Intelligent Transport Systems (ITS);
Testing;
Conformance test specifications for ITS Security;
Part 2: Test Suite Structure and Test Purposes (TSS & TP)
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.1</td>
<td>Introduction</td>
</tr>
<tr>
<td>5.2</td>
<td>Test Purposes (TP)</td>
</tr>
<tr>
<td>5.2.1</td>
<td>TP definition conventions</td>
</tr>
<tr>
<td>5.2.2</td>
<td>Check that AT certificate is used to sign communication messages of ITS-S</td>
</tr>
<tr>
<td>5.2.3</td>
<td>Check Signature ECC point type</td>
</tr>
<tr>
<td>5.2.4</td>
<td>CAM profile</td>
</tr>
<tr>
<td>5.2.4.1</td>
<td>Check header fields</td>
</tr>
<tr>
<td>5.2.4.2</td>
<td>Check that IUT sends digest as sender info</td>
</tr>
<tr>
<td>5.2.4.3</td>
<td>Check that IUT sends cert to unknown ITS-S</td>
</tr>
<tr>
<td>5.2.4.4</td>
<td>Check that IUT restarts the timer when the certificate has been sent</td>
</tr>
<tr>
<td>5.2.4.5</td>
<td>Check that IUT sends certificate when requested</td>
</tr>
<tr>
<td>5.2.4.6</td>
<td>Check that IUT send certificate chain when requested</td>
</tr>
<tr>
<td>5.2.4.7</td>
<td>Check generation time</td>
</tr>
<tr>
<td>5.2.4.8</td>
<td>Check secured CAM its_aid value</td>
</tr>
<tr>
<td>5.2.4.9</td>
<td>Check sending certificate request to unknown station</td>
</tr>
<tr>
<td>5.2.4.10</td>
<td>Check Payload</td>
</tr>
<tr>
<td>5.2.4.11</td>
<td>Check presence of trailer field</td>
</tr>
<tr>
<td>5.2.4.12</td>
<td>Check signature</td>
</tr>
<tr>
<td>5.2.5</td>
<td>DENM profile</td>
</tr>
<tr>
<td>5.2.5.1</td>
<td>Check header fields</td>
</tr>
<tr>
<td>5.2.5.2</td>
<td>Check that signer info is a certificate</td>
</tr>
<tr>
<td>5.2.5.3</td>
<td>Check generation time</td>
</tr>
<tr>
<td>5.2.5.4</td>
<td>Check generation location</td>
</tr>
<tr>
<td>5.2.5.5</td>
<td>Check secured DENM its_aid value</td>
</tr>
<tr>
<td>5.2.5.6</td>
<td>Check Payload</td>
</tr>
<tr>
<td>5.2.5.7</td>
<td>Check trailer field presence</td>
</tr>
<tr>
<td>5.2.5.8</td>
<td>Check signature</td>
</tr>
<tr>
<td>5.2.6</td>
<td>Generic signed message profile</td>
</tr>
<tr>
<td>5.2.6.1</td>
<td>Check header field</td>
</tr>
<tr>
<td>5.2.6.2</td>
<td>Check that signer info is a certificate</td>
</tr>
<tr>
<td>5.2.6.3</td>
<td>Check generation time</td>
</tr>
<tr>
<td>5.2.6.4</td>
<td>Check generation location</td>
</tr>
<tr>
<td>5.2.6.5</td>
<td>Check payload</td>
</tr>
<tr>
<td>5.2.6.6</td>
<td>Check signature</td>
</tr>
<tr>
<td>5.2.7</td>
<td>Profiles for certificates</td>
</tr>
<tr>
<td>5.2.7.1</td>
<td>Check that certificate version is 2</td>
</tr>
<tr>
<td>Section</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>-------------</td>
</tr>
<tr>
<td>5.2.7.2</td>
<td>Check the certificate chain</td>
</tr>
<tr>
<td>5.2.7.3</td>
<td>Geographical regions</td>
</tr>
<tr>
<td>5.2.7.3.1</td>
<td>Check Rectangular regions</td>
</tr>
<tr>
<td>5.2.7.3.2</td>
<td>Check Polygonal Region</td>
</tr>
<tr>
<td>5.2.7.3.3</td>
<td>Check Identified Region</td>
</tr>
<tr>
<td>5.2.7.4</td>
<td>Check ECC point type of the certificate signature</td>
</tr>
<tr>
<td>5.2.7.5</td>
<td>Check ECC point type of the certificate verification key</td>
</tr>
<tr>
<td>5.2.7.6</td>
<td>Check the certificate signature</td>
</tr>
<tr>
<td>5.2.7.7</td>
<td>AA certificate profile</td>
</tr>
<tr>
<td>5.2.7.7.1</td>
<td>Check the subject type</td>
</tr>
<tr>
<td>5.2.7.7.2</td>
<td>Check AA certificate subject name</td>
</tr>
<tr>
<td>5.2.7.7.3</td>
<td>Check that signer info is a digest</td>
</tr>
<tr>
<td>5.2.7.7.4</td>
<td>Check subject attributes presence and order</td>
</tr>
<tr>
<td>5.2.7.7.5</td>
<td>Check the time_start_and_end presence</td>
</tr>
<tr>
<td>5.2.7.7.6</td>
<td>Check verification key validity</td>
</tr>
<tr>
<td>5.2.7.7.7</td>
<td>Check ITS-AID</td>
</tr>
<tr>
<td>5.2.7.7.8</td>
<td>Check that AA cert is signed by Root cert</td>
</tr>
<tr>
<td>5.2.7.7.9</td>
<td>Check validity restriction presence and order</td>
</tr>
<tr>
<td>5.2.7.8</td>
<td>AT certificate profile</td>
</tr>
<tr>
<td>5.2.7.8.1</td>
<td>Check subject type</td>
</tr>
<tr>
<td>5.2.7.8.2</td>
<td>Check that signer info is a digest</td>
</tr>
<tr>
<td>5.2.7.8.3</td>
<td>Check subject name</td>
</tr>
<tr>
<td>5.2.7.8.4</td>
<td>Check the presence and the order of subject attributes</td>
</tr>
<tr>
<td>5.2.7.8.5</td>
<td>Check presence of time_start_and_end validity restriction</td>
</tr>
<tr>
<td>5.2.7.8.6</td>
<td>Check verification key validity</td>
</tr>
<tr>
<td>5.2.7.8.7</td>
<td>Check ITS-AID-SSP</td>
</tr>
<tr>
<td>5.2.7.8.8</td>
<td>Check that AT certificate is signed by AA cert</td>
</tr>
<tr>
<td>5.2.7.8.9</td>
<td>Check assurance level</td>
</tr>
<tr>
<td>5.2.7.8.10</td>
<td>Check validity restriction presence and order</td>
</tr>
<tr>
<td>5.3</td>
<td>Receiver Behaviour</td>
</tr>
<tr>
<td>5.3.1</td>
<td>Overview</td>
</tr>
<tr>
<td>5.3.2</td>
<td>CAM Profile</td>
</tr>
<tr>
<td>5.3.2.1</td>
<td>Check that IUT accepts well-formed Secured CAM</td>
</tr>
<tr>
<td>5.3.2.2</td>
<td>Check the message protocol version</td>
</tr>
<tr>
<td>5.3.2.3</td>
<td>Check header fields</td>
</tr>
<tr>
<td>5.3.2.4</td>
<td>Check signer info</td>
</tr>
<tr>
<td>5.3.2.5</td>
<td>Check generation time</td>
</tr>
<tr>
<td>5.3.2.6</td>
<td>Check its_aid</td>
</tr>
<tr>
<td>5.3.2.7</td>
<td>Check payload</td>
</tr>
<tr>
<td>5.3.2.8</td>
<td>Check presence of trailer field</td>
</tr>
<tr>
<td>5.3.2.9</td>
<td>Check signature</td>
</tr>
<tr>
<td>5.3.2.10</td>
<td>Check signing certificate type</td>
</tr>
<tr>
<td>5.3.3</td>
<td>DENM Profile</td>
</tr>
<tr>
<td>5.3.3.1</td>
<td>Check that IUT accepts well-formed Secured DENM</td>
</tr>
<tr>
<td>5.3.3.2</td>
<td>Check the message protocol version</td>
</tr>
<tr>
<td>5.3.3.3</td>
<td>Check header fields</td>
</tr>
<tr>
<td>5.3.3.4</td>
<td>Check signer info</td>
</tr>
<tr>
<td>5.3.3.5</td>
<td>Check generation time</td>
</tr>
<tr>
<td>5.3.3.6</td>
<td>Check its_aid</td>
</tr>
<tr>
<td>5.3.3.7</td>
<td>Check generation location</td>
</tr>
<tr>
<td>5.3.3.8</td>
<td>Check Payload</td>
</tr>
<tr>
<td>5.3.3.9</td>
<td>Check presence of trailer field</td>
</tr>
<tr>
<td>5.3.3.10</td>
<td>Check signature</td>
</tr>
<tr>
<td>5.3.3.11</td>
<td>Check signing certificate type</td>
</tr>
<tr>
<td>5.3.4</td>
<td>Generic Signed Message Profile</td>
</tr>
<tr>
<td>5.3.4.1</td>
<td>Check that IUT accepts well-formed GN Beacon message</td>
</tr>
<tr>
<td>5.3.4.2</td>
<td>Check the message protocol version</td>
</tr>
<tr>
<td>5.3.4.3</td>
<td>Check header fields</td>
</tr>
<tr>
<td>5.3.4.4</td>
<td>Check signer info</td>
</tr>
<tr>
<td>5.3.4.5</td>
<td>Check generation time</td>
</tr>
<tr>
<td>5.3.4.6</td>
<td>Check generation location</td>
</tr>
<tr>
<td>5.3.4.7</td>
<td>Check Payload</td>
</tr>
</tbody>
</table>
5.3.4.8  Check presence of trailer field ................................................................. 117
5.3.4.9  Check signature ...................................................................................... 118
5.3.4.10 Check signing certificate type ................................................................. 119
5.3.5  Profiles for certificates ............................................................................. 120
5.3.5.1 Check that certificate version is 2 ............................................................. 120
5.3.5.2 Check that enrolment certificate is not used for sign other certificates .......... 121
5.3.5.3 Check that any certificate signed with AT certificate is not accepted .......... 121
5.3.5.4 Check that AA certificate signed with other AA certificate is not accepted .... 122
5.3.5.5 Check the certificate signature ............................................................... 122
5.3.5.6 Check circular region of subordinate certificate ......................................... 123
5.3.5.7 Check rectangular region of subordinate certificate ................................. 126
5.3.5.8 Check polygonal region of subordinate certificate ..................................... 129
5.3.5.9 Check identified region of subordinate certificate ...................................... 133
5.3.5.10 Check time validity restriction presence .................................................. 140
5.3.5.11 Check time validity restriction conforming to the issuing certificate .......... 141
5.3.5.12 Check AID subject attribute presence ..................................................... 143
5.3.5.13 Check AID-SSP subject attribute value conforming to the issuing certificate ... 145

