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].type
        indicating 'its_aid'
      and not containing other header fields
  then
    the IUT discards a SecuredMessage

| TP Id | TP_SEC_ITSS_RCV_DENM_04_05_BO |
|---|---|
| Summary | Check that IUT discards a secured DENM if the message does not contain the header field of type '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
  and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
  when
    the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)
      containing header_fields[0].type
        indicating 'signer_info'
      containing header_fields[1].type
        indicating 'generation_location'
      and containing header_fields[2].type
        indicating 'its_aid'
      and not containing other header fields
  then
    the IUT discards a SecuredMessage

| TP Id | TP_SEC_ITSS_RCV_DENM_04_06_BO |
|---|---|
| Summary | Check that IUT discards a secured DENM if the message contains more than one header field of type 'its_aid' |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)
         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_DENM'
         and not containing other header fields
   then
      the IUT discards a SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_DENM_04_06a_BO |
|---|---|
| Summary | Check that IUT discards a secured DENM if the message does not contain the header field of type 'its_aid' |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)
         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 not containing other header fields
   then
      the IUT discards a SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_DENM_04_07_BO |
|---|---|
| Summary | Check that IUT discards a secured DENM if the message contains more than one 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
and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
when
the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)
containing header_fields[0].type
indicating 'signer_info'
and containing header_fields[1].type
indicating 'generation_time'
and containing header_fields[2]
containing type
indicating 'generation_location'
and containing generation_location
indicating X_LOCATION
and containing header_fields[3]
containing type
indicating 'generation_location'
and containing generation_location
indicating X_LOCATION
and containing header_fields[4].type
indicating 'its_aid'
and not containing other header fields
then
the IUT discards a SecuredMessage

| TP Id | TP_SEC_ITSS_RCV_DENM_04_08_BO |
|---|---|
| Summary | Check that IUT discards a secured DENM if the message does not contain the 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
and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
when
the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)
containing header_fields[0].type
indicating 'signer_info'
containing header_fields[1].type
indicating 'generation_time'
and containing header_fields[2].type
indicating 'its_aid'
and not containing other header fields
then
the IUT discards a SecuredMessage

| TP Id | TP_SEC_ITSS_RCV_DENM_04_09_BO |
|---|---|
| Summary | Check that IUT discards a Secured DENM if the header fields are not in the ascending order according to the numbering of the enumeration. |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)
         containing header_fields[0].type
            indicating 'signer_info'
         and containing header_fields[1].type
            indicating 'its_aid'
         and containing header_fields[2].type
            indicating 'generation_time'
         and containing header_fields[3].type
            indicating 'generation_location'
   then
      the IUT discards the SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_DENM_04_10_BO |
|---|---|
| Summary | Check that IUT discards a Secured DENM containing header field of type 'generation_time_standard_deviation' |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)
         containing header_fields[0].type
            indicating 'signer_info'
         and containing header_fields[1].type
            indicating 'generation_time'
         and containing header_fields[2]
            containing type
               indicating 'generation_time_standard_deviation'
            and containing generation_time_with_standard_deviation
               containing time
                  indicating CURRENT_TIME
               and containing log_std_dev
                  indicating 255
         and containing header_fields[3].type
            indicating 'generation_location'
         and containing header_fields[4].type
            indicating 'its_aid'
   then
      the IUT discards a SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_DENM_04_11_BO |
|---|---|
| Summary | Check that IUT discards the Secured DENM containing the header fields of type 'expiry_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
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)
         containing header_fields[0].type
            indicating 'signer_info'
         and containing header_fields[1]
            containing type
               indicating 'generation_time'
            containing generation_time
               indicating CURRENT_TIME
         and containing header_fields[2]
            containing type
               indicating 'expiration'
            and containing expiry_time
               indicating CURRENT_TIME + 1 h
         and containing header_fields[3].type
            indicating 'generation_location'
         and containing header_fields[4].type
            indicating 'its_aid'
         and not containing other header fields
   then
      the IUT discards the SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_DENM_04_12_BV |
|---|---|
| Summary | Check that IUT accepts the Secured DENM containing additional non-standard HeaderField |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)
         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 'its_aid'
         and containing header_fields[4]
            containing type
               indicating non-standard header field type (1000)
            and containing other_header
               indicating non-empty data
         and not containing other header fields
   then
      the IUT accepts the SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_DENM_04_13_BO |
|---|---|
| Summary | Check that IUT discards the Secured CAM containing the header field 'encryption_parameter' and 'recipient_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 with CERT_IUT_A_AT
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)
         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 'its_aid'
         and containing header_fields[4]
            containing type
               indicating 'encryption_parameters'
            and containing enc_params
               containing symm_algorithm
                  indicating 'aes_128_ccm'
               and containing nonce
         and containing header_fields[5]
            containing type
               indicating 'recipient_info'
            and containing recipients
               containing recipients[0]
                  containing cert_id
                     referencing to CERT_IUT_A_AT
                  and containing pk_encryption
                     indicating 'ecies_nistp256'
                  and containing enc_key
         and not containing other header fields
   then
      the IUT discards the SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_DENM_04_14_BO |
|---|---|
| Summary | Check that IUT discards the Secured DENM containing the header fields of type 'request_unrecognized_certificate' |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state with X_IUT_AT_CERT<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing header_fields[0].type<br>indicating 'signer_info'<br>and containing header_fields[1]<br>containing type<br>indicating 'generation_time'<br>containing generation_time<br>indicating CURRENT_TIME<br>and containing header_fields[2]<br>containing type<br>indicating 'request_unrecognized_certificate'<br>and containing digests[0]<br>indicating the digest of X_IUT_AT_CERT<br>and containing header_fields[3].type<br>indicating 'generation_location'<br>and containing header_fields[4].type<br>indicating 'its_aid'<br>and not containing other header fields<br>then<br>the IUT discards the SecuredMessage | |
| NOTE: X_IUT_AT_CERT - Any valid AT certificate has been used to authorize IUT. | |

### 5.3.3.4 Check signer info

| TP Id | 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 | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing header_fields['signer_info']<br>containing signer.type<br>indicating 'self'<br>then<br>the IUT discards a SecuredMessage | |

| TP Id | TP_SEC_ITSS_RCV_DENM_05_02_BO |
|---|---|
| Summary | Check that IUT discards a Secured DENM if the header_fields contains a signer of type 'certificate_digest_with_other_algorithm' |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing header_fields['signer_info']<br>containing signer.type<br>indicating 'certificate_digest_with_other_algorithm'<br>then<br>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 | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing header_fields['signer_info']<br>containing signer.type<br>indicating 'certificate_chain'<br>then<br>the IUT discards a SecuredMessage | |

| TP Id | TP_SEC_ITSS_RCV_DENM_05_04_BO |
|---|---|
| Summary | Check that IUT discards a secured DENM if the header_fields contains a signer info of unknown or reserved type |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing header_fields['signer_info']<br>containing signer.type<br>indicating X_UNKNOWN_SIGNERINFO_TYPE<br>then<br>the IUT discards a SecuredMessage | |
| NOTE: Values to be used as X_UNKNOWN_SIGNERINFO_TYPE are 5, 239, 240 and 255. | |

### 5.3.3.5 Check generation time

| TP Id | TP_SEC_ITSS_RCV_DENM_06_01_BO |
|---|---|
| Summary | Check that IUT discards a Secured DENM 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 | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)
         containing header_fields['signer_info']
               containing certificate (CERT_TS_MSG_06_01_BO_AT)
                  containing validity_restrictions['time_start_and_end']
                     containing start_validity
                        indicating START_VALIDITY_AT
                     and containing end_validity
                        indicating END_VALIDITY_AT
         and containing header_fields ['generation_time']
            containing generation_time
               indicating GEN_TIME < START_VALIDITY_AT
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_DENM_06_02_BO |
|---|---|
| Summary | Check that IUT discards a Secured DENM 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 | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)
         containing header_fields['signer_info']
               containing certificate (CERT_TS_MSG_06_02_BO_AT)
                  containing validity_restrictions['time_start_and_end']
                     containing start_validity
                        indicating START_VALIDITY_AT
                     and containing end_validity
                        indicating END_VALIDITY_AT
         and containing header_fields ['generation_time']
            containing generation_time
               indicating GEN_TIME > END_VALIDITY_AT
   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 a 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** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing header_fields['its_aid']<br>indicating 'AID_CAM'<br>and containing payload_field<br>containing type<br>indicating 'signed'<br>and containing data<br>containing DENM payload<br>then<br>the IUT discards the DENM message | |

| **TP Id** | TP_SEC_ITSS_RCV_DENM_07_02_BO |
|---|---|
| **Summary** | Check that IUT discards a Secured DENM when its_aid value is undefined |
| **Reference** | ETSI TS 103 097 [1], clause 7.2 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing header_fields['its_aid']<br>indicating 'AID_UNDEFINED'<br>and containing payload_field<br>containing type<br>indicating 'signed'<br>and containing data<br>containing DENM payload<br>then<br>the IUT discards the message | |

### 5.3.3.7 Check generation location

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

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

| TP Id | TP_SEC_ITSS_RCV_DENM_08_03_BO |
|---|---|
| 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 AND 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
                  containing region_type
                     indicating 'polygon'
                  and 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
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_DENM_08_04_BO |
|---|---|
| Summary | Check that IUT discards Secured DENM if the HeaderField generation_location is outside of the identified validity region of the signing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY AND 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'].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 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<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing payload_field<br>containing type<br>indicating 'signed'<br>and containing data<br>indicating length 0<br>then<br>the IUT discards the message | |

| **TP Id** | TP_SEC_ITSS_RCV_DENM_09_03_BO |
|---|---|
| **Summary** | Check that IUT discards the Secured DENM containing payload of type 'unsecured' |
| **Reference** | ETSI TS 103 097 [1], clause 7.2 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing payload_field<br>containing type<br>indicating 'unsecured'<br>and containing data<br>indicating length > 0<br>then<br>the IUT discards the message | |

| **TP Id** | TP_SEC_ITSS_RCV_DENM_09_04_BO |
|---|---|
| **Summary** | Check that IUT discards the Secured DENM containing payload of type 'encrypted' |
| **Reference** | ETSI TS 103 097 [1], clause 7.2 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing payload_field<br>containing type<br>indicating 'encrypted'<br>and containing data<br>indicating length > 0<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_DENM_09_05_BO |
|---|---|
| Summary | Check that IUT discards the Secured DENM containing payload of type 'signed_external' |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing payload_field<br>containing type<br>indicating 'signed_external'<br>and containing data<br>indicating length > 0<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_DENM_09_06_BO |
|---|---|
| Summary | Check that IUT discards the Secured DENM containing exactly one non-empty payload of type 'signed_and_encrypted' |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing payload_field<br>containing type<br>indicating 'signed_and_encrypted'<br>and containing data<br>indicating length > 0<br>then<br>the IUT discards the message | |

### 5.3.3.9 Check presence of trailer field

| TP Id | TP_SEC_ITSS_RCV_DENM_10_01_BO |
|---|---|
| Summary | Check that IUT discards the Secured DENM if the message does not contain the trailer field of type signature |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing trailer_fields<br>not containing trailer_fields['signature']<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_DENM_10_02_BO |
|---|---|
| Summary | Check that IUT discards the Secured DENM containing more than one instance of TrailerField of type 'signature' |
| Reference | ETSI TS 103 097 [1], clause 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing trailer_fields[0]<br>containing type<br>indicating 'signature'<br>and containing trailer_fields[1]<br>containing type<br>indicating 'signature'<br>then<br>the IUT discards the message | |