Annex A (informative): Bibliography ................................................................. 146

History ............................................................................................................. 147
Intellectual Property Rights

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

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

Foreword

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

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

- **Part 1:** "Protocol Implementation Conformance Statement (PICS)"
- **Part 2:** "Test Suite Structure and Test Purposes (TSS & TP)"
- **Part 3:** "Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)"

Modal verbs terminology

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

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

The present document provides the Test Suite Structure and Test Purposes (TSS & TP) for Security as defined in ETSI TS 103 097 [1] in accordance with the relevant guidance given in ISO/IEC 9646-7 [7]. The ISO standard for the methodology of conformance testing (ISO/IEC 9646-1 [4] and ISO/IEC 9646-2 [5]) as well as the ETSI rules for conformance testing (ETSI ETS 300 406 [8]) are used as a basis for the test methodology.

2 References

2.1 Normative references

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

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

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

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

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


2.2 Informative references

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

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

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

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

3 Definitions and abbreviations

3.1 Definitions

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

3.2 Abbreviations

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

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>AA</td>
<td>Authorization Authority</td>
</tr>
<tr>
<td>AID</td>
<td>Application Identifier</td>
</tr>
<tr>
<td>AT</td>
<td>Authorization Ticket</td>
</tr>
<tr>
<td>ATS</td>
<td>Abstract Test Suite</td>
</tr>
<tr>
<td>BO</td>
<td>Exceptional Behaviour</td>
</tr>
<tr>
<td>BV</td>
<td>Valid Behaviour</td>
</tr>
<tr>
<td>CAM</td>
<td>Co-operative Awareness Messages</td>
</tr>
<tr>
<td>CAN</td>
<td>Controller Area Network</td>
</tr>
<tr>
<td>CERT</td>
<td>Certificate</td>
</tr>
<tr>
<td>DE</td>
<td>Data Element</td>
</tr>
<tr>
<td>DENM</td>
<td>Decentralized Environmental Notification Message</td>
</tr>
<tr>
<td>EA</td>
<td>Enrolment Authority</td>
</tr>
<tr>
<td>ECC</td>
<td>Elliptic Curve Cryptography</td>
</tr>
<tr>
<td>GN</td>
<td>GeoNetworking</td>
</tr>
<tr>
<td>ITS</td>
<td>Intelligent Transportation Systems</td>
</tr>
<tr>
<td>ITS-S</td>
<td>Intelligent Transport System - Station</td>
</tr>
<tr>
<td>IUT</td>
<td>Implementation under Test</td>
</tr>
<tr>
<td>MSG</td>
<td>Message</td>
</tr>
<tr>
<td>PICS</td>
<td>Protocol Implementation Conformance Statement</td>
</tr>
<tr>
<td>SSP</td>
<td>Service Specific Permissions</td>
</tr>
<tr>
<td>TP</td>
<td>Test Purposes</td>
</tr>
<tr>
<td>TSS</td>
<td>Test Suite Structure</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Root</th>
<th>Group</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>ITS-S data transfer</td>
<td>Valid</td>
</tr>
<tr>
<td></td>
<td>ITS-S - AA authorization</td>
<td>Valid</td>
</tr>
<tr>
<td></td>
<td>ITS-S - EA enrolment</td>
<td>Valid</td>
</tr>
<tr>
<td></td>
<td>Sending behaviour</td>
<td>Valid</td>
</tr>
<tr>
<td></td>
<td>Receiving behaviour</td>
<td>Valid and Invalid</td>
</tr>
<tr>
<td></td>
<td>Generic messages</td>
<td>Valid</td>
</tr>
<tr>
<td></td>
<td>CAM testing</td>
<td>Valid</td>
</tr>
<tr>
<td></td>
<td>DENM testing</td>
<td>Valid</td>
</tr>
<tr>
<td></td>
<td>Certificate testing</td>
<td>Valid</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Identifier</th>
<th>TP &lt;root&gt; &lt;tgt&gt; &lt;gr&gt; &lt;sgr&gt; &lt;rn&gt; &lt;sn&gt; &lt;x&gt;</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;root&gt; = root</td>
<td>SEC</td>
<td>ITS-S data transfer</td>
</tr>
<tr>
<td>&lt;tgt&gt; = target</td>
<td>ITSS</td>
<td>ITS-S - AA authorization</td>
</tr>
<tr>
<td></td>
<td>AA</td>
<td>ITS-S - EA enrolment</td>
</tr>
<tr>
<td>&lt;gr&gt; = group</td>
<td>SND</td>
<td>Sending behaviour</td>
</tr>
<tr>
<td></td>
<td>RCV</td>
<td>Receiving behaviour</td>
</tr>
<tr>
<td>&lt;sgr&gt; = sub-group</td>
<td>MSG</td>
<td>Generic messages</td>
</tr>
<tr>
<td></td>
<td>CAM</td>
<td>CAM testing</td>
</tr>
<tr>
<td></td>
<td>DENM</td>
<td>DENM testing</td>
</tr>
<tr>
<td></td>
<td>CERT</td>
<td>Certificate testing</td>
</tr>
<tr>
<td>&lt;rn&gt; = requirement sequential number</td>
<td>01 to 99</td>
<td>01 to 99</td>
</tr>
<tr>
<td>&lt;sn&gt; = test purpose sequential number</td>
<td>BV</td>
<td>Valid Behaviour tests</td>
</tr>
<tr>
<td>&lt;x&gt; = category</td>
<td>BO</td>
<td>Invalid Behaviour Tests</td>
</tr>
</tbody>
</table>

5.1.3 Rules for the behaviour description

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

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

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

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

5.1.5 Mnemonics for PICS reference

To avoid an update of all TPs when the PICS document is changed, table 3 introduces mnemonics name and the correspondence with the real PICS item number. The PICS item column refers to Table/Item of ETSI TS 103 096-1 [2] if not stated otherwise.