### 5.3.3.10 Check signature

| TP Id | TP_SEC_ITSS_RCV_DENM_11_01_BO |
|---|---|
| Summary | 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 |
| Reference | ETSI TS 103 097 [1], clauses 4.2.2 and 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing header_fields ['signer_info']<br>containing signer<br>containing certificate (CERT_TS_A_AT)<br>containing subject_attributes['verification key']<br>containing key (KEY)<br>and containing trailer_fields[0]<br>containing type<br>indicating 'signature'<br>containing signature<br>NOT verifiable using KEY<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_DENM_11_02_BO |
|---|---|
| Summary | Check that IUT discards the Secured DENM if the message contains trailer field of type 'signature' with reserved public key algorythms |
| Reference | ETSI TS 103 097 [1], clauses 4.2.2 and 7.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing trailer_fields<br>containing an instance of type TrailerField<br>containing type<br>indicating 'signature'<br>and containing signature.algorithm<br>indicating X_RESERVED_PK_ALGORYTHM<br>then<br>the IUT discards the message | |
| NOTE: Values to be provided as X_RESERVED_PK_ALGORYTHM are: 240, 255. | |

### 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 6.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage<br>containing header_fields ['signer_info']<br>containing signer.type<br>indicating 'certificate'<br>containing signer.certificate (CERT_TS_EA_A)<br>containing subject_info.subject_type<br>indicating 'enrolment_credentials'<br>containing header_fields['its_aid']<br>indicating 'AID_DENM'<br>then<br>the IUT discards the message | |

| 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 6.3 |
| 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 ['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_DENM'
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_DENM_12_03_BO |
|---|---|
| Summary | Check that IUT discards a Secured DENM if the signer certificate of the message contains the subject type 'enrolment_authority' |
| 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 current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)
         containing header_fields ['signer_info']
            containing signer
               containing type
                  indicating 'certificate'
               containing certificate (CERT_TS_A_EA)
                  containing subject_info.subject_type
                     indicating 'enrolment_authority'
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_DENM_12_04_BO |
|---|---|
| Summary | Check that IUT discards a Secured DENM if the signer certificate of the message contains the subject type 'root_ca' |
| Reference | ETSI TS 103 097 [1], clause 6.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>containing certificate (CERT_TS_ROOT)<br>containing subject_info.subject_type<br>indicating 'root_ca'<br>then<br>the IUT discards the message | |

### 5.3.3.12 Check certificate validity

| TP Id | TP_SEC_ITSS_RCV_DENM_13_01_BO |
|---|---|
| Summary | Check that IUT discards secured DENM signed with the not yet valid certificate |
| Reference | ETSI TS 103 097 [1], clause 6.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is before the time validity period of CERT_TS_MSG_13_01_BO_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing header_fields['signer_info'].signer<br>containing certificate (CERT_TS_MSG_13_01_BO_AT)<br>containing validity_restrictions['time_start_and_end']<br>containing start_validity<br>indicating START_VALIDITY_AT > CURRENT_TIME<br>and containing end_validity<br>indicating END_VALIDITY_AT > START_VALIDITY_AT<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_DENM_13_02_BO |
|---|---|
| Summary | Check that IUT discards secured DENM signed with the expired certificate |
| Reference | ETSI TS 103 097 [1], clause 6.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is before the time validity period of CERT_TS_MSG_13_02_BO_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)
         containing header_fields['signer_info'].signer
            containing certificate (CERT_TS_MSG_13_02_BO_AT)
               containing validity_restrictions['time_start_and_end']
                  containing start_validity
                     indicating START_VALIDITY_AT < CURRENT_TIME
                  and containing end_validity
                     indicating END_VALIDITY_AT < CURRENT_TIME
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_DENM_13_03_BO |
|---|---|
| Summary | Check that IUT discards secured DENM when IUT location is outside the circular validity restriction of the signing certificate |
| Reference | ETSI TS 103 097 [1], clause 6.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the validity period of CERT_TS_MSG_13_03_BO_AT
   and the IUT current location is set to CURRENT_IUT_LOCATION
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_B)
         containing header_fields['signer_info'].signer
            containing certificate (CERT_TS_MSG_13_03_BO_AT)
               containing validity_restrictions['region']
                  containing region
                     containing region_type
                        indicating 'circle'
                     and containing circular_region
                        indicating REGION
                           not containing the CURRENT_IUT_LOCATION
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_DENM_13_04_BO |
|---|---|
| Summary | Check that IUT discards secured DENM when IUT location is outside the rectangular validity restriction of the signing certificate |
| Reference | ETSI TS 103 097 [1], clause 6.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

with
the IUT being in the 'authorized' state
and the IUT current time is inside the validity period of CERT_TS_MSG_13_04_BO_AT
and the IUT current location is set to CURRENT_IUT_LOCATION
ensure that
when
the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_C)
containing header_fields['signer_info'].signer
containing certificate (CERT_TS_MSG_13_04_BO_AT)
containing validity_restrictions['region']
containing region
containing region_type
indicating 'rectangle'
and containing rectangular_regions
indicating REGION
not containing the CURRENT_IUT_LOCATION
then
the IUT discards the message

| TP Id | TP_SEC_ITSS_RCV_DENM_13_05_BO |
|---|---|
| Summary | Check that IUT discards secured DENM when IUT location is outside the polygonal validity restriction of the signing certificate |
| Reference | ETSI TS 103 097 [1], clause 6.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

with
the IUT being in the 'authorized' state
and the IUT current time is inside the validity period of CERT_TS_MSG_13_05_BO_AT
and the IUT current location is set to CURRENT_IUT_LOCATION
ensure that
when
the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_D)
containing header_fields['signer_info'].signer
containing certificate (CERT_TS_MSG_13_05_BO_AT)
containing validity_restrictions['region']
containing region
containing region_type
indicating 'polygon'
and containing polygonal_region
indicating REGION
not containing the CURRENT_IUT_LOCATION
then
the IUT discards the message

| TP Id | TP_SEC_ITSS_RCV_DENM_13_06_BO |
|---|---|
| Summary | Check that IUT discards secured DENM when IUT location is outside the identified validity restriction of the signing certificate |
| Reference | ETSI TS 103 097 [1], clause 6.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

with
  the IUT being in the 'authorized' state
  and the IUT current time is inside the validity period of CERT_TS_MSG_13_06_BO_AT
  and the IUT current location is set to CURRENT_IUT_LOCATION
ensure that
  when
    the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_E)
      containing header_fields['signer_info'].signer
        containing certificate (CERT_TS_MSG_13_06_BO_AT)
          containing validity_restrictions['region']
            containing region
              containing region_type
                indicating 'id'
              and containing id_region
                indicating REGION
                  not containing the CURRENT_IUT_LOCATION
  then
    the IUT discards 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 |
|---|---|
| **Summary** | Check that IUT accepts a well-formed Secured GN Beacon signed with the certificate without 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
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
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_A_AT)
                  containing subject_info.subject_type
                     indicating 'authorization_ticket'
                  and containing subject_attributes['verification key'] (KEY)
                  and containing validity_restrictions['time_start_and_end']
                     indicating CERT_TS_AT_TIME_VALIDITY
                  and not containing validity_restrictions['region']
         and containing header_fields [1]
            containing type
               indicating 'generation_time'
            and containing generation_time
               indicating CURRENT_TIME
                  inside CERT_TS_AT_TIME_VALIDITY
         and containing header_fields [2]
            containing type
               indicating 'generation_location'
            and containing generation_location
         and containing header_fields[3]
            containing type
               indicating 'its_aid'
            and containing its_aid
               indicating 'AID_BEACON'
         and containing payload_field
            containing type
               indicating 'signed'
            and containing data
               indicating length > 0
         and containing trailer_fields
            containing trailer_fields[0]
               containing type
                  indicating 'signature'
               and containing signature
                  verifiable using KEY
   then
      the IUT accepts the message
```

NOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name 'MSG_SEC_RCV_GENMSG_A'. Only differences to this snippet are mentioned in subsequent test purposes.

| 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
   and the IUT current time is inside the time validity period of CERT_TS_B_AT
   and the IUT current location is inside the region validity period of CERT_TS_B_AT
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_B_AT)
                  containing subject_info.subject_type
                     indicating 'authorization_ticket'
                  and containing subject_attributes['verification key'] (KEY)
                  and containing validity_restrictions['time_start_and_end']
                     indicating CERT_TS_AT_TIME_VALIDITY
                  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'
            and containing generation_time
               indicating CURRENT_TIME
         and containing header_fields [2]
            containing type
               indicating 'generation_location'
            and containing generation_location
               indicating position inside the REGION
         and containing header_fields[3]
            containing type
               indicating 'its_aid'
            and containing its_aid
               indicating 'AID_BEACON'
         and containing payload_field
            containing type
               indicating 'signed'
            and containing data
               indicating length > 0
         and containing trailer_fields
            containing trailer_fields[0]
               containing type
                  indicating 'signature'
               and containing signature
                  verifiable using KEY
   then
      the IUT accepts the message
```

NOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name 'MSG_SEC_RCV_GENMSG_B'. Only differences to this snippet are mentioned in subsequent test purposes.

| 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
   and the IUT current time is inside the time validity period of CERT_TS_C_AT
   and the IUT current location is inside the region validity period of CERT_TS_C_AT
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_C_AT)
                  containing subject_info.subject_type
                     indicating 'authorization_ticket'
                  and containing subject_attributes['verification key'] (KEY)
                  and containing validity_restrictions['time_start_and_end']
                     indicating CERT_TS_AT_TIME_VALIDITY
                  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'
            and containing generation_time
               indicating CURRENT_TIME
         and containing header_fields [2]
            containing type
               indicating 'generation_location'
            and containing generation_location
               indicating position inside the REGION
         and containing header_fields[3]
            containing type
               indicating 'its_aid'
            and containing its_aid
               indicating 'AID_BEACON'
         and containing payload_field
            containing type
               indicating 'signed'
            and containing data
               indicating length > 0
         and containing trailer_fields
            containing trailer_fields[0]
               containing type
                  indicating 'signature'
               containing signature
                  verifiable using KEY
   then
      the IUT accepts the message
```

NOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name 'MSG_SEC_RCV_GENMSG_C'. Only differences to this snippet are mentioned in subsequent test purposes.

| 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
   and the IUT current time is inside the time validity period of CERT_TS_D_AT
   and the IUT current location is inside the region validity period of CERT_TS_D_AT
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_D_AT)
                  containing subject_info.subject_type
                     indicating 'authorization_ticket'
                  and containing subject_attributes['verification key'] (KEY)
                  and containing validity_restrictions['time_start_and_end']
                     indicating CERT_TS_AT_TIME_VALIDITY
                  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'
            and containing generation_time
               indicating CURRENT_TIME
         and containing header_fields [2]
            containing type
               indicating 'generation_location'
            and containing generation_location
               indicating position inside the REGION
         and containing header_fields[3]
            containing type
               indicating 'its_aid'
            and containing its_aid
               indicating 'AID_BEACON'
         and containing payload_field
            containing type
               indicating 'signed'
            and containing data
               indicating length > 0
         and containing trailer_fields
            containing trailer_fields[0]
               containing type
                  indicating 'signature'
               and containing signature
                  verifiable using KEY
   then
      the IUT accepts the message
```

NOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name 'MSG_SEC_RCV_GENMSG_D'. Only differences to this snippet are mentioned in subsequent test purposes.