<table>
<thead>
<tr>
<th>Mnemonic</th>
<th>PICS item</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 PICS_GN_SECURITY</td>
<td>A.32/12 ETSI ETSI TS 102 871-1 [3]</td>
</tr>
<tr>
<td>2 PICS_CERTIFICATE_SELECTION</td>
<td>A.3/1</td>
</tr>
<tr>
<td>3 PICS_USE_CIRCULAR_REGION</td>
<td>A.4/2</td>
</tr>
<tr>
<td>4 PICS_USE_RECTANGULAR_REGION</td>
<td>A.4/3</td>
</tr>
<tr>
<td>5 PICS_USE_POLYGONAL_REGION</td>
<td>A.4/4</td>
</tr>
<tr>
<td>6 PICS_USE_IDENTIFIED_REGION</td>
<td>A.4/5</td>
</tr>
<tr>
<td>7 PICS_USE_ISO31661_REGION_DICTIONARY</td>
<td>A.6/1</td>
</tr>
<tr>
<td>8 PICS_USE_UN_STATS_REGION_DICTIONARY</td>
<td>A.5/1</td>
</tr>
<tr>
<td>9 PICS_USE_UN_STATS_REGION_DICTIONARY</td>
<td>A.5/2</td>
</tr>
</tbody>
</table>

5.2 Sending behaviour

5.2.1 Check the message protocol version

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_MSG_01_01_BV</th>
<th>Summary</th>
<th>Reference</th>
<th>PICS Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Check that ITS-S sends a SecuredMessage containing protocol version set to 2</td>
<td>ETSI TS 103 097 [1], clause 5.2</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

Expected behaviour

with {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is requested to send a SecuredMessage
  } then {
    the IUT sends a SecuredMessage
    containing protocol_version
    indicating value '2'
  }
}
5.2.2 Check that AT certificate is used to sign communication messages of ITS-S

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

---

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

---
5.2.3 Check Signature ECC point type

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_MSG_05_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 4.2.9</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>
| **Expected behaviour** | with {
| | the IUT being in the 'authorized' state |
| | ensure that {
| | when {
| | the IUT is requested to send a CAM |
| | then {
| | the IUT sends a SecuredMessage {
| | containing header_fields['its_aid'] |
| | containing its_aid |
| | indicating 'AID_CAM' |
| | and containing trailer_fields['signature'] |
| | containing signature.ecdsa_signature |
| | containing R.type |
| | indicating compressed_lsb_y_0 |
| | or indicating compressed_lsb_y_1 |
| | or indicating x_coordinate_only |
| | }
| | }
| | }

5.2.4 CAM profile

5.2.4.1 Check header fields

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CAM_02_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that the secured CAM contains exactly one element of these header fields: signer_info, generation_time, its_aid</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td>Check that generation_time_standard_deviation, expiration, encryption_parameters, recipient_info are not used</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>
| **Expected behaviour** | with {
| | the IUT being in the 'authorized' state |
| | ensure that {
| | when {
| | the IUT is requested to send a CAM |
| | then {
| | the IUT sends a SecuredMessage {
| | containing header_fields[0] |
| | containing type |
| | indicating 'signer_info' |
| | and containing header_fields [n].type |
| | indicating value < header_fields [n+1].type |
| | and containing header_fields ['generation_time'] |
| | and containing header_fields['its_aid'] |
| | indicating 'AID_CAM' |
| | and not containing header_fields['generation_time_standard_deviation'] |
| | and not containing header_fields['expiration'] |
| | and not containing header_fields['encryption_parameters'] |
| | and not containing header_fields['recipient_info'] |
| | }
| | }
| | }
5.2.4.2 Check that IUT sends digest as sender info

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CAM_05_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>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</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td></td>
<td><strong>Expected behaviour</strong></td>
</tr>
<tr>
<td></td>
<td>with {</td>
</tr>
<tr>
<td></td>
<td>the IUT being in the 'authorized' state</td>
</tr>
<tr>
<td></td>
<td>and the IUT is configured to send more than one CAM per second</td>
</tr>
<tr>
<td></td>
<td>and the IUT having sent a CAM</td>
</tr>
<tr>
<td></td>
<td>containing header_fields['signer_info'].signer.type</td>
</tr>
<tr>
<td></td>
<td>indicating 'certificate'</td>
</tr>
<tr>
<td></td>
<td>containing generation_time</td>
</tr>
<tr>
<td></td>
<td>indicating TIME_LAST</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>ensure that {</td>
</tr>
<tr>
<td></td>
<td>when {</td>
</tr>
<tr>
<td></td>
<td>the IUT sends one of the next SecuredMessage</td>
</tr>
<tr>
<td></td>
<td>containing header_fields['signer_info'] {</td>
</tr>
<tr>
<td></td>
<td>containing signer {</td>
</tr>
<tr>
<td></td>
<td>containing type</td>
</tr>
<tr>
<td></td>
<td>indicating 'certificate'</td>
</tr>
<tr>
<td></td>
<td>containing certificate</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>} containing header_fields['its_aid']</td>
</tr>
<tr>
<td></td>
<td>indicating 'AID_CAM'</td>
</tr>
<tr>
<td></td>
<td>} then {</td>
</tr>
<tr>
<td></td>
<td>this message</td>
</tr>
<tr>
<td></td>
<td>contains header_fields['generation_time']</td>
</tr>
<tr>
<td></td>
<td>indicating TIME (TIME &gt;= TIME_LAST + 1sec)</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CAM_05_02_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>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</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td></td>
<td><strong>Expected behaviour</strong></td>
</tr>
<tr>
<td></td>
<td>with {</td>
</tr>
<tr>
<td></td>
<td>the IUT being in the 'authorized' state</td>
</tr>
<tr>
<td></td>
<td>and the IUT is configured to send more than one CAM per second</td>
</tr>
<tr>
<td></td>
<td>and the IUT having sent a CAM</td>
</tr>
<tr>
<td></td>
<td>containing header_fields['signer_info'].signer.type</td>
</tr>
<tr>
<td></td>
<td>indicating 'certificate'</td>
</tr>
<tr>
<td></td>
<td>at TIME_1</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>ensure that {</td>
</tr>
<tr>
<td></td>
<td>when {</td>
</tr>
<tr>
<td></td>
<td>the IUT is requested to send next CAM right after 1 second after the TIME_1</td>
</tr>
<tr>
<td></td>
<td>} then {</td>
</tr>
<tr>
<td></td>
<td>the IUT sends a SecuredMessage {</td>
</tr>
<tr>
<td></td>
<td>containing header_fields['its_aid']</td>
</tr>
<tr>
<td></td>
<td>indicating 'AID_CAM'</td>
</tr>
<tr>
<td></td>
<td>containing header_fields['signer_info'] {</td>
</tr>
<tr>
<td></td>
<td>containing signer {</td>
</tr>
<tr>
<td></td>
<td>containing type</td>
</tr>
<tr>
<td></td>
<td>indicating 'certificate'</td>
</tr>
<tr>
<td></td>
<td>containing certificate</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>
5.2.4.3 Check that IUT sends cert to unknown ITS-S

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CAM_06_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>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</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
    the IUT being in the 'authorized' state  
    and the IUT is configured to send more than one CAM per second  
    and the IUT having already sent CAM at TIME_1  
        containing header_fields['signer_info'].signer.type  
        indicating 'certificate'  
    and the IUT having received a SecuredMessage  
        at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec)  
        containing header_fields['its_aid']  
        indicating 'AID_CAM'  
        containing header_fields['signer_info'] {  
            containing signer  
            containing type  
                indicating 'certificate_digest_with_sha256'  
                containing digest  
                indicating HashedId3 value  
                referenced to unknown certificate  
        }  
}

ensure that {
    when {
        the IUT is requested to send CAM  
        at TIME_3 (TIME_1 < TIME_2 < TIME_3 < TIME_1 + 1sec)  
    } then {
        the IUT sends a SecuredMessage {  
            containing header_fields['its_aid']  
            indicating 'AID_CAM'  
            containing header_fields[0] {  
                containing type  
                    indicating 'signer_info'  
                    containing signer {  
                        containing type  
                            indicating 'certificate'  
                            containing certificate  
                    }  
            }  
        }  
    }  
}
5.2.4.4 Check that IUT restarts the timer when the certificate has been sent

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CAM_07a_01_TI</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT restarts the certificate sending timer when the certificate has been sent</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**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'
      containing header_fields['signer_info'].signer.digest
        referenced to 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 of 1sec
  }
}
5.2.4.5 Check that IUT sends certificate when requested

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC.ITSS_SND_CAM_08_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>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</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**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 security_profile
        indicating '1'
      containing header_fields['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate
            referenced by the requested digest
        }
      }
    }
  }
}
### 5.2.4.6 Check that IUT send certificate\_chain when requested

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CAM_09_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>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.</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**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 a CAM
  containing header\_fields['signer\_info'].signer.type
    indicating 'certificate'
    at TIME\_1
  and the IUT having received a SecuredMessage
  containing header\_fields['request\_unrecognized\_certificate']
    containing digests
      containing HashedId3 value
        referencing to the AA certificate
    at TIME\_2 (TIME\_1 < TIME\_2 < TIME\_1+1sec)
}

ensure that {
  when {
    the IUT is requested to send a CAM
    at TIME\_3 (TIME\_1 < TIME\_2 < TIME\_3 < TIME\_1+1sec)
  } then {
    the IUT sends a SecuredMessage
    containing header\_fields['its\_aid']
      indicating 'AID\_CAM'
    containing header\_fields['signer\_info']
      containing signer
        containing type
          indicating 'certificate\_chain'
        containing certificates[last]
          indicating the AT certificate
        containing certificates[last-1]
          indicating the AA certificate
  }
}
5.2.4.7 Check generation time

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CAM_10_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that message generation time is inside the validity period of the signing certificate; Check that message generation time value is realistic</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 5.4 and 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**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 TIME_1 (CUR_TIME - 5min <= TIME_1 <= CUR_TIME + 5min)
      }
    } containing header_fields ['signer_info'] {
      containing signer {
        containing type
        indicating 'certificate'
        containing certificate {
          not containing validity_restrictions['time_start_and_end']
          or containing validity_restrictions['time_start_and_end'] {
            containing start_validity
            indicating value <= TIME_1
            containing end_validity
            indicating value > TIME_1
          }
        }
      }
    }
    containing its_aid
    indicating 'AID_CAM'
  }
}

5.2.4.8 Check secured CAM its_aid value

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CAM_11_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the sent Secured CAM contains exactly one HeaderField its_aid that is set to 'AID_CAM'</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 5.4 and 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is requested to send CAM
  } then {
    the IUT sends a SecuredMessage {
      containing header_fields ['its_aid'] {
        containing its_aid
        indicating 'AID_CAM'
      }
    }
}

ETSI
5.2.4.9 Check sending certificate request to unknown station

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CAM_12_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the IUT sends certificate request when it receives a message from unknown station</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

Expected behaviour

with {
    the IUT being in the 'authorized' state
    and the IUT has receiving a SecuredMessage {
        containing header_fields['signer_info'].signer {
            containing type
                indicating 'certificate_digest_with_sha256'
            containing digest
                indicating HashedId3 value DIGEST_A
                referenced to unknown certificate
        }
    }
}

ensure that {
    when {
        the IUT is requested to send CAM
    } then {
        the IUT sends a SecuredMessage {
            containing header_fields['request_unrecognized_certificate'] {
                containing digests
                    containing HashedId3 value DIGEST_A
            }
            containing header_fields['its_aid'] {
                containing its_aid
                    indicating 'AID_CAM'
            }
        }
    }
}

5.2.4.10 Check Payload

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CAM_14_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the Secured CAM contains non-empty payload of type signed</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

Expected behaviour

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

ensure that {
    when {
        the IUT is requested to send a CAM
    } then {
        the IUT sends a SecuredMessage {
            containing header_fields['its_aid'] {
                containing its_aid
                    indicating 'AID_CAM'
            }
            containing payload_field {
                containing type
                    indicating 'signed'
                containing not-empty data
            }
        }
    }
}

5.2.4.11 Check presence of trailer field

Void.
5.2.4.12 Check signature

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CAM_16_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the secured CAM contains only one TrailerField of type signature; Check that the signature contained in the SecuredMessage is calculated over the right fields by cryptographically verifying the signature</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

Expected behaviour

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is requested to send a CAM
  } then {
    the IUT sends a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
          indicating 'certificate_digest_with_ecdsap256'
          containing digest
          referenced to the certificate
          containing subject_info.subject_type
          indicating 'authorization_ticket' (2)
          and containing subject_attributes['verification key'] (KEY)
        }
      } or containing signer {
        containing type
        indicating 'certificate'
        containing certificate
        containing subject_info.subject_type
        indicating 'authorization_ticket' (2)
        and containing subject_attributes['verification key'] (KEY)
      }
      containing header_fields ['its_aid'] {
        containing its_aid
        indicating 'AID_CAM'
      }
      containing trailer_fields {
        containing single instance of type TrailerField {
          containing type
          indicating 'signature'
          containing signature
          verifiable using KEY
        }
      }
    }
  }
}
5.2.5  DENM profile

5.2.5.1  Check header fields

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_DENM_02_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the secured DENM contains exactly one element of these header fields: signer_info, generation_time, generation_location, message_type. Check that the header fields are in the ascending order according to the numbering of the enumeration except of the signer_info, which is encoded first. Check that generation_time_with_confidence (generation_time_standard_deviation) is not used.</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is requested to send DENM
  } then {
    the IUT sends a SecuredMessage {
      containing header_fields[0]
      containing type
        indicating 'signer_info'
      containing header_fields[n].type
        indicating value less than header_fields[n+1].type
      containing header_fields['generation_time']
      containing header_fields['generation_location']
      containing header_fields['its_aid'] {
        containing its_aid
          indicating 'AID_DENM'
      }
      not containing header_fields['generation_time_with_confidence']
    }
  }
}
```

5.2.5.2  Check that signer info is a certificate

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_DENM_03_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that secured DENM contains the certificate as a signer_info</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
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['signer_info']{
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate
        }
      }
    }
  }
}
```
### 5.2.5.3 Check generation time

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_DENM_04_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that message generation time is inside the validity period of the signing certificate; Check that message generation time value is realistic</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 5.4 and 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```latex
with \{
  \text{the IUT being in the 'authorized' state}
\}
\text{ensure that (}
  \text{when (}
    \text{the IUT is requested to send a DENM}
  \)} \text{ then (}
    \text{the IUT sends a SecuredMessage (}
      \text{containing exactly one header_fields['generation_time'] (}
        \text{containing generation_time (}
          \text{indicating TIME_1 (CUR_TIME - 10min <= TIME_1 <= CUR_TIME + 5min)}
        \}
      )
    \}
    \text{containing header_fields['signer_info'] (}
      \text{containing signer (}
        \text{containing type (indicating 'certificate')}
        \text{containing certificate (}
          \text{containing validity_restrictions['time_start_and_end'] (}
            \text{containing start_validity (indicating value <= TIME_1)}
            \text{containing end_validity (indicating value > TIME_1)}
          \}
        \or not containing validity_restrictions['time_start_and_end'])
      \}
    \}
  \}
}\}
```

### 5.2.5.4 Check generation location

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_DENM_05_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the secured DENM contains exactly one HeaderField generation_location when AT certificate does not contain any region restrictions</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```latex
with \{
  \text{the IUT has been authorized with the AT certificate (CERT_IUT_A_AT)}
  \text{not containing validity_restrictions['region']}
\}
\text{ensure that (}
  \text{when (}
    \text{the IUT is requested to send DENM}
  \)} \text{ then (}
    \text{the IUT sends a SecuredMessage (}
      \text{containing exactly one header_field ['generation_location']}
      \text{containing generation_location}
      \text{containing header_field ['its_aid'] (}
        \text{containing its_aid (indicating 'AID_DENM')}
      \}
    \}
  \}
}\}
```
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 containing in the validity restriction of the certificate pointed by the signer_info field
Reference | ETSI TS 103 097 [1], clause 7.2
PICS Selection | PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_CIRCULAR_REGION