| 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 Selection | PICS_GN_SECURITY |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_E_AT
   and the IUT current location is inside the region validity period of CERT_TS_E_AT
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_E_AT)
                  containing subject_info.subject_type
                     indicating 'authorization_ticket'
                  and containing subject_attributes['verification key'] (KEY)
                  and containing validity_restrictions['time_start_and_end']
                     indicating CERT_TS_AT_TIME_VALIDITY
                  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'
            and containing generation_time
               indicating CURRENT_TIME
         and containing header_fields [2]
            containing type
               indicating 'generation_location'
            and containing generation_location
               indicating position inside the REGION
         and containing header_fields[3]
            containing type
               indicating 'its_aid'
            and containing its_aid
               indicating 'AID_BEACON'
         and containing payload_field
            containing type
               indicating 'signed'
            and containing data
               indicating length > 0
         and containing trailer_fields
            containing trailer_fields[0]
               containing type
                  indicating 'signature'
               and containing signature
                  verifiable using KEY
   then
      the IUT accepts the message
```

NOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name 'MSG_SEC_RCV_GENMSG_E'. Only differences to this snippet are mentioned in subsequent test purposes.

### 5.3.4.2 Check the message protocol version

| TP Id | 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 5.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing protocol_version<br>indicating 1<br>then<br>the IUT discards a SecuredMessage | |

| TP Id | TP_SEC_ITSS_RCV_GENMSG_02_02_BO |
|---|---|
| Summary | 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 5.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing protocol_version<br>indicating 3<br>then<br>the IUT discards a SecuredMessage | |

### 5.3.4.3 Check header fields

| TP Id | TP_SEC_ITSS_RCV_GENMSG_04_01_BO |
|---|---|
| Summary | Check that IUT discards a secured GN Message if the header_fields contains more than one header field of type 'signer_info' |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing header_fields[0].type<br>indicating 'signer_info'<br>and containing header_fields[1].type<br>indicating 'signer_info'<br>and containing header_fields[2].type<br>indicating 'generation_time'<br>and containing header_fields[3].type<br>indicating 'generation_location'<br>and containing header_fields[4].type<br>indicating 'its_aid'<br>and not containing other header fields<br>then<br>the IUT discards a SecuredMessage | |

| TP Id | TP_SEC_ITSS_RCV_GENMSG_04_02_BO |
|---|---|
| Summary | Check that IUT discards a secured GN Message if the header_fields does not contain the header field of type 'signer_info' |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing header_fields[0].type<br>indicating 'generation_time'<br>and containing header_fields[1].type<br>indicating 'generation_location'<br>and containing header_fields[2].type<br>indicating 'its_aid<br>and not containing other header fields<br>then<br>the IUT discards a SecuredMessage | |

| TP Id | TP_SEC_ITSS_RCV_GENMSG_04_03_BO |
|---|---|
| Summary | Check that IUT is able to receive a secured GN Message if the signer_info header field is not encoded first |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing header_fields[0].type<br>indicating 'generation_time'<br>and containing header_fields[1].type<br>indicating 'generation_location'<br>and containing header_fields[2].type<br>indicating 'its_aid'<br>and containing header_fields[3].type<br>indicating 'signer_info'<br>and not containing other header fields<br>then<br>the IUT discards the SecuredMessage | |

| TP Id | TP_SEC_ITSS_RCV_GENMSG_04_04_BO |
|---|---|
| Summary | Check that IUT discards a secured GN Message if the message contains more than one header field of type 'generation_time' |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

with
the IUT being in the 'authorized' state
and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
when
the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
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].type
indicating 'its_aid'
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 Message 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
the IUT being in the 'authorized' state
and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
when
the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
containing header_fields[0].type
indicating 'signer_info'
and containing header_fields[1].type
indicating 'generation_location'
and containing header_fields[2].type
indicating 'its_aid'
and not containing other header fields
then
the IUT discards a SecuredMessage

| TP Id | TP_SEC_ITSS_RCV_GENMSG_04_06_BO |
|---|---|
| Summary | Check that IUT discards a Secured GN Message if the message contains more than one header field of type 'its_aid' |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
         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_BEACON'
         and containing header_fields[4]
            containing type
               indicating 'its_aid'
            containing 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_06a_BO |
|---|---|
| Summary | Check that IUT discards a secured GN Message if the message does not contain the header field of type 'its_aid' |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
         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 not containing other header fields
   then
      the IUT discards a SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_GENMSG_04_07_BO |
|---|---|
| Summary | Check that IUT discards a secured GN Message if the message contains more than one header field of 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
  and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
  when
    the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
      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 Id | TP_SEC_ITSS_RCV_GENMSG_04_08_BO |
|---|---|
| Summary | Check that IUT discards a secured GN Message if the header_fields contains no element of header field of 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
  and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
  when
    the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
      containing header_fields[0].type
        indicating 'signer_info'
      and containing header_fields[1].type
        indicating 'generation_time'
      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_09_BO |
|---|---|
| Summary | Check that IUT is able to receive a Secured GN Beacon if the header fields are not in the ascending order according to the numbering of the enumeration. |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
         containing header_fields[0].type
            indicating 'signer_info'
         and containing header_fields[1].type
            indicating 'its_aid'
         and containing header_fields[2].type
            indicating 'generation_time'
         and containing header_fields[3].type
            indicating 'generation_location'
   then
      the IUT discards the SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_GENMSG_04_11_BV |
|---|---|
| Summary | Check that IUT accepts a GN Secured Message containing optional header field of type 'expiry_time' |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
         containing header_fields[0].type
            indicating 'signer_info'
            containing signer
               containing certificate
                  indicating CERT_TS_A_AT
         and containing header_fields[1]
            containing type
               indicating 'generation_time'
            containing generation_time
               indicating TIME_1 inside the validity period of CERT_TS_A_AT
         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
```

| TP Id | TP_SEC_ITSS_RCV_GENMSG_04_12_BV |
|---|---|
| Summary | Check that IUT accepts the Secured GN Message containing additional non-standard HeaderField |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

with
  the IUT being in the 'authorized' state
  and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
  when
    the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
      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 'its_aid'
      and containing header_fields[4]
        containing type
          indicating non-standard header field type (1000)
        and containing other_header
          indicating non-empty data
      and not containing other header fields
  then
    the IUT accepts the SecuredMessage

| TP Id | TP_SEC_ITSS_RCV_GENMSG_04_13_BV |
|---|---|
| Summary | Check that ITS-S accepts a Secured GN Message containing header fields 'encryption_parameters' and 'recipient_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 with CERT_IUT_A_AT
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
         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 'its_aid'
         and containing header_fields[4]
            containing type
               indicating 'encryption_parameters'
            and containing enc_params
               containing symm_algorithm
                  indicating 'aes_128_ccm'
               and containing nonce
         and containing header_fields[5]
            containing type
               indicating 'recipient_info'
            and containing recipients
               containing recipients[0]
                  containing cert_id
                     referencing to CERT_IUT_A_AT
                  and containing pk_encryption
                     indicating 'ecies_nistp256'
                  and containing enc_key
         and not containing other header fields
   then
      the IUT accepts the SecuredMessage
```

### 5.3.4.4 Check signer info

| TP Id | 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 | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
         containing header_fields['signer_info']
            containing signer.type
               indicating 'self'
   then
      the IUT discards a SecuredMessage
```

| TP Id | TP_SEC_ITSS_RCV_GENMSG_05_02_BO |
|---|---|
| Summary | Check that IUT discards a secured GN Beacon if the header_fields contains a signer of type 'certificate_digest_with_other_algorithm' |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing header_fields['signer_info']<br>containing signer.type<br>indicating 'certificate_digest_with_other_algorithm'<br>then<br>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 | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing header_fields['signer_info']<br>containing signer.type<br>indicating 'certificate_chain'<br>then<br>the IUT discards a SecuredMessage | |

| TP Id | TP_SEC_ITSS_RCV_GENMSG_05_04_BO |
|---|---|
| Summary | Check that IUT discards a Secured Messageif the header_fields contains a signer info of unknown or reserved type |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing header_fields['signer_info']<br>containing signer.type<br>indicating X_UNKNOWN_SIGNERINFO_TYPE<br>then<br>the IUT discards a SecuredMessage | |
| NOTE: Values to be used as X_UNKNOWN_SIGNERINFO_TYPE are 5, 239, 240 and 255. | |

### 5.3.4.5 Check generation time

| TP Id | TP_SEC_ITSS_RCV_GENMSG_06_01_BO |
|---|---|
| **Summary** | Check that IUT discards a secured GN Message containing generation_time before the message signing certificate validity period |
| **Reference** | ETSI TS 103 097 [1], clauses 5.4 and 7.3 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing header_fields['signer_info']<br>containing certificate (CERT_TS_MSG_06_01_BO_AT)<br>containing validity_restrictions['time_start_and_end']<br>containing start_validity<br>indicating START_VALIDITY_AT<br>and containing end_validity<br>indicating END_VALIDITY_AT<br>and containing header_fields ['generation_time']<br>containing generation_time<br>indicating GEN_TIME < START_VALIDITY_AT<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_GENMSG_06_02_BO |
|---|---|
| **Summary** | Check that IUT discards the secured GN Message containing generation_time after the message signing certificate validity period |
| **Reference** | ETSI TS 103 097 [1], clauses 5.4 and 7.3 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing header_fields['signer_info']<br>containing certificate (CERT_TS_MSG_06_02_BO_AT)<br>containing validity_restrictions['time_start_and_end']<br>containing start_validity<br>indicating START_VALIDITY_AT<br>and containing end_validity<br>indicating END_VALIDITY_AT<br>and containing header_fields ['generation_time']<br>containing generation_time<br>indicating GEN_TIME > END_VALIDITY_AT<br>then<br>the IUT discards the message | |

### 5.3.4.6 Check its_aid

| TP Id | TP_SEC_ITSS_RCV_GENMSG_07_01_BO |
|---|---|
| Summary | Check that IUT discards SecuredMessage when its_aid value is undefined |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing header_fields['its_aid']<br>indicating 'AID_UNDEFINED'<br>then<br>the IUT discards the message | |

### 5.3.4.7 Check generation location

| TP Id | TP_SEC_ITSS_RCV_GENMSG_08_01_BO |
|---|---|
| Summary | Check that IUT discards Secured GN Message if the HeaderField generation_location is outside of the circular validity region of the signing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_B_AT<br>and the IUT current location is inside the validiti region of CERT_TS_B_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_B)<br>containing header_fields ['signer_info']<br>containing certificate (CERT_TS_B_AT)<br>containing validity_restrictions ['region']<br>containing region<br>containing region_type<br>indicating 'circle'<br>and containing circular_region<br>indicating REGION<br>and containing header_fields ['generation_location']<br>indicating location outside of the REGION<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_GENMSG_08_02_BO |
|---|---|
| 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 AND PICS_USE_RECTANGULAR_REGION |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_C_AT
   and the IUT current location is inside the validiti region of CERT_TS_C_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_C)
         containing header_fields ['signer_info']
            containing certificate (CERT_TS_C_AT)
               containing validity_restrictions ['region']
                  containing region
                     containing region_type
                        indicating 'rectangle'
                     and containing rectangular_regions
                        indicating REGION
         and containing header_fields ['generation_location']
            indicating locatoin outside of the REGION
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_GENMSG_08_03_BO |
|---|---|
| Summary | Check that IUT discards Secured GN Message if the optional HeaderField generation_location is outside of the polygonal validity region of the signing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_D_AT
   and the IUT current location is inside the validiti region of CERT_TS_D_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_D)
         containing header_fields ['signer_info']
            containing certificate (CERT_TS_D_AT)
               containing validity_restrictions ['region']
                  containing region
                     containing region_type
                        indicating 'polygon'
                     and containing polygonal_region
                        indicating REGION
         and containing header_fields ['generation_location']
            indicating location outside of the REGION
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_GENMSG_08_04_BO |
|---|---|
| Summary | Check that IUT discards Secured GN Message if the optional HeaderField generation_location is outside of the identified validity region of the signing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_E_AT
   and the IUT current location is inside the validiti region of CERT_TS_E_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_E)
         containing header_fields ['signer_info']
            containing certificate (CERT_TS_E_AT)
               containing validity_restrictions ['region']
                  containing region
                     containing region_type
                        indicating 'id_region'
                     and containing identified_region
                        indicating REGION
         and containing header_fields ['generation_location']
            indicating location outside of the REGION
   then
      the IUT discards the message
```

### 5.3.4.8 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 | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
         containing payload_field
            containing type
               indicating 'signed'
            and containing data
               indicating length 0
   then
      the IUT discards the message
```

| TP Id | 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<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing payload_field<br>containing type<br>indicating 'unsecured'<br>and containing data<br>indicating length > 0<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_GENMSG_09_04_BO |
|---|---|
| Summary | Check that IUT discards the Secured GN Message containing payload element of type 'encrypted' |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing payload_field<br>containing type<br>indicating 'encrypted'<br>and containing data<br>indicating length > 0<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_GENMSG_09_05_BV |
|---|---|
| Summary | Check that IUT accepts a well-formed Secured GN Message containing payload of type signed_external |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing payload_field<br>containing type<br>indicating 'signed_external'<br>then<br>the IUT accepts the message | |

| TP Id | TP_SEC_ITSS_RCV_GENMSG_09_06_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 | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing payload_field<br>containing type<br>indicating 'signed_and_encrypted'<br>then<br>the IUT accepts the message | |

### 5.3.4.9 Check presence of trailer field

| TP Id | 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 of type 'signature' |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing trailer_fields<br>not containing trailer_fields['signature']<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_GENMSG_10_02_BO |
|---|---|
| Summary | Check that IUT discards the Secured GN Message containing more than one instance of TrailerField of type 'signature' |
| Reference | ETSI TS 103 097 [1], clause 7.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_DENM_A)<br>containing trailer_fields[0]<br>containing type<br>indicating 'signature'<br>and containing trailer_fields[1]<br>containing type<br>indicating 'signature'<br>then<br>the IUT discards the message | |

### 5.3.4.10 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], clauses 4.2.2 and 7.3 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing header_fields ['signer_info']<br>containing signer<br>containing certificate (CERT_TS_A_AT)<br>containing subject_attributes['verification key']<br>containing key (KEY)<br>and containing trailer_fields[0]<br>containing type<br>indicating 'signature'<br>containing signature<br>NOT verifiable using KEY<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_GENMSG_11_02_BO |
|---|---|
| **Summary** | Check that IUT discards the Secured Message if the message contains trailer field of type 'signature' with reserved public key algorythms |
| **Reference** | ETSI TS 103 097 [1], clauses 4.2.2 and 7.3 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing trailer_fields<br>containing an instance of type TrailerField<br>containing type<br>indicating 'signature'<br>and containing signature.algorithm<br>indicating X_RESERVED_PK_ALGORYTHM<br>then<br>the IUT discards the message | |
| NOTE: Values to be provided as X_RESERVED_PK_ALGORYTHM are: 240, 255. | |

### 5.3.4.11 Check signing certificate type

| TP Id | 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 6.3 |
| PICS Selection | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>containing certificate (CERT_TS_A_EC)<br>containing subject_info.subject_type<br>indicating 'enrolment_credentials'<br>then<br>the IUT discards the message | |

| 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 6.3 |
| PICS Selection | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>containing certificate (CERT_TS_A_AA)<br>containing subject_info.subject_type<br>indicating 'authorization_authority'<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_GENMSG_12_03_BO |
|---|---|
| Summary | Check that IUT discards a Secured GN Message if the signer certificate of the message contains the subject type 'enrolment_authority' |
| 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 current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
         containing header_fields ['signer_info']
            containing signer
               containing type
                  indicating 'certificate'
               containing certificate (CERT_TS_A_EA)
                  containing subject_info.subject_type
                     indicating 'enrolment_authority'
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_GENMSG_12_04_BO |
|---|---|
| Summary | Check that IUT discards a Secured GN Message if the signer certificate of the message contains the subject type 'root_ca' |
| 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 current time is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
         containing header_fields ['signer_info']
            containing signer
               containing type
                  indicating 'certificate'
               containing certificate (CERT_TS_ROOT)
                  containing subject_info.subject_type
                     indicating 'root_ca'
   then
      the IUT discards the message
```

### 5.3.4.12 Check certificate validity

| **TP Id** | TP_SEC_ITSS_RCV_GENMSG_13_01_BO |
|---|---|
| **Summary** | Check that IUT discards secured message signed with the not yet valid certificate |
| **Reference** | ETSI TS 103 097 [1], clause 6.1 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is before the time validity period of CERT_TS_MSG_13_01_BO_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing header_fields['signer_info'].signer<br>containing certificate (CERT_TS_MSG_13_01_BO_AT)<br>containing validity_restrictions['time_start_and_end']<br>containing start_validity<br>indicating START_VALIDITY_AT > CURRENT_TIME<br>and containing end_validity<br>indicating END_VALIDITY_AT > START_VALIDITY_AT<br>then<br>the IUT discards the message | |

| **TP Id** | TP_SEC_ITSS_RCV_GENMSG_13_02_BO |
|---|---|
| **Summary** | Check that IUT discards secured message signed with the expired certificate |
| **Reference** | ETSI TS 103 097 [1], clause 6.1 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is before the time validity period of CERT_TS_MSG_13_02_BO_AT<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_A)<br>containing header_fields['signer_info'].signer<br>containing certificate (CERT_TS_MSG_13_02_BO_AT)<br>containing validity_restrictions['time_start_and_end']<br>containing start_validity<br>indicating START_VALIDITY_AT < CURRENT_TIME<br>and containing end_validity<br>indicating END_VALIDITY_AT < CURRENT_TIME<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_GENMSG_13_03_BO |
|---|---|
| Summary | Check that IUT discards secured message when IUT location is outside the circular validity restriction of the signing certificate |
| Reference | ETSI TS 103 097 [1], clause 6.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

with
the IUT being in the 'authorized' state
and the IUT current time is inside the validity period of CERT_TS_MSG_13_03_BO_AT
and the IUT current location is set to CURRENT_IUT_LOCATION
ensure that
when
the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_B)
containing header_fields['signer_info'].signer
containing certificate (CERT_TS_MSG_13_03_BO_AT)
containing validity_restrictions['region']
containing region
containing region_type
indicating 'circle'
and containing circular_region
indicating REGION
not containing the CURRENT_IUT_LOCATION
then
the IUT discards the message

| TP Id | TP_SEC_ITSS_RCV_GENMSG_13_04_BO |
|---|---|
| Summary | Check that IUT discards secured message when IUT location is outside the rectangular validity restriction of the signing certificate |
| Reference | ETSI TS 103 097 [1], clause 6.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

with
the IUT being in the 'authorized' state
and the IUT current time is inside the validity period of CERT_TS_MSG_13_04_BO_AT
and the IUT current location is set to CURRENT_IUT_LOCATION
ensure that
when
the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_C)
containing header_fields['signer_info'].signer
containing certificate (CERT_TS_MSG_13_04_BO_AT)
containing validity_restrictions['region']
containing region
containing region_type
indicating 'rectangle'
and containing rectangular_regions
indicating REGION
not containing the CURRENT_IUT_LOCATION
then
the IUT discards the message

| TP Id | TP_SEC_ITSS_RCV_GENMSG_13_05_BO |
|---|---|
| Summary | Check that IUT discards secured message when IUT location is outside the polygonal validity restriction of the signing certificate |
| Reference | ETSI TS 103 097 [1], clause 6.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the validity period of CERT_TS_MSG_13_05_BO_AT
   and the IUT current location is set to CURRENT_IUT_LOCATION
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_D)
         containing header_fields['signer_info'].signer
            containing certificate (CERT_TS_MSG_13_05_BO_AT)
               containing validity_restrictions['region']
                  containing region
                     containing region_type
                        indicating 'polygon'
                     and containing polygonal_region
                        indicating REGION
                           not containing the CURRENT_IUT_LOCATION
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_GENMSG_13_06_BO |
|---|---|
| Summary | Check that IUT discards secured message when IUT location is outside the identified validity restriction of the signing certificate |
| Reference | ETSI TS 103 097 [1], clause 6.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the validity period of CERT_TS_MSG_13_06_BO_AT
   and the IUT current location is set to CURRENT_IUT_LOCATION
ensure that
   when
      the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_E)
         containing header_fields['signer_info'].signer
            containing certificate (CERT_TS_MSG_13_06_BO_AT)
               containing validity_restrictions['region']
                  containing region
                     containing region_type
                        indicating 'id'
                     and containing id_region
                        indicating REGION
                           not containing the CURRENT_IUT_LOCATION
   then
      the IUT discards 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 7.4.1 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_01_01_BO_AT<br>ensure that<br>when the IUT is receiving a SecuredMessage<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>and containing certificate (CERT_TS_01_01_BO_AT)<br>containing version<br>indicating '3'<br>then<br>the IUT discards the message | |

| **TP Id** | 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 7.4.1 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_01_02_BO_AT<br>ensure that<br>when the IUT is receiving a SecuredMessage<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>and containing certificate (CERT_TS_01_02_BO_AT)<br>containing version<br>indicating '1'<br>then<br>the IUT discards the message | |

| 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 7.4.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

with
  the IUT being in the 'authorized' state
  and the IUT current time is inside the time validity period of CERT_TS_01_03_BO_AT
ensure that
  when the IUT is receiving a SecuredMessage
    containing header_fields ['signer_info']
      containing signer
        containing type
          indicating 'certificate_chain'
        and containing certificates[0] (CERT_TS_01_03_BO_AA)
          containing version
            indicating '3'
        and containing certificates[1] (CERT_TS_01_03_BO_AT)
          containing signer_info.type
            indicating 'certificate_digest_with_sha256'
          and containing signer_info.digest
            referencing to CERT_TS_01_03_BO_AA
  then
    the IUT discards the message

| TP Id | 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 7.4.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

with
  the IUT being in the 'authorized' state
  and the IUT current time is inside the time validity period of CERT_TS_01_04_BO_AT
ensure that
  when the IUT is receiving a SecuredMessage
    containing header_fields ['signer_info']
      containing signer
        containing type
          indicating 'certificate_chain'
        containing certificates[0] (CERT_TS_01_04_BO_AA)
          containing version
            indicating '1'
        and containing certificates[1] (CERT_TS_01_04_BO_AT)
          containing signer_info.digest
            referencing to CERT_TS_01_04_BO_AA
  then
    the IUT discards the message

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

| **TP Id** | TP_SEC_ITSS_RCV_CERT_02_01_BO |
|---|---|
| **Summary** | Check that IUT discards a SecuredMessage if the issuer certificate of the authorization ticket certificate contains the subject type 'enrolment_credential' |
| **Reference** | ETSI TS 103 097 [1], clause 6.3 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_02_01_BO_AT<br>ensure that<br>when the IUT is receiving a SecuredMessage<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>and containing certificate (CERT_TS_02_01_BO_AT)<br>containing signer_info.type<br>indicating 'certificate_digest_with_sha256'<br>and containing signer_info.digest<br>referencing to certificate (CERT_TS_A_EC)<br>containing subject_info.subject_type<br>indicating 'enrolment_credential'<br>then<br>the IUT discards the message | |

| **TP Id** | TP_SEC_ITSS_RCV_CERT_02_02_BO |
|---|---|
| **Summary** | Check that IUT discards a SecuredMessage if the issuer certificate of the authorization authority certificate contains the subject type 'enrolment_credential' |
| **Reference** | ETSI TS 103 097 [1], clause 6.3 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_02_02_BO_AT<br>ensure that<br>when the IUT is receiving a SecuredMessage<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate_chain'<br>and containing certificates[0] (CERT_TS_02_02_BO_AA)<br>containing signer_info.digest<br>referencing to certificate CERT_TS_A_EC<br>containing subject_info.subject_type<br>indicating 'enrolment_credential'<br>and containing certificates[1] (CERT_TS_02_02_BO_AT)<br>containing signer_info.digest<br>referencing to CERT_TS_02_02_BO_AA<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_CERT_02_03_BO |
|---|---|
| Summary | Check that IUT discards a SecuredMessage if the issuer certificate of the authorization ticket certificate contains the subject type 'enrolment_authority' |
| 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 current time is inside the time validity period of CERT_TS_02_03_BO_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_02_03_BO_AT)
               containing signer_info.type
                  indicating 'certificate_digest_with_sha256'
               and containing signer_info.digest
                  referencing to certificate (CERT_TS_A_EA)
                     containing subject_info.subject_type
                        indicating 'enrolment_authority'
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_02_04_BO |
|---|---|
| Summary | Check that IUT discards a SecuredMessage if the issuer certificate of the authorization authority certificate contains the subject type 'enrolment_authority' |
| 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 current time is inside the time validity period of CERT_TS_02_04_BO_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate_chain'
            and containing certificates[0] (CERT_TS_02_04_BO_AA)
               containing signer_info.digest
                  referencing to certificate CERT_TS_A_EA
                     containing subject_info.subject_type
                        indicating 'enrolment_authority'
            and containing certificates[1] (CERT_TS_02_04_BO_AT)
               containing signer_info.digest
                  referencing to CERT_TS_02_04_BO_AA
   then
      the IUT discards the message
```