Expected behaviour

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

TP Id | TP_SEC_ITSS_SND_DENM_05_03_BV
---|---
Summary | Check that the secured DENM contains exactly one HeaderField generation_location which is inside the rectangular region containing in the validity restriction of the certificate pointed by the signer_info field
Reference | ETSI TS 103 097 [1], clause 7.2
PICS Selection | PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION

Expected behaviour

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 a DENM
  } then {
    the IUT sends a SecuredMessage {
      containing exactly one header_field ['generation_location']
      containing generation_location indicating value inside the REGION
      containing header_field ['its_aid'] {
        containing its_aid indicating 'AID_DENM'
      }
    }
  }
}
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_DENM_05_04_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the secured DENM contains exactly one HeaderField generation_location which is inside the polygonal region containing in the validity restriction of the certificate pointed by the signer_info field</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
with {
    the IUT has been authorized with the AT certificate (CERT_IUT_D_AT) {
      containing validity_restrictions ['region'] {
        containing region{
          containing region_type
            indicating 'polygon'
          containing polygonal_region
            indicating REGION
        }
      }
    }
}

ensure that {
    when {
      the IUT is requested to send a DENM
    } then {
      the IUT sends a SecuredMessage {
        containing exactly one header_field ['generation_location']
          containing generation_location
            indicating value inside the REGION
        containing header_field ['its_aid'] {
          containing its_aid
            indicating 'AID_DENM'
        }
      }
    }
}
```
TP Id | TP_SEC_ITSS_SND_DENM_05_05_BV
---|---
Summary | Check that the secured DENM contains exactly one HeaderField generation_location which is inside the identified region containing in the validity restriction of the certificate pointed by the signer_info field
Reference | ETSI TS 103 097 [1], clause 7.2
PICS Selection | PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION

Expected behaviour

with {
  the IUT has been authorized with the AT certificate (CERT_IUT_E_AT) {
    containing validity_restrictions ['region'] {
      containing region{
        containing region_type
        indicating 'id_region'
        containing identified_region
        indicating REGION
      }
    }
  }
}

ensure that {
  when {
    the IUT is requested to send a DENM
  } then {
    the IUT sends a SecuredMessage {
      containing header_fields {
        containing exactly one instance of HeaderField {
          containing type
          indicating 'generation_location'
          containing generation_location
          indicating value inside the REGION
          containing header_field ['its_aid'] {
            containing its_aid
            indicating 'AID_DENM'
          }
        }
      }
    }
  }
}
}
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_DENM_05_06_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the secured GeoNetworking message contains exactly one HeaderField generation_location and this location is inside the certificate validation restriction</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**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
        }
      }
    }
    containing exactly one header_field ['generation_location']
    containing generation_location
    indicating location inside the REGION
  containing header_field ['its_aid'] { 
    containing its_aid
    indicating 'AID_DENM'
  }
  }
}
5.2.5.5 Check secured DENM its_aid value

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_DENM_06_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the sent Secured DENM contains exactly one HeaderField its_aid that is set to 'AID_DENM'</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 5.4 and 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**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 ['its_aid']
      containing its_aid indicating 'AID_DENM'
    }
  }
}

5.2.5.6 Check Payload

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_DENM_08_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the Secured DENM contains non-empty payload of type signed</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**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 ['its_aid'] {
        containing its_aid indicating 'AID_DENM'
      }
      containing payload_field {
        containing type indicating 'signed'
        containing not-empty data
      }
    }
  }
}

5.2.5.7 Check trailer field presence

Void.
### 5.2.5.8 Check signature

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_DENM_10_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the secured DENM contains only one TrailerField of type signature; Check that the signature contained in the SecuredMessage is calculated over the right fields by cryptographically verifying the signature</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

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

5.2.6.1  Check header field

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_GENMSG_02_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the generic secured message contains exactly one element of these header fields: signer_info, generation_time, generation_location. Check that the header fields are in the ascending order according to the numbering of the enumeration except of the signer_info, which is encoded first.</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE</td>
</tr>
</tbody>
</table>

**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 [0].type indicating 'signer_info'
      containing header_fields [1..n] where header_fields [i].type < header_fields [i+1].type
      containing header_fields ['generation_time']
      containing header_fields ['generation_location']
      containing header_fields ['its_aid'] indicating 'AID_BEACON'
    }
  }
}

5.2.6.2  Check that signer info is a certificate

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_GENMSG_03_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that generic secured message contains the certificate as a signer_info</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is requested to send a Beacon
  } then {
    the IUT sends a SecuredMessage {
      containing header_fields ['its_aid'] indicating 'AID_BEACON'
      containing exactly one header_fields ['signer_info'] {
        containing signer {
          containing type indicating 'certificate'
          containing certificate
        }
      }
    }
  }
}
### 5.2.6.3 Check generation time

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_GENMSG_04_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that message generation time is inside the validity period of the signing certificate; Check that message generation time value is realistic</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 5.4 and 7.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE</td>
</tr>
</tbody>
</table>

**Expected behaviour**

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

ensure that {
  when {
    the IUT is requested to send a Beacon 
  } then {
    the IUT sends a SecuredMessage {
      containing header_fields ['its_aid']
      indicating 'AID_BEACON'
      containing exactly one header_fields ['generation_time'] {
        containing generation_time 
        indicating TIME_1 (CUR_TIME - 10min <= TIME_1 <= CUR_TIME + 5min)
      }
      containing header_fields ['signer_info'] {
        containing signer {
          containing type 
          indicating 'certificate'
          containing certificate {
            containing validity_restrictions ['time_start_and_end'] {
              containing start_validity 
              indicating value <= TIME_1
              containing end_validity 
              indicating value > TIME_1
            }
            or not containing validity_restrictions ['time_start_and_end']
          }
        }
      }
    }
  }
}

### 5.2.6.4 Check generation location

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_GENMSG_05_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the secured GeoNetworking message contains exactly one HeaderField generation_location when AT certificate does not contain any region restrictions</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT has been authorized with the AT certificate (CERT_AT_A) 
  does not containing validity_restrictions ['region'] 
} 

ensure that {
  when {
    the IUT is requested to send a Beacon 
  } then {
    the IUT sends a SecuredMessage {
      containing header_fields ['its_aid']
      indicating 'AID_BEACON'
      containing exactly one header_fields ['generation_location']
      containing generation_location
    }
  }
}
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_GENMSG_05_02_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.3</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE, PICS_USE_CIRCULAR_REGION</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td>with {</td>
<td></td>
</tr>
<tr>
<td>the IUT has been authorized with the AT certificate (CERT_AT_B) {</td>
<td></td>
</tr>
<tr>
<td>containing validity_restrictions ['region'] {</td>
<td></td>
</tr>
<tr>
<td>containing region{</td>
<td></td>
</tr>
<tr>
<td>containing region_type indicating 'circle'</td>
<td></td>
</tr>
<tr>
<td>containing circular_region</td>
<td></td>
</tr>
<tr>
<td>indicating REGION</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>ensure that {</td>
<td></td>
</tr>
<tr>
<td>when {</td>
<td></td>
</tr>
<tr>
<td>the IUT is requested to send a Beacon</td>
<td></td>
</tr>
<tr>
<td>} then {</td>
<td></td>
</tr>
<tr>
<td>the IUT sends a SecuredMessage {</td>
<td></td>
</tr>
<tr>
<td>containing header_fields ['its_aid']</td>
<td></td>
</tr>
<tr>
<td>indicating 'AID_BEACON'</td>
<td></td>
</tr>
<tr>
<td>containing exactly one header_fields['generation_location']</td>
<td></td>
</tr>
<tr>
<td>containing generation_location</td>
<td></td>
</tr>
<tr>
<td>indicating value inside the REGION</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_GENMSG_05_03_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.3</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE, PICS_USE_RECTANGULAR_REGION</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td>with {</td>
<td></td>
</tr>
<tr>
<td>the IUT has been authorized with the AT certificate (CERT_AT_C) {</td>
<td></td>
</tr>
<tr>
<td>containing validity_restrictions ['region'] {</td>
<td></td>
</tr>
<tr>
<td>containing region{</td>
<td></td>
</tr>
<tr>
<td>containing region_type indicating 'rectangle'</td>
<td></td>
</tr>
<tr>
<td>containing rectangular_region</td>
<td></td>
</tr>
<tr>
<td>containing instance of RectangularRegion</td>
<td></td>
</tr>
<tr>
<td>indicating REGION</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>ensure that {</td>
<td></td>
</tr>
<tr>
<td>when {</td>
<td></td>
</tr>
<tr>
<td>the IUT is requested to send a Beacon</td>
<td></td>
</tr>
<tr>
<td>} then {</td>
<td></td>
</tr>
<tr>
<td>the IUT sends a SecuredMessage {</td>
<td></td>
</tr>
<tr>
<td>containing header_fields ['its_aid']</td>
<td></td>
</tr>
<tr>
<td>indicating 'AID_BEACON'</td>
<td></td>
</tr>
<tr>
<td>containing exactly one header_fields['generation_location']</td>
<td></td>
</tr>
<tr>
<td>containing generation_location</td>
<td></td>
</tr>
<tr>
<td>indicating value inside the REGION</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>
**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_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE, PICS_USE_POLYGONAL_REGION

**Expected behaviour**

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

---

**TP 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_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE, 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 \( \text{generation}_\text{location} \) and this location is inside the certificate validation restriction
Reference | ETSI TS 103 097 [1], clause 7.3
PICS Selection | PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE

**Expected behaviour**

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

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_GENMSG_06_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the secured message contains the Payload element of type signed, signed_external or signed_and_encrypted</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
    the IUT being in the 'authorized' state
} ensure that {
    when {
        the IUT is requested to send a Beacon
    } then {
        the IUT sends a SecuredMessage {
            containing header_fields ['its_aid']
                indicating 'AID_BEACON'
            and containing payload_field {
                containing type
                    indicating 'signed' or 'signed_external' or 'signed_and_encrypted'
            }
        }
    }
}

### 5.2.6.6 Check signature

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_GENMSG_07_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the secured message contains only one TrailerField of type signature; Check that the signature contained in the SecuredMessage is calculated over the right fields by cryptographically verifying the signature</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY, PICS_ITS_AID_OTHER_PROFILE</td>
</tr>
</tbody>
</table>

**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 ['signer_info'] {
                containing signer {
                    containing type
                        indicating 'certificate'
                    containing certificate
                        indicating CERT
                }
            }
            containing header_fields ['its_aid']
                indicating 'AID_BEACON'
            containing trailer_fields ['signature']
                containing signature
                verifiable using CERT.subject_attributes['verification_key']
        }
    }
}
5.2.7 Profiles for certificates

5.2.7.1 Check that certificate version is 2

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_01_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that AT certificate has version 2</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 6.1 and 7.4</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate in the SecuredMessage
}
ensure that {
  when {
    the IUT is requested to send a SecuredMessage
  } then {
    the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
        containing type
          indicating certificate
        containing certificate {
          containing version
            indicating '2'
        }
      }
  }
}

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_01_02_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that AA certificate has version 2</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 6.1 and 7.4</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate chain in the next CAM
}
ensure that {
  when {
    the IUT is requested to send a CAM
  } then {
    the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
        containing type
          indicating certificate_chain
        containing certificates.length >1
        containing certificates[last-1] {
          containing version
            indicating '2'
        }
      }
  }
}
5.2.7.2  Check the certificate chain

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_02_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the certificate chain is valid</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 4.2.10</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

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 {
        indicating certificate_chain
        containing certificates[N] {
          containing signer_info {
            indicating 'certificate_digest_with_sha256'
            containing digest
              referenced to the certificates[N - 1]
          }
        }
      }
  }
}

5.2.7.3  Geographical regions

5.2.7.3.1  Check Rectangular regions

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_04_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the rectangular certificate validity region contains not more than six valid rectangles</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 4.2.20 and 4.2.23</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION</td>
</tr>
</tbody>
</table>

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 {
        indicating 'certificate'
        containing certificate {
          containing no validity restriction or validity_restrictions['region']{
            containing region_type
              indicating 'rectangle'
            containing rectangular_region {
              indicating length <= 6
              containing elements of type RectangularRegion
                indicating continuous region without holes
                containing northwest and southeast
                  indicating northwest is on the north from southeast
            }
          }
        }
      }
  }
}
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_04_02_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the rectangular certificate validity region of the subordinate certificate is well formed and inside the validity region of the issuing certificate</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 4.2.20 and 4.2.23</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate chain in the next CAM
} ensure that {
  when {
    the IUT is requested to send a CAM
  } then {
    the IUT sends a SecuredMessage
    containing header_fields['signer_info'].signer {
      containing type
        indicating 'certificate_chain'
      containing certificates
        indicating CERTIFICATES {
          containing CERTIFICATES[N] {
            containing validity_restrictions['region'] {
              indicating 'rectangle'
              containing rectangular_region {
                indicating length <= 6
                and containing elements of type RectangularRegion
                indicating northwest on the north from southeast
                and indicating continuous region without holes
                which is inside the CERTIFICATES[N-1].validity_restrictions['region'] if region validity restriction is contained in certificate CERTIFICATES[N-1]
              }
            }
          }
        }
    }
  }
}
### 5.2.7.3.2 Check Polygonal Region

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_05_01_BV</th>
</tr>
</thead>
</table>
| **Summary**    | Check that the polygonal certificate validity region contains at least three and no more than 12 points  
Check that the polygonal certificate validity region does not contain intersections and holes |
| **Reference**  | ETSI TS 103 097 [1], clause 4.2.24 |
| **PICS Selection** | PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION |
| **Expected behaviour** | |
|  | with {  
|  | the IUT being in the 'authorized' state  
|  | the IUT being requested to include certificate in the next CAM  
|  } ensure that {  
|  | when {  
|  | the IUT is requested to send a CAM  
|  } then {  
|  | the IUT sends a SecuredMessage  
|  | containing header_fields['signer_info'].signer {  
|  | containing type  
|  | indicating 'certificate'  
|  | containing certificate {  
|  | containing validity_restrictions['region'] {  
|  | containing region_type  
|  | indicating 'polygon'  
|  | containing polygonal_region {  
|  | indicating length >=3 and <=12  
|  | indicating continuous region without holes and intersections  
|  | }  
|  | }  
|  }  
| }  
| }  
| |}
Summary
Check that the polygonal certificate validity region is inside the validity region of the issuing certificate.
Check that the issuing polygonal certificate validity region contains at least three and no more than 12 points.
Check that the issuing polygonal certificate validity region does not contain intersections and holes.

Reference
ETSI TS 103 097 [1], clause 4.2.24

PICS Selection
PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION

Expected behaviour

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

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_06_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the identified certificate validity region contains values that correspond to numeric country codes as defined in ISO 3166-1 [9]</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 4.2.26</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_USE_ISO31661_REGION_DICTIONARY, PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate in the next CAM
} ensure that {
  when {
    the IUT is requested to send a CAM
  } then {
    the IUT sends a SecuredMessage
    containing header_fields['signer_info'].signer {
      containing type
      indicating 'certificate'
      containing certificate {
        containing validity_restrictions['region']{
          containing region_type
          indicating 'id'
          containing id_region {
            containing region_dictionary
            indicating 'iso_3166_1' (0)
            containing region_identifier
            indicating valid value according to 'iso_3166_1'
            containing local_region
          }
        }
      }
    }
  }
}
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 [9]
Check that the identified certificate validity region contains values defining the region which is inside the validity region of the issuing certificate

Reference:
ETSI TS 103 097 [1], clause 4.2.26

PICS Selection:
PICS_USE_ISO31661_REGION_DICTIONARY, PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION

Expected behaviour:

with {
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate chain in the next CAM
}
ensure that {
  when {
    the IUT is requested to send a CAM
  } then {
    the IUT sends a SecuredMessage
    containing header_fields['signer_info'].signer {
      containing type
      indicating 'certificate_chain'
      containing certificates
      indicating CERTIFICATES {
        containing CERTIFICATES[0] {
          containing region_type
          indicating 'id'
          containing id_region {
            containing region_dictionary
            indicating 'iso_3166_1' (0)
            containing region_identifier
            indicating valid value according to 'iso_3166_1' dictionary
            containing local_region
          }
        }
        containing CERTIFICATES[n] (1..N) {
          containing no validity restriction of type region
          or containing validity_restrictions['region'] {
            containing region_type
            indicating 'id'
            containing id_region {
              containing region_dictionary
              indicating 'iso_3166_1' (0)
              containing region_identifier
              indicating CERTIFICATES[n-1].id_region.region_identifier
              containing local_region
              indicating CERTIFICATES[n-1].validity_restrictions['region'].id_region.local_region
              or indicating any value if CERTIFICATES[n-1].validity_restrictions['region'].id_region.local_region == 0
            }
          }
        }
      }
    }
  }
}
### TP Id
TP_SEC_ITSS_SND_CERT_06_03_BV

### Summary
Check that the identified certificate validity region contains values that correspond to numeric country codes as defined by United Nations Statistics Division [10]

### Reference
ETSI TS 103 097 [1], clause 4.2.26

### PICS Selection
PICS_USE_UN_STATS_REGION_DICTIONARY, PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION

### Expected behaviour