### 5.3.5.3 Check that authorization ticket certificate is not used for sign other certificates

| TP Id | TP_SEC_ITSS_RCV_CERT_03_01_BO |
|---|---|
| Summary | Check that IUT discards a SecuredMessage if the issuer certificate of the authorization ticket certificate contains the subject type 'authorization_ticket' |
| Reference | ETSI TS 103 097 [1], clause 6.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_03_01_BO_AT<br>ensure that<br>when the IUT is receiving a SecuredMessage<br>containing header_fields ['signer_info'].signer<br>containing certificate (CERT_TS_03_01_BO_AT)<br>containing signer_info.digest<br>referencing to CERT_TS_03_BO_CA<br>containing subject_info.subject_type<br>indicating 'authorization_ticket'<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_CERT_03_02_BO |
|---|---|
| Summary | Check that IUT discards a SecuredMessage if the issuer certificate of the authorization authority certificate contains the subject type 'authorization_ticket' |
| Reference | ETSI TS 103 097 [1], clause 6.3 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_03_02_BO_AT<br>ensure that<br>when the IUT is receiving a SecuredMessage<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate_chain'<br>and containing certificates[0] (CERT_TS_03_02_BO_AA)<br>containing signer_info.digest<br>referencing to CERT_TS_03_BO_CA<br>containing subject_info.subject_type<br>indicating 'authorization_ticket'<br>and containing certificates[1] (CERT_TS_03_02_BO_AT)<br>containing signer_info.digest<br>referencing to CERT_TS_03_02_BO_AA<br>then<br>the IUT discards the message | |

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

| | |
|---|---|
| **TP Id** | TP_SEC_ITSS_RCV_CERT_04_01_BO |
| **Summary** | Check that IUT discards a SecuredMessage if the issuer certificate of the AA certificate contains the subject type 'authorization_authority' |
| **Reference** | ETSI TS 103 097 [1], clause 6.3 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_04_01_BO_AT<br>ensure that<br>when the IUT is receiving a SecuredMessage<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate_chain'<br>and containing certificates[0] (CERT_TS_04_01_BO_AA)<br>containing signer_info.digest<br>referencing to CERT_TS_A_AA<br>and containing certificates[1] (CERT_TS_04_01_BO_AT)<br>containing signer_info.digest<br>referencing to CERT_TS_04_01_BO_AA<br>then<br>the IUT discards the message | |

### 5.3.5.5 Check the certificate signature

| | |
|---|---|
| **TP Id** | TP_SEC_ITSS_RCV_CERT_05_01_BO |
| **Summary** | Check that IUT discards the message when signing AT certificate has an invalid signature |
| **Reference** | ETSI TS 103 097 [1], clauses 6.1 and 7.4.1 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when the IUT is receiving a SecuredMessage<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>and containing certificate (CERT_TS_A_AT)<br>containing signer_info.digest<br>referencing to a CERT_TS_A_AA<br>and containing signature<br>NOT verifiable with CERT_TS_A_AA.subject_attributes['verification_key'].key<br>then<br>the IUT discards the message | |

| TP Id | 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 an invalid signature |
| Reference | ETSI TS 103 097 [1], clauses 6.1 and 7.4.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_A_AT<br>ensure that<br>when the IUT is receiving a SecuredMessage<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate_chain'<br>and containing certificates[0] (CERT_TS_A_AA)<br>containing signer_info.digest<br>referencing to a CERT_ROOT<br>and containing signature<br>NOT verifiable with CERT_ROOT.subject_attributes['verification_key'].key<br>and containing certificates[1] (CERT_TS_A_AT)<br>containing signer_info.digest<br>referencing to a CERT_TS_A_AA<br>then<br>the IUT discards the message | |

### 5.3.5.6 Check circular region of subordinate certificate

| TP Id | TP_SEC_ITSS_RCV_CERT_06_01_BV |
|---|---|
| Summary | Check that the IUT accepts a message when the signing certificate of this message contains the same circular region validity restriction as its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_06_01_BV_AT<br>and the IUT current location is inside the CURCULAR_REGION_AA<br>ensure that<br>when the IUT is receiving a SecuredMessage<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>containing certificate (CERT_TS_06_01_BV_AT)<br>containing validity_restrictions['region']<br>containing region_type<br>indicating 'circle'<br>containing circular_region<br>indicating CURCULAR_REGION_AA<br>containing signer_info.digest<br>referencing to a CERT_TS_B_AA<br>containing validity_restrictions['region']<br>containing region_type<br>indicating 'circle'<br>and containing circular_region<br>indicating CURCULAR_REGION_AA<br>then<br>the IUT accepts the message | |

| TP Id | TP_SEC_ITSS_RCV_CERT_06_02_BV |
|---|---|
| Summary | Check that the IUT accepts a message when the signing certificate of this message contains the circular region validity restriction which is fully inside in the circular region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_06_02_BV_AT
   and the IUT current location is inside the CURCULAR_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_06_02_BV_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'circle'
                  and containing circular_region
                     indicating CURCULAR_REGION_AT
               and containing signer_info.digest
                  referencing to a certificate CERT_TS_B_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'circle'
                        and containing circular_region
                           indicating CURCULAR_REGION_AA
                              fully covering CURCULAR_REGION_AT
   then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_06_03_BV |
|---|---|
| Summary | Check that the IUT accepts a message when the signing certificate of this message contains the circular region validity restriction which is fully inside in the rectangular region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION |
| **Expected behaviour** | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_06_03_BV_AT
   and the IUT current location is inside the CURCULAR_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_06_03_BV_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'circle'
                  and containing circular_region
                     indicating CURCULAR_REGION_AT
               and containing signer_info.digest
                  referencing to a certificate CERT_TS_C_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'rectangular'
                        and containing rectangular_region[0]
                           indicating RECT_REGION_AA
                              fully covering CURCULAR_REGION_AT
    then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_06_04_BV |
|---|---|
| Summary | Check that the IUT accepts a message when the signing certificate of this message contains the circular region validity restriction which is fully inside in the polygonal region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION |
| **Expected behaviour** | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_06_04_BV_AT
   and the IUT current location is inside the CURCULAR_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_06_04_BV_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'circle'
                  and containing circular_region
                     indicating CURCULAR_REGION_AT
               and containing signer_info.digest
                  referencing to a certificate CERT_TS_D_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'polygon'
                        and containing polygonal_region
                           indicating POLYGON_REGION_AA
                              fully covering CURCULAR_REGION_AT
   then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_06_05_BV |
|---|---|
| Summary | Check that the IUT accepts a message when the signing certificate of this message contains the circular region validity restriction which is fully inside in the identified region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_06_05_BV_AT
   and the IUT current location is inside the CURCULAR_REGION_AT
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_BV_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'circle'
                  and containing circular_region
                     indicating CURCULAR_REGION_AT
               and containing signer_info.digest
                  referencing to a certificate CERT_TS_E_AA
                     containing validity_restrictions['region']
                        and containing region_type
                           indicating 'id'
                        and containing id_region
                           containing region_dictionary
                              indicating 'iso_3166_1'
                           and containing local_region
                              indicating 0
                           and containing region_identifier
                              indicating ID_REGION_AT
                                 fully covering CURCULAR_REGION_AT
   then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_06_06_BO |
|---|---|
| Summary | Check that the IUT discards a message when the signing certificate of this message does not contain the region validity restriction but its issuing certificate contains the circular region validity restriction |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_06_06_BO_AT
   and the IUT current location is inside the CURCULAR_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_06_06_BO_AT)
               not containing validity_restrictions['region']
               and containing signer_info.digest
                  referencing to a CERT_TS_B_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'circle'
                        and containing circular_region
                           indicating CURCULAR_REGION_AT
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_06_07_BO |
|---|---|
| Summary | Check that the IUT discards a message when the signing certificate of this message contains circular region validity restriction which is outside of the circular region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_06_07_BO_AT
   and the IUT current location is inside the CURCULAR_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_06_07_BO_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'circle'
                  and containing circular_region
                     indicating CURCULAR_REGION_AT
               and containing signer_info.digest
                  referencing to a CERT_TS_06_07_BO_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'circle'
                        and containing circular_region
                           indicating CURCULAR_REGION_AA_OUTSIDE
                              not including CURCULAR_REGION_AT
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_06_08_BO |
|---|---|
| Summary | Check that the IUT discards a message when the signing certificate of this message contains circular region validity restriction which is not fully covered by the the circular region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION |
| **Expected behaviour** | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_06_08_BO_AT
   and the IUT current location is inside the CURCULAR_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_06_08_BO_AT)
               containing validity_restrictions['region']
                     containing region_type
                        indicating 'circle'
                     and containing circular_region
                        indicating CURCULAR_REGION_AT
               and containing signer_info.digest
                  referencing to a CERT_TS_06_08_BO_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'circle'
                        and containing circular_region
                           indicating CURCULAR_REGION_AA_INTERSECT
                              including partially CURCULAR_REGION_AT
   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 |
| **Summary** | Check that the IUT accepts a message when the signing certificate of this message contains the same rectangular region validity restriction as its issuing certificate |
| **Reference** | ETSI TS 103 097 [1], clause 7.4.1 |
| **PICS Selection** | PICS_GN_SECURITY AND PICS_USE_RECTANGULAR_REGION |
| **Expected behaviour** | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_07_01_BV_AT
   and the IUT current location is inside the RECT_REGION_AA
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_07_01_BV_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'rectangle'
                  and containing rectangular_region[0]
                     indicating RECT_REGION_AA
               and containing signer_info.digest
                  referencing to a CERT_TS_C_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'rectangular'
                        and containing rectangular_region[0]
                           indicating RECT_REGION_AA
   then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_07_03_BV |
|---|---|
| Summary | Check that the IUT accepts a message when the signing certificate of this message contains the validity restriction with rectangular region which is fully inside in the rectangular region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_RECTANGULAR_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_07_03_BV_AT
   and the IUT current location is inside the RECT_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_07_03_BV_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'rectangle'
                  and containing rectangular_region[0]
                     indicating RECT_REGION_AT
               and containing signer_info.digest
                  referencing to a certificate CERT_TS_C_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'rectangular'
                        and containing rectangular_region[0]
                           indicating RECT_REGION_AA
                              fully covering RECT_REGION_AT
   then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_07_04_BV |
|---|---|
| Summary | Check that the IUT accepts a message when the signing certificate of this message contains the rectangular region validity restriction which is fully inside in the polygonal region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_RECTANGULAR_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_07_04_BV_AT
   and the IUT current location is inside the RECT_REGION_AT
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_BV_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 certificate CERT_TS_D_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'polygon'
                        containing polygonal_region
                           indicating POLYGON_REGION_AA
                              fully covering RECT_REGION_AT
   then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_07_05_BV |
|---|---|
| Summary | Check that the IUT accepts a message when the signing certificate of this message contains the rectangular region validity restriction which is fully inside in the identified region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_RECTANGULAR_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_07_05_BV_AT
   and the IUT current location is inside the RECT_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_07_05_BV_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'rectangle'
                  and containing rectangular_region[0]
                     indicating RECT_REGION_AT
               and containing signer_info.digest
                  referencing to a certificate CERT_TS_E_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'id'
                        and containing id_region
                           containing region_dictionary
                              indicating 'iso_3166_1' (0)
                           and containing local_region
                              indicating 0
                           and containing region_identifier
                              indicating ID_REGION_AT
                                 fully covering RECT_REGION_AT
   then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_07_06_BO |
|---|---|
| Summary | Check that the IUT discards a message when the signing certificate of this message does not contain the region validity restriction but its issuing certificate contains the rectangular region validity restriction |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_RECTANGULAR_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_07_06_BO_AT
   and the IUT current location is inside the RECT_REGION_AT
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_06_BO_AT)
               not containing validity_restrictions['region']
               and containing signer_info.digest
                  referencing to a CERT_TS_C_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'rectangular'
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_07_07_BO |
|---|---|
| Summary | Check that the IUT discards a message when the signing certificate of this message contains rectangular region validity restriction which is outside of the rectangular region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_RECTANGULAR_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_07_07_BO_AT
   and the IUT current location is inside the RECT_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_07_07_BO_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'rectangle'
                  and containing rectangular_region[0]
                     indicating RECT_REGION_AT
               and containing signer_info.digest
                  referencing to a CERT_TS_07_07_BO_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'rectangle'
                        and containing rectangular_region[0]
                           indicating RECT_REGION_AA_OUTSIDE
                              not including RECT_REGION_AT
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_07_08_BO |
|---|---|
| Summary | Check that the IUT discards a message when the signing certificate of this message contains rectangular region validity restriction which is not fully covered by the the rectangular region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_RECTANGULAR_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_07_08_BO_AT
   and the IUT current location is inside the RECT_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_07_08_BO_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'rectangle'
                  and containing rectangular_region[0]
                     indicating RECT_REGION_AT
               and containing signer_info.digest
                  referencing to a CERT_TS_07_08_BO_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'rectangle'
                        and containing rectangular_region[0]
                           indicating RECT_REGION_AA_INTERSECT
                              including partialy RECT_REGION_AT
   then
      the IUT discards the message
```

### 5.3.5.8 Check polygonal region of subordinate certificate

| | |
|---|---|
| **TP Id** | TP_SEC_ITSS_RCV_CERT_08_01_BV |
| **Summary** | Check that the IUT accepts a message when the signing certificate of this message contains the same polygonal region validity restriction as its issuing certificate |
| **Reference** | ETSI TS 103 097 [1], clause 7.4.1 |
| **PICS Selection** | PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION |
| **Expected behaviour** | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_08_01_BV_AT
   and the IUT current location is inside the POLYGON_REGION_AA
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_08_01_BV_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'polygon'
                  and containing polygonal_region
                     indicating POLYGON_REGION_AA
               and containing signer_info.digest
                  referencing to a CERT_TS_D_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'polygon'
                        and containing polygonal_region
                           indicating POLYGON_REGION_AA
   then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_08_02_BV |
|---|---|
| Summary | Check that the IUT accepts a message when the signing certificate of this message contains the polygonal region validity restriction which is fully inside in the circular region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION |
| **Expected behaviour** | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_08_02_BV_AT
   and the IUT current location is inside the POLYGON_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_08_02_BV_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'polygon'
                  and containing polygonal_region
                     indicating POLYGON_REGION_AT
               and containing signer_info.digest
                  referencing to a certificate CERT_TS_B_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'circle'
                        and containing circular_region
                           indicating CURCULAR_REGION_AA
                              fully including POLYGON_REGION_AT
   then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_08_03_BV |
|---|---|
| Summary | Check that the IUT accepts a message when the signing certificate of this message contains the polygonal region validity restriction which is fully inside in the rectangular region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_08_03_BV_AT
   and the IUT current location is inside the POLYGON_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_08_03_BV_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'polygon'
                  and containing polygonal_region
                     indicating POLYGON_REGION_AT
               and containing signer_info.digest
                  referencing to a certificate CERT_TS_C_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'rectangular'
                        and containing rectangular_region[0]
                           indicating RECT_REGION_AA
                              fully covering POLYGON_REGION_AT
   then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_08_04_BV |
|---|---|
| Summary | Check that the IUT accepts a message when the signing certificate of this message contains the polygonal region validity restriction which is fully inside in the polygonal region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION |
| **Expected behaviour** | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_08_04_BV_AT
   and the IUT current location is inside the POLYGON_REGION_AA
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_08_04_BV_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'polygon'
                  and containing polygonal_region
                     indicating POLYGON_REGION_AT
               and containing signer_info.digest
                  referencing to a CERT_TS_D_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'polygon'
                        and containing polygonal_region
                           indicating POLYGON_REGION_AA
                              fully including POLYGON_REGION_AT
   then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_08_05_BV |
|---|---|
| Summary | Check that the IUT accepts a message when the signing certificate of this message contains the polygonal region validity restriction which is fully inside in the identified region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_08_04_BV_AT
   and the IUT current location is inside the POLYGON_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_08_05_BV_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'polygon'
                  and containing polygonal_region
                     indicating POLYGON_REGION_AT
               and containing signer_info.digest
                  referencing to a certificate CERT_TS_E_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'id'
                        and containing id_region
                           containing region_dictionary
                              indicating 'iso_3166_1' (0)
                           and containing local_region
                              indicating 0
                           and containing region_identifier
                              indicating ID_REGION_AT
                                 fully including POLYGON_REGION_AT
   then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_08_06_BO |
|---|---|
| Summary | Check that the IUT discards a message when the signing certificate of this message does not contain the region validity restriction but its issuing certificate contains the polygonal region validity restriction |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_08_06_BO_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_08_06_BO_AT)
               not containing validity_restrictions['region']
               and containing signer_info.digest
                  referencing to a CERT_TS_D_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'polygon'
   then
      the IUT discards the message
```

| | |
|---|---|
| **TP Id** | TP_SEC_ITSS_RCV_CERT_08_07_BO |
| **Summary** | Check that the IUT discards a message when the signing certificate of this message contains polygonal region validity restriction containing less than 3 points |
| **Reference** | ETSI TS 103 097 [1], clause 7.4.1 |
| **PICS Selection** | PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_08_07_BO_AT
   and the IUT current location is inside the POLYGON_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_08_07_BO_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'polygon'
                  and containing polygonal_region (POLYGON_REGION_08_04_BO)
                     indicating length = 2
               and containing signer_info.digest
                  referencing to a CERT_TS_D_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'polygon'
                        and containing polygonal_region
                           indicating POLYGON_REGION_AA
                              fully covering all points of POLYGON_REGION_08_04_BO
    then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_08_08_BO |
|---|---|
| Summary | Check that the IUT discards a message when the signing certificate of this message contains polygonal region validity restriction which is outside of the polygonal region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_08_08_BO_AT
   and the IUT current location is inside the POLYGON_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_08_08_BO_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'polygon'
                  and containing polygonal_region
                     indicating POLYGON_REGION_AT
               and containing signer_info.digest
                  referencing to a CERT_TS_08_08_BO_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'polygon'
                        and containing polygonal_region
                           indicating POLYGON_REGION_AA_OUTSIDE
                              not including POLYGON_REGION_AT
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_08_09_BO |
|---|---|
| Summary | Check that the IUT discards a message when the signing certificate of this message contains polygonal region validity restriction which is not fully covered by the the polygonal region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_08_09_BO_AT
   and the IUT current location is inside the POLYGON_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_08_09_BO_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'polygon'
                  and containing polygonal_region
                     indicating POLYGON_REGION_AT
               and containing signer_info.digest
                  referencing to a CERT_TS_08_09_BO_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'polygon'
                        and containing polygonal_region
                           indicating POLYGON_REGION_AA_INTERSECT
                              including partialy POLYGON_REGION_AT
   then
      the IUT discards the message
```

### 5.3.5.9 Check identified region of subordinate certificate

| | |
|---|---|
| **TP Id** | TP_SEC_ITSS_RCV_CERT_09_01_BV |
| **Summary** | Check that the IUT accepts a message when its signing certificate contains the identified 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 7.4.1 |
| **PICS Selection** | PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION |
| **Expected behaviour** | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_09_01_BV_AT
   and the IUT current location is inside the ID_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_09_01_BV_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'id'
                  and containing id_region
                     containing region_dictionary
                        indicating 'iso_3166_1'
                     and containing region_identifier
                        indicating ID_REGION_AT
                     and containing local_region
                        indicating 0
               containing signer_info.digest
                  referencing to a certificate CERT_TS_E_AA
                     containing region_type
                        indicating 'id'
                     and containing id_region
                        containing region_dictionary
                           indicating 'iso_3166_1'
                        and containing region_identifier
                           indicating ID_REGION_AT
                        and containing local_region
                           indicating 0
   then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_09_02_BV |
|---|---|
| Summary | Check that the IUT accepts a message when its signing certificate contains the identified region validity restriction with the same identified region as the issuing certificate and with local area definition |
| Reference | ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_09_02_BV_AT
   and the IUT current location is inside the ID_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_09_02_BV_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'id'
                  and containing id_region
                     containing region_dictionary
                        indicating 'iso_3166_1'
                     and containing region_identifier
                        indicating ID_REGION_AT
                     and containing local_region
                        indicating ID_LOCAL_REGION_1
               containing signer_info.digest
                  referencing to a certificate CERT_TS_E_AA
                     containing region_type
                        indicating 'id'
                     and containing id_region
                        containing region_dictionary
                           indicating 'iso_3166_1'
                        and containing region_identifier
                           indicating ID_REGION_AT
                        and containing local_region
                           indicating 0
   then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_09_03_BV |
|---|---|
| Summary | Check that the IUT accepts a message when its signing certificate contains the identified region validity restriction fully containing in the circular validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_09_03_BV_AT
   and the IUT current location is inside the ID_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_09_03_BV_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'id'
                  and containing id_region
                     containing region_dictionary
                        indicating 'iso_3166_1'
                     and containing region_identifier
                        indicating ID_REGION_AT
                     and containing local_region
                        indicating 0
               and containing signer_info.digest
                  referencing to a certificate CERT_TS_09_03_BV_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'circle'
                        and containing circular_region
                           fully covering ID_REGION_AT
   then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_09_04_BV |
|---|---|
| Summary | Check that the IUT accepts a message when the signing certificate of this message contains the polygonal region validity restriction which is fully inside in the rectangular region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_09_03_BV_AT
   and the IUT current location is inside the ID_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_09_04_BV_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'id'
                  and containing id_region
                     containing region_dictionary
                        indicating 'iso_3166_1'
                     and containing region_identifier
                        indicating ID_REGION_AT
                     and containing local_region
                        indicating 0
               and containing signer_info.digest
                  referencing to a certificate CERT_TS_09_04_BV_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'rectangular'
                        containing rectangular_region[0]
                           fully covering ID_REGION_AT
   then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_09_05_BV |
|---|---|
| Summary | Check that the IUT accepts a message when the signing certificate of this message contains the polygonal region validity restriction which is fully inside in the polygonal region validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_09_05_BV_AT
   and the IUT current location is inside the ID_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_09_05_BV_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'id'
                  and containing id_region
                     containing region_dictionary
                        indicating 'iso_3166_1'
                     and containing region_identifier
                        indicating ID_REGION_AT
                     and containing local_region
                        indicating 0
               and containing signer_info.digest
                  referencing to a certificate CERT_TS_09_05_BV_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'polygon'
                        and containing polygonal_region
                           fully covering ID_REGION_AT
   then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_09_06_BV |
|---|---|
| Summary | Check that the IUT accepts a message when the signing certificate of the message contains the identified region validity restriction with the identified region which is fully covered by the identified region of the validity restriction of its issuing certificate |
| Reference | ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_09_06_BV_AT
   and the IUT current location is inside the ID_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_09_06_BV_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'id'
                  and containing id_region
                     containing region_dictionary
                        indicating 'un_stats'
                     and containing region_identifier
                        indicating ID_REGION_AT
                     and containing local_region
                        indicating 0
               and containing signer_info.digest
                  referencing to a CERT_TS_09_06_BV_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'id'
                        and containing id_region
                           containing region_dictionary
                              indicating 'un_stats'
                           and containing region_identifier
                              indicating ID_REGION_AA_UNSTATS
                                 which includes ID_REGION_AT
                           and containing local_region
                              indicating 0
   then
      the IUT accepts the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_09_07_BO |
|---|---|
| Summary | Check that the IUT discards a message when the signing certificate of this message does not contain the region validity restriction but its issuing certificate contains the identified region validity restriction |
| Reference | ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION |
| **Expected behaviour** | |

with
the IUT being in the 'authorized' state
and the IUT current time is inside the time validity period of CERT_TS_09_07_BO_AT
ensure that
when the IUT is receiving a SecuredMessage
containing header_fields ['signer_info']
containing signer
containing type
indicating 'certificate'
and containing certificate (CERT_TS_09_07_BO_AT)
not containing validity_restrictions['region']
and containing signer_info.digest
referencing to the certificate CERT_TS_E_AA
containing validity_restrictions['region']
containing region_type
indicating 'id'
then
the IUT discards the message

| TP Id | TP_SEC_ITSS_RCV_CERT_09_08_BO |
|---|---|
| Summary | Check that the IUT discards a message when the signing certificate and its issuing certificate are both containing the identified region validity restrictions with the same region id but different local regions |
| Reference | ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_09_08_BO_AT
   and the IUT current location is inside the ID_REGION_AA, local region 1
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_09_08_BO_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'id'
                  and containing id_region
                     containing region_dictionary
                        indicating 'iso_3166_1'
                     containing region_identifier
                        indicating ID_REGION_AA
                     containing local_region
                        indicating ID_LOCAL_REGION_1
               containing signer_info.digest
                  referencing to a CERT_TS_09_08_BO_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'id'
                        containing id_region
                           containing region_dictionary
                              indicating 'iso_3166_1'
                           containing region_identifier
                              indicating ID_REGION_AA
                           containing local_region
                              indicating ID_LOCAL_REGION_2
                                 not equal to ID_LOCAL_REGION_1
   then
      the IUT discards the message
```