```plaintext
with {
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate in the next CAM
} ensure that {
  when {
    the IUT is requested to send a CAM
  } then {
    the IUT sends a SecuredMessage
    containing header_fields['signer_info'].signer {
      containing type
        indicating 'certificate'
      containing certificate {
        containing validity_restrictions['region']{
          containing region_type
            indicating 'id'
          containing id_region {
            containing region_dictionary
              indicating 'un_stats' (1)
            containing region_identifier
              indicating valid value according to UN-Stats dictionary
            containing local_region
          }
        }
      }
    }
  }
}
```
**Summary**

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

**Reference**

ETSI TS 103 097 [1], clause 4.2.26

**PICS Selection**

PICS_USE_UN_STATS_REGION_DICTIONARY, PICS_CERTIFICATE_SELECTION, PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION

**Expected behaviour**

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

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_07_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>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</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 4.2.9</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

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 signature.ecdsa_signature
        containing R.type
        indicating compressed_lsb_y_0
        or indicating compressed_lsb_y_1
        or indicating x_coordinate_only
      }
    }
  }
}

5.2.7.5  Check ECC point type of the certificate verification key

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_08_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the certificate verification key contains ECC point of type set to either compressed_lsb_y_0, compressed_lsb_y_1 or uncompressed</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 4.2.4</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

Expected behaviour

with {
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate in the next CAM
} ensure that {
  when {
    the IUT is requested to send a CAM
  } then {
    the IUT sends a SecuredMessage
    containing header_fields['signer_info'].signer {
      containing type
      indicating 'certificate'
      containing certificate {
        containing subject_attributes['verification_key']
        containing key.public_key.type
        indicating compressed_lsb_y_0
        or indicating compressed_lsb_y_1
        or indicating uncompressed
      }
    }
  }
}
### 5.2.7.6 Check the certificate signature

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_09_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check the certificate signature</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clauses 6.1 and 7.4</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td>with {</td>
<td></td>
</tr>
<tr>
<td>the IUT being in the 'authorized' state</td>
<td></td>
</tr>
<tr>
<td>the IUT being requested to include certificate in the next CAM</td>
<td></td>
</tr>
<tr>
<td>} ensure that {</td>
<td></td>
</tr>
<tr>
<td>when {</td>
<td></td>
</tr>
<tr>
<td>the IUT is requested to send a CAM</td>
<td></td>
</tr>
<tr>
<td>} then {</td>
<td></td>
</tr>
<tr>
<td>the IUT sends a SecuredMessage</td>
<td></td>
</tr>
<tr>
<td>containing header_fields['signer_info'].signer {</td>
<td></td>
</tr>
<tr>
<td>containing type</td>
<td></td>
</tr>
<tr>
<td>indicating 'certificate'</td>
<td></td>
</tr>
<tr>
<td>containing certificate {</td>
<td></td>
</tr>
<tr>
<td>containing signer_info {</td>
<td></td>
</tr>
<tr>
<td>containing type</td>
<td></td>
</tr>
<tr>
<td>indicating 'certificate_digest_with_sha256'</td>
<td></td>
</tr>
<tr>
<td>containing digest</td>
<td></td>
</tr>
<tr>
<td>referenced to the certificate CERT</td>
<td></td>
</tr>
<tr>
<td>} containing signature</td>
<td></td>
</tr>
<tr>
<td>verifiable using CERT.subject_attributes['verification_key'].key</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_09_02_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check the signatures of the certificates in the chain</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clauses 6.1 and 7.4</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td>with {</td>
<td></td>
</tr>
<tr>
<td>the IUT being in the 'authorized' state</td>
<td></td>
</tr>
<tr>
<td>the IUT being requested to include certificate chain in the next CAM</td>
<td></td>
</tr>
<tr>
<td>} ensure that {</td>
<td></td>
</tr>
<tr>
<td>when {</td>
<td></td>
</tr>
<tr>
<td>the IUT is requested to send a CAM</td>
<td></td>
</tr>
<tr>
<td>} then {</td>
<td></td>
</tr>
<tr>
<td>the IUT sends a SecuredMessage</td>
<td></td>
</tr>
<tr>
<td>containing header_fields['signer_info'].signer {</td>
<td></td>
</tr>
<tr>
<td>containing type</td>
<td></td>
</tr>
<tr>
<td>indicating 'certificate_chain'</td>
<td></td>
</tr>
<tr>
<td>containing certificates</td>
<td></td>
</tr>
<tr>
<td>indicating CERTIFICATES {</td>
<td></td>
</tr>
<tr>
<td>containing CERTIFICATES[N] {</td>
<td></td>
</tr>
<tr>
<td>containing signer_info {</td>
<td></td>
</tr>
<tr>
<td>containing type</td>
<td></td>
</tr>
<tr>
<td>indicating 'certificate_digest_with_sha256'</td>
<td></td>
</tr>
<tr>
<td>containing digest</td>
<td></td>
</tr>
<tr>
<td>referenced to the certificate CERTIFICATES[N-1]</td>
<td></td>
</tr>
<tr>
<td>} containing signature</td>
<td></td>
</tr>
<tr>
<td>verifiable using CERTIFICATES[N-1] .subject_attributes['verification_key'].key</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>
5.2.7.7 AA certificate profile

5.2.7.7.1 Check the subject type

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_AA_01_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the subject_type of the AA certificate is set to authorization_authority</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.4.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate chain in the next CAM
} ensure that {
  when {
    the IUT is requested to send a CAM
  } then {
    the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
        containing type
          indicating certificate_chain
          containing certificates[last-1] {
            containing subject_info.subject_type
              indicating 'authorization_authority' (2)
          }
      }
  }
}

5.2.7.7.2 Check AA certificate subject name

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_AA_02_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>The subject_name variable-length vector shall have a maximum length of 32 bytes</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 6.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**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_name
              indicating length <= 32 bytes
          }
      }
  }
}
5.2.7.7.3 Check that signer info is a digest

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC.ITSS_SND_CERT_AA_04_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that signer info of the AA certificate is a digest</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.4.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

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 signer_info {
            containing type
            indicating 'certificate_digest_with_sha256'
            containing digest
          }
        }
      }
  }
}

5.2.7.7.4 Check subject attributes presence and order

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC.ITSS_SND_CERT_AA_05_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that all necessary subject attributes are present and arranged in ascending order</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 6.1, 7.4 and 7.4.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

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_attributes[0..N] {
            indicating subject_attributes[n].type
            < subject_attributes[n+1].type
            containing subject_attributes['verification_key']
            containing subject_attributes['assurance_level']
            containing subject_attributes['its_aid_list']
          }
        }
      }
  }
}

ETSI
### 5.2.7.7.5 Check the time_start_and_end presence

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

### 5.2.7.7.6 Check verification key validity

Void.

### 5.2.7.7.7 Check ITS-AID

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_AA_08_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that all AIDs containing in the in the its_aid_list in AA certificate are unique</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 6.9 and 7.4.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td>with {</td>
<td></td>
</tr>
<tr>
<td>the IUT being in the 'authorized' state</td>
<td></td>
</tr>
<tr>
<td>the IUT being requested to include certificate chain in the next CAM</td>
<td></td>
</tr>
<tr>
<td>} ensure that {</td>
<td></td>
</tr>
<tr>
<td>when {</td>
<td></td>
</tr>
<tr>
<td>the IUT is requested to send a CAM</td>
<td></td>
</tr>
<tr>
<td>} then {</td>
<td></td>
</tr>
<tr>
<td>the IUT sends a SecuredMessage</td>
<td></td>
</tr>
<tr>
<td>containing header_fields['signer_info'].signer {</td>
<td></td>
</tr>
<tr>
<td>containing type</td>
<td></td>
</tr>
<tr>
<td>indicating certificate_chain</td>
<td></td>
</tr>
<tr>
<td>containing certificates[last-1] {</td>
<td></td>
</tr>
<tr>
<td>containing subject_attributes['its_aid_list']</td>
<td></td>
</tr>
<tr>
<td>containing its_aid_list[0..N]</td>
<td>containing unique items</td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>
5.2.7.7.8 Check that AA cert is signed by Root cert

Void.

5.2.7.7.9 Check validity restriction presence and order

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_AA_10_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that all mandatory validity restrictions are present and arranged in ascending order</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 6.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

Expected behaviour

with {
   the IUT being in the 'authorized' state
   the IUT being requested to include certificate chain in the next CAM
} ensure that {
   when {
      the IUT is requested to send a CAM
   } then {
      the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
         containing type indicating certificate_chain
         containing certificates[last-1] {
            containing validity_restrictions
            indicating validity_restrictions[n].type
            < validity_restrictions[n+1].type
         }
      }
   }
}

5.2.7.8 AT certificate profile

5.2.7.8.1 Check subject type

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_AT_01_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the subject_type of the AT certificate is set to 'authorization_ticket' (1)</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.4.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

Expected behaviour

with {
   the IUT being in the 'authorized' state
   the IUT being requested to include certificate in the next CAM
} ensure that {
   when {
      the IUT is requested to send a CAM
   } then {
      the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
         containing type indicating 'certificate'
         containing certificate {
            containing subject_info.subject_type
            indicating 'authorization_ticket' (1)
         }
      }
   }
}
5.2.7.8.2 Check that signer info is a digest

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_AT_02_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that signer info of the AA certificate is a digest</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 6.1, 7.4 and 7.4.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**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 signer_info |
containing type |
indicating 'certificate_digest_with_sha256' |
containing digest |
|
|
|

5.2.7.8.3 Check subject name

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_AT_03_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the subject_name variable-length vector is empty for AT certificates</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.4.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with |
the IUT being in the 'authorized' state |
the IUT being requested to include certificate in the next CAM |
} ensure that |
when |
the IUT is requested to send a CAM |
} then |
the IUT sends a SecuredMessage |
containing header_fields['signer_info'].signer |
containing type |
indicating 'certificate' |
containing certificates |
containing subject_info.subject_name |
indicating length = 0 |
|
|
|
5.2.7.8.4 Check the presence and the order of subject attributes

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_AT_04_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that subject attributes are present and arranged in ascending order</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 7.4 and 7.4.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate in the next CAM
} ensure that {
  when {
    the IUT is requested to send a CAM
  } then {
    the IUT sends a SecuredMessage
    containing header_fields['signer_info'].signer {
      containing type
      indicating 'certificate'
      containing certificate {
        containing subject_attributes [0..N] {
          indicating subject_attributes[n].type
          < subject_attributes[n+1].type
          containing subject_attributes['verification_key']
          containing subject_attributes['assurance_level']
          containing subject_attributes['its_aid_ssp_list']
        }
      }
    }
  }
}
5.2.7.8.5  Check presence of time_start_and_end validity restriction

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_AT_05_01_BV</th>
</tr>
</thead>
</table>
| **Summary** | Check that time_start_and_end is included in the AT certificate validation restrictions  
Check that time_start_and_end is inside the AA certificate time restrictions |
| **Reference** | ETSI TS 103 097 [1], clause 7.4.1 |
| **PICS Selection** | PICS_GN_SECURITY |

**Expected behaviour**

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

5.2.7.8.6  Check verification key validity

Void.
5.2.7.8.7 Check ITS-AID-SSP

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_AT_07_01_BV</th>
</tr>
</thead>
</table>
| Summary | Check that all AIDs containing in the its_aid_ssp_list in AT certificate are unique  
Check that all AIDs containing in the its_aid_ssp_list in AT certificate are also containing in the its_aid_list in the correspondent AA certificate  
Check that the length of SSP of each AID is 31 octets maximum |
| Reference | ETSI TS 103 097 [1], clauses 6.9 and 7.4.1 |
| PICS Selection | PICS_GN_SECURITY |
| Expected behaviour | with {
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate chain in the next CAM
} ensure that {
  when {
    the IUT is requested to send a CAM
  } then {
    the IUT sends a SecuredMessage containing header_fields['signer_info'].signer {
      containing type indicating certificate_chain
      containing certificates[last-1] {
        containing subject_info.subject_type indicating 'authorization_authority' (2)
        containing subject_attributes['its_aid_list'] containing its_aid_list[0..N] indicating ITS_AID_LIST_AA
      }
    }
    containing certificates[last] {
      containing subject_info.subject_type indicating 'authorization_ticket' (1)
      containing subject_attributes['its_aid_ssp_list'] containing its_aid_ssp_list[0..N] {
        containing its_aid indicating unique value containing in the ITS_AID_LIST_AA 
        containing service_specific_permissions indicating length <= 31 octet
      }
    }
  }
} |
5.2.7.8.8   Check that AT certificate is signed by AA cert

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_AT_08_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that AT certificate is signed by AA cert</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 6.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

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

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_AT_09_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the assurance level of the subordinate certificate is equal to or less than the assurance level of the issuing certificate</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.4</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

Expected behaviour