| | |
|---|---|
| **TP Id** | TP_SEC_ITSS_RCV_CERT_09_09_BO |
| **Summary** | Check that the IUT discards a message when the identified region of the validity restriction of its signing certificate is different and not fully covered by the one in the issuing certificate |
| **Reference** | ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1 |
| **PICS Selection** | PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_09_09_BO_AT
   and the IUT current location is inside the ID_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_09_09_BO_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'id'
                  and containing id_region
                     containing region_dictionary
                        indicating 'iso_3166_1'
                     and containing region_identifier
                        indicating ID_REGION_AT
                     and containing local_region
                        indicating 0
               containing signer_info.digest
                  referencing to a CERT_TS_09_09_BO_AA
                     containing validity_restrictions['region']
                        containing region_type
                           indicating 'id'
                        and containing id_region
                           containing region_dictionary
                              indicating 'iso_3166_1'
                           and containing region_identifier
                              indicating ID_REGION_AA_OTHER
                                 other than ID_REGION_AT
                           and containing local_region
                              indicating 0
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_09_10_BO |
|---|---|
| Summary | Check that the IUT discards a message when the identified region validity restriction of its signing certificate contains unknown area code |
| Reference | ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION |

**Expected behaviour**

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_09_10_BO_AT
   and the IUT current location is inside the ID_REGION_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_09_10_BO_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'id'
                  and containing id_region
                     containing region_dictionary
                        indicating 'iso_3166_1'
                     and containing region_identifier
                        indicating ID_REGION_UNKNOWN
                           not existing in ISO 3166-1 [4]
                     and containing local_region
                        indicating 0
               and containing signer_info.digest
                  referencing to a CERT_TS_A_AA
                     not containing validity_restrictions [4]
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_09_11_BO |
|---|---|
| Summary | Check that the IUT discards a message when the validity restriction of its signing certificate contains the identified region of type iso-3166-1 but region code is from the UN-Stats dictionary |
| Reference | ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1 |
| PICS Selection | PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_09_11_BO_AT
   and the IUT current location is inside the    ID_REGION_AA_UNSTATS
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_09_11_BO_AT)
               containing validity_restrictions['region']
                  containing region_type
                     indicating 'id'
                  and containing id_region
                     containing region_dictionary
                        indicating 'iso_3166_1'
                     and containing region_identifier
                        indicating ID_REGION_AA_UNSTATS
                     and containing local_region
                        indicating 0
               and containing signer_info.digest
                  referencing to a CERT_TS_A_AA
                     not containing validity_restrictions['region']
   then
      the IUT discards the message
```

## 5.3.5.10 Check time validity restrictions

### 5.3.5.10.1 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], 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 SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            containing certificate (CERT_TS_10_01_BO_AT)
               not containing validity_restrictions['time_start_and_end']
               and not containing validity_restrictions['time_end']
               and not containing validity_restrictions['time_start_and_duration']

   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_10_02_BO |
|---|---|
| Summary | Check that the IUT discards a message when the issuing certificate of the message signing certificate does not contain the time validity restriction |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>ensure that<br>when the IUT is receiving a SecuredMessage<br>containing header_fields ['signer_info'].signer<br>containing type<br>indicating 'certificate'<br>containing certificate (CERT_TS_10_02_BO_AT)<br>containing signer_info.digest<br>referencing to CERT_TS_10_02_BO_AA<br>not containing validity_restrictions['time_start_and_end']<br>and not containing validity_restrictions['time_end']<br>and not containing validity_restrictions['time_start_and_duration']<br><br>then<br>the IUT discards the message | |

### 5.3.5.10.2 Check AT certificate time validity restriction presence

| TP Id | TP_SEC_ITSS_RCV_CERT_10_03_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 7.4.2 and 7.4.4 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is less then time_end validity restricyion of CERT_TS_10_03_BO_AT<br>ensure that<br>when the IUT is receiving a SecuredMessage<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>containing certificate (CERT_TS_10_03_BO_AT)<br>containing validity_restrictions['time_end']<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_CERT_10_04_BO |
|---|---|
| Summary | Check that the IUT discards a message when its signing certificate contains 'time_start_and_duration' validity restriction |
| Reference | ETSI TS 103 097 [1], clauses 7.4.2 and 7.4.4 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

with
the IUT being in the 'authorized' state
and the IUT current time is inside the time validity period of CERT_TS_10_04_BO_AT
ensure that
when the IUT is receiving a SecuredMessage
containing header_fields ['signer_info']
containing signer
containing type
indicating 'certificate'
containing certificate (CERT_TS_10_04_BO_AT)
containing validity_restrictions['time_start_and_duration']
then
the IUT discards the message

| TP Id | TP_SEC_ITSS_RCV_CERT_10_05_BO |
|---|---|
| Summary | Check that the IUT discards a message when the issuing certificate of the message signing certificate contains 'time_end' validity restriction |
| Reference | ETSI TS 103 097 [1], clauses 7.4.2 and 7.4.4 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

with
the IUT being in the 'authorized' state
and the IUT current time is less then time_end validity restricyion of CERT_TS_10_05_BO_AT
ensure that
when the IUT is receiving a SecuredMessage
containing header_fields ['signer_info'].signer
containing type
indicating 'certificate'
containing certificate (CERT_TS_10_05_BO_AT)
containing signer_info.digest
referencing to CERT_TS_10_05_BO_AA
containing validity_restrictions['time_end']
then
the IUT discards the message

| TP Id | TP_SEC_ITSS_RCV_CERT_10_06_BO |
|---|---|
| Summary | Check that the IUT discards a message when its signing certificate contains 'time_start_and_duration' validity restriction |
| Reference | ETSI TS 103 097 [1], clauses 7.4.2 and 7.4.4 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

with
the IUT being in the 'authorized' state
and the IUT current time is less then time_end validity restricyion of CERT_TS_10_06_BO_AT
ensure that
when the IUT is receiving a SecuredMessage
containing header_fields ['signer_info'].signer
containing type
indicating 'certificate'
containing certificate (CERT_TS_10_06_BO_AT)
containing signer_info.digest
referencing to CERT_TS_10_06_BO_AA
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 Id | 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 validity period of its issuing certificate |
| 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
   and the IUT current time is greater than START_VALIDITY_AA and less than END_VALIDITY_AA
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
                        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
               containing end_validity
                  indicating END_VALIDITY_AA + 1d
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_11_02_BO |
|---|---|
| Summary | Check that the IUT discards a message when the validity period of its signing certificate starts before the validity period of the issuing certificate |
| 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
   and the IUT current time is greater than START_VALIDITY_AA and less than END_VALIDITY_AA
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
                  and containing end_validity
                     indicating END_VALIDITY_AA
         and containing validity_restrictions['time_start_and_end']
            containing start_validity
               indicating START_VALIDITY_AA - 1d
            and containing end_validity
               indicating END_VALIDITY_AA
   then
      the IUT discards the message
```

| TP Id | 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 but the signing certificate is not expired yet |
| 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
   and the IUT current time is greater than START_VALIDITY_AA and less than END_VALIDITY_AA
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info'].signer.certificate (CERT_TS_11_03_BO_AT)
         containing signer_info.digest
            referencing to CERT_TS_11_03_BO_AA
               containing validity_restrictions['time_start_and_end']
                  containing start_validity
                     indicating START_VALIDITY_AA - 365d
                  and containing end_validity
                     indicating START_VALIDITY_AA - 1d
         and containing validity_restrictions['time_start_and_end']
            containing start_validity
               indicating START_VALIDITY_AA - 365d
            and containing end_validity
               indicating END_VALIDITY_AA
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_11_04_BO |
|---|---|
| Summary | Check that the IUT discards a message when the validity period of the signing certificate is after the validity period of its issuing certificate |
| 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
   and the IUT current time is greater than START_VALIDITY_AA and less than END_VALIDITY_AA
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
                  and containing end_validity
                     indicating END_VALIDITY_AA + 365d
         and containing validity_restrictions['time_start_and_end']
            containing start_validity
               indicating START_VALIDITY_AA
            and containing end_validity
               indicating END_VALIDITY_AA +365d
   then
      the IUT discards the message
```

### 5.3.5.12 Check AID-SSP subject attribute presence and value

| **TP Id** | 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 7.4.2 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_12_01_BO_AT<br>ensure that<br>when the IUT is receiving a SecuredMessage<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>and containing certificate (CERT_TS_12_01_BO_AT)<br>not containing subject_attributes['its_aid_ssp_list']<br>then<br>the IUT discards the message | |

| **TP Id** | TP_SEC_ITSS_RCV_CERT_12_02_BO |
|---|---|
| **Summary** | Check that the IUT discards a Secured CAM when its signing certificate does not contain a record with AID_CAM in the its_aid_ssp_list subject attribute |
| **Reference** | ETSI TS 103 097 [1], clause 7.4.2 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_12_02_BO_AT<br>ensure that<br>when the IUT is receiving a Secured CAM (MSG_SEC_RCV_CAM_01)<br>containing header_fields ['its_aid']<br>containing its_aid<br>indicating 'AID_CAM'<br>and containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>and containing certificate (CERT_TS_12_02_BO_AT)<br>containing subject_attributes['its_aid_ssp_list']<br>not containing an item<br>containing its_aid<br>indicating 'AID_CAM'<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_CERT_12_03_BO |
|---|---|
| Summary | Check that the IUT discards a Secured DENM when its signing certificate does not contain a record with AID_DENM in the its_aid_ssp_list subject attribute |
| Reference | ETSI TS 103 097 [1], clause 7.4.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_12_03_BO_AT
ensure that
   when the IUT is receiving a Secured DENM (MSG_SEC_RCV_DENM_A)
      containing header_fields ['its_aid']
         containing its_aid
            indicating 'AID_DENM'
      and containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and 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'
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_12_04_BO |
|---|---|
| Summary | Check that the IUT discards a Secured CAM when its signing certificate contains two records with AID_CAM in the its_aid_ssp_list subject attribute |
| Reference | ETSI TS 103 097 [1], clause 7.4.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_12_04_BO_AT
ensure that
   when the IUT is receiving a Secured CAM (MSG_SEC_RCV_CAM_01)
      containing header_fields ['its_aid']
         containing its_aid
            indicating 'AID_CAM'
      and containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_12_04_BO_AT)
               containing subject_attributes['its_aid_ssp_list']
                  containing item [0].its_aid
                     indicating 'AID_CAM'
                  and containing item [1].its_aid
                     indicating 'AID_CAM'
   then
      the IUT discards the message
```

### 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 |
| **Summary** | Check that the IUT discards a message when the signing AT certificate contains a CAM AID-SSP 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** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_13_01_BO_AT<br>ensure that<br>when the IUT is receiving a Secured CAM (MSG_SEC_RCV_CAM_01)<br>containing header_fields ['signer_info'].signer.certificate (CERT_TS_13_01_BO_AT)<br>containing signer_info.digest<br>referencing to CERT_TS_13_01_BO_AA<br>containing subject_attributes['its_aid_list']<br>not containing 'AID_CAM'<br>and containing subject_attributes['its_aid_ssp_list']<br>containing a record<br>containing its_aid<br>indicating 'AID_CAM'<br>then<br>the IUT discards the message | |

| | |
|---|---|
| **TP Id** | 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-SSP record whereas the issuing AA certificate does not contain the AID record with AID_DENM |
| **Reference** | ETSI TS 103 097 [1], clause 7.4.1 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_13_02_BO_AT<br>ensure that<br>when the IUT is receiving a Secured DENM (MSG_SEC_RCV_DENM_A)<br>containing header_fields ['signer_info'].signer.certificate (CERT_TS_13_02_BO_AT)<br>containing signer_info.digest<br>referencing to CERT_TS_13_02_BO_AA<br>containing subject_attributes['its_aid_list']<br>not containing 'AID_DENM'<br>and containing subject_attributes['its_aid_ssp_list']<br>containing a record<br>containing its_aid<br>indicating 'AID_DENM'<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_CERT_13_03_BO |
|---|---|
| Summary | Check that IUT discards a SecuredMessage if the AA certificate does not contain a subject_attribute of type its_aid_list |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_13_03_BO_AT<br>ensure that<br>when the IUT is receiving a Secured CAM (MSG_SEC_RCV_CAM_01)<br>containing header_fields ['signer_info'].signer.certificate (CERT_TS_13_03_BO_AT)<br>containing signer_info.digest<br>referencing to CERT_TS_13_03_BO_AA<br>not containing subject_attributes['its_aid_list']<br>then<br>the IUT discards the message | |

### 5.3.5.14 Check the authorization ticket certificate signer info

| TP Id | TP_SEC_ITSS_RCV_CERT_14_01_BO |
|---|---|
| Summary | Check that IUT discards the AT certificate with signer info of type 'certificate' |
| Reference | ETSI TS 103 097 [1], clause 7.4.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_14_01_BO_AT<br>ensure that<br>when the IUT is receiving a SecuredMessage<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>and containing certificate (CERT_TS_14_01_BO_AT)<br>containing signer_info<br>containing type<br>indicating 'certificate'<br>and containing certificate<br>indicating CERT_TS_AA_A<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_CERT_14_02_BO |
|---|---|
| Summary | Check that IUT discards the AT certificate with signer info of type 'certificate_chain' |
| Reference | ETSI TS 103 097 [1], clause 7.4.2 |
| PICS Selection | PICS_GN_SECURITY |
| **Expected behaviour** | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_14_02_BO_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_14_02_BO_AT)
               containing signer_info
                  containing type
                     indicating 'certificate_chain'
                  and containing certificates[0]
                     indicating certificate (CERT_TEST_ROOT)
                  and containing certificates[1]
                     indicating certificate (CERT_TS_AA_A)
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_14_03_BO |
|---|---|
| Summary | Check that IUT discards the AT certificate with signer info of type 'certificate_digest_with_other_algorithm' |
| Reference | ETSI TS 103 097 [1], clause 7.4.2 |
| PICS Selection | PICS_GN_SECURITY |
| **Expected behaviour** | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_14_03_BO_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_14_03_BO_AT)
               containing signer_info
                  containing type
                     indicating 'certificate_digest_with_other_algorithm'
                  and containing digest
                     referencing CERT_TS_AA_A
   then
      the IUT discards the message
```

### 5.3.5.15 Check the authorization authority certificate signer info

| **TP Id** | TP_SEC_ITSS_RCV_CERT_15_01_BO |
|---|---|
| **Summary** | Check that IUT discards the AA certificate with signer info of type 'certificate' |
| **Reference** | ETSI TS 103 097 [1], clause 7.4.4 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_15_01_BO_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_15_01_BO_AT)
               containing signer_info.digest
                  referencing to certificate (CERT_TS_15_01_BO_AA)
                     containing signer_info
                        containing type
                           indicating 'certificate'
                        and containing certificate
                           indicating CERT_TEST_ROOT
   then
      the IUT discards the message
```

| **TP Id** | TP_SEC_ITSS_RCV_CERT_15_02_BO |
|---|---|
| **Summary** | Check that IUT discards the AA certificate with signer info of type 'certificate_chain' |
| **Reference** | ETSI TS 103 097 [1], clause 7.4.4 |
| **PICS Selection** | PICS_GN_SECURITY |
| **Expected behaviour** | |

```
with
   the IUT being in the 'authorized' state
   and the IUT current time is inside the time validity period of CERT_TS_15_02_BO_AT
ensure that
   when the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info']
         containing signer
            containing type
               indicating 'certificate'
            and containing certificate (CERT_TS_15_02_BO_AT)
               containing signer_info.digest
                  referencing to certificate (CERT_TS_15_02_BO_AA)
                     containing signer_info
                        containing type
                           indicating 'certificate_chain'
                        and containing certificates[0]
                           indicating certificate (CERT_ROOT)
                        and containing certificates[1]
                           indicating certificate (CERT_TS_15_02_BO_CA)
                              containing signer_info
                                 containing type
                                    indicating 'certificate_digest_with_sha256'
                                 and containing digest
                                    referencing to CERT_TEST_ROOT
   then
      the IUT discards the message
```

| TP Id | TP_SEC_ITSS_RCV_CERT_15_03_BO |
|---|---|
| Summary | Check that IUT discards the AA certificate with signer info of type 'certificate_digest_with_other_algorithm' |
| Reference | ETSI TS 103 097 [1], clause 7.4.4 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_15_03_BO_AT<br>ensure that<br>when the IUT is receiving a SecuredMessage<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>and containing certificate (CERT_TS_15_03_BO_AT)<br>containing signer_info.digest<br>referencing to certificate (CERT_TS_15_03_BO_AA)<br>containing signer_info<br>containing type<br>indicating 'certificate_digest_with_other_algorithm'<br>and containing digest<br>referencing CERT_TEST_ROOT<br>then<br>the IUT discards the message | |

### 5.3.5.16 Check the subject_name of the AT certificate

| TP Id | TP_SEC_ITSS_RCV_CERT_16_01_BO |
|---|---|
| Summary | Check that IUT discards a SecuredMessage if the subject_name of the AT certificate is not an empty name field |
| Reference | ETSI TS 103 097 [1], clause 7.4.2 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_16_01_BO_AT<br>ensure that<br>when the IUT is receiving a SecuredMessage<br>containing header_fields ['signer_info']<br>containing signer<br>containing type<br>indicating 'certificate'<br>and containing certificate (CERT_TS_14_01_BO_AT)<br>containing subject_info.subject_name<br>indicating non-empty string ('Invalid name')<br>then<br>the IUT discards the message | |

### 5.3.5.17 Check certificate assurance level presence and values

| TP Id | TP_SEC_ITSS_RCV_CERT_17_01_BO |
|---|---|
| Summary | Check that IUT discards a SecuredMessage if the subject attribute of type assurance_level is missing in the AT certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_17_01_BO_AT<br>ensure that<br>when the IUT is receiving a Secured CAM (MSG_SEC_RCV_CAM_1)<br>containing header_fields ['signer_info'].signer<br>containing type<br>indicating 'certificate'<br>and containing certificate (CERT_TS_17_01_BO_AT)<br>not containing subject_attributes['assurance_level']<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_CERT_17_02_BO |
|---|---|
| Summary | Check that IUT discards a SecuredMessage if the subject attribute of type assurance_level is missing in the AA certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY |
| **Expected behaviour** | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_17_02_BO_AT<br>ensure that<br>when the IUT is receiving a Secured CAM (MSG_SEC_RCV_CAM_1)<br>containing header_fields ['signer_info'].signer<br>containing type<br>indicating 'certificate'<br>and containing certificate (CERT_TS_17_02_BO_AT)<br>containing signer_info.digest<br>referencing to certificate (CERT_TS_17_02_BO_AA)<br>not containing subject_attributes['assurance_level']<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_CERT_17_03_BO |
|---|---|
| Summary | Check that IUT discards a SecuredMessage if the assurance level of issuing certificate is less then assurance level of subordinate certificate |
| 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
  and the IUT current time is inside the time validity period of CERT_TS_17_03_BO_AT
ensure that
  when the IUT is receiving a Secured CAM (MSG_SEC_RCV_CAM_1)
    containing header_fields ['signer_info'].signer
      containing type
        indicating 'certificate'
      and containing certificate (CERT_TS_17_03_BO_AT)
        containing subject_attributes['assurance_level']
          containing assurance_level
            indicating 0x80 (assurance level=4, confidence=0)
        and containing signer_info.digest
          referencing to certificate (CERT_TS_A_AA)
            containing subject_attributes['assurance_level']
              containing assurance_level
                indicating 0x60 (assurance level=3, confidence=0)
  then
    the IUT discards the message

| TP Id | TP_SEC_ITSS_RCV_CERT_17_04_BO |
|---|---|
| Summary | Check that IUT discards a SecuredMessage if the assurance level of issuing certificate is equal to the assurance level of the subordinate certificate but the confidence of subject assurance of issuing certificate is less then the confidence of the subordinate certificate |
| 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
  and the IUT current time is inside the time validity period of CERT_TS_17_04_BO_AT
ensure that
  when the IUT is receiving a Secured CAM (MSG_SEC_RCV_CAM_1)
    containing header_fields ['signer_info'].signer
      containing type
        indicating 'certificate'
      and containing certificate (CERT_TS_17_04_BO_AT)
        containing subject_attributes['assurance_level']
          containing assurance_level
            indicating 0x61 (assurance level=3, confidence=1)
        and containing signer_info.digest
          referencing to certificate (CERT_TS_A_AA)
            containing subject_attributes['assurance_level']
              containing assurance_level
                indicating 0x60 (assurance level=3, confidence=0)
  then
    the IUT discards the message

### 5.3.5.18 Check certificate verification key presence

| TP Id | TP_SEC_ITSS_RCV_CERT_18_01_BO |
|---|---|
| Summary | Check that IUT discards a SecuredMessage if the subject attribute of type verification_key is missing in the AT certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_18_01_BO_AT<br>ensure that<br>when the IUT is receiving a Secured CAM (MSG_SEC_RCV_CAM_1)<br>containing header_fields ['signer_info'].signer<br>containing type<br>indicating 'certificate'<br>and containing certificate (CERT_TS_18_01_BO_AT)<br>not containing subject_attributes['verification_key']<br>then<br>the IUT discards the message | |

| TP Id | TP_SEC_ITSS_RCV_CERT_18_02_BO |
|---|---|
| Summary | Check that IUT discards a SecuredMessage if the subject attribute of type verification_key is missing in the AA certificate |
| Reference | ETSI TS 103 097 [1], clause 7.4.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>and the IUT current time is inside the time validity period of CERT_TS_18_02_BO_AT<br>ensure that<br>when the IUT is receiving a Secured CAM (MSG_SEC_RCV_CAM_1)<br>containing header_fields ['signer_info'].signer<br>containing type<br>indicating 'certificate'<br>and containing certificate (CERT_TS_18_02_BO_AT)<br>containing signer_info.digest<br>referencing to certificate (CERT_TS_18_02_BO_AA)<br>not containing subject_attributes['verification_key']<br>then<br>the IUT discards the message | |

### 5.3.5.19 Check invalid region type in validity restriction of certificates

| TP Id | TP_SEC_ITSS_RCV_CERT_19_01_BO |
|---|---|
| Summary | Check that IUT discards a SecuredMessage if the reserved region type has been used in region validity restriction of the AT certificate |
| Reference | ETSI TS 103 097 [1], clause 4.2.21 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | |
| with<br>the IUT being in the 'authorized' state<br>ensure that<br>when<br>the IUT is receiving a SecuredMessage<br>containing header_fields ['signer_info'].signer.certificate (CERT_TS_19_01_BO_AT)<br>containing validity_restrictions['region']<br>containing region_type<br>indicating 240<br>then<br>the IUT discards 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 |
| V1.3.1 | March 2017 | Publication |
| | | |
| | | |