```plaintext
with {
  the IUT being in the 'authorized' state
  the IUT being requested to include certificate chain in the next CAM
} ensure that {
  when {
    the IUT is requested to send a CAM
  } then {
    the IUT sends a SecuredMessage
      containing header_fields['signer_info'].signer {
        containing type
          indicating certificate_chain
          containing certificates[last-1] (CERT_AA) {
            containing subject_attributes ['assurance_level']
              containing assurance_level
                containing bits [5-7] indicating assurance level AL_AA
          }
          containing certificates[last] (CERT_AT) {
            containing subject_attributes ['assurance_level']
              containing assurance_level
                containing bits [5-7] indicating assurance level AL_AT (AL_AT <= AL_AA)
          }
      }
  }
}
```

5.2.7.8.10  Check validity restriction presence and order

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_SND_CERT_AT_10_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that all necessary validity restrictions are present and arranged in ascending order</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 6.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

Expected behaviour

```plaintext
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
              indicating validity_restrictions[n].type < validity_restrictions[n+1].type
          }
      }
  }
}
```

5.3  Receiver Behaviour

5.3.1  Overview

All test purposes of receiving behaviour are considered optional.
5.3.2 CAM Profile

5.3.2.1 Check that IUT accepts well-formed Secured CAM

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CAM_01_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT accepts a well-formed Secured CAM containing certificate in signer_info</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Expected behaviour</th>
</tr>
</thead>
<tbody>
<tr>
<td>with {}</td>
</tr>
<tr>
<td>the IUT being in the 'authorized' state</td>
</tr>
<tr>
<td>} ensure that {}</td>
</tr>
<tr>
<td>when {}</td>
</tr>
<tr>
<td>the IUT is receiving a SecuredMessage</td>
</tr>
<tr>
<td>containing protocol_version</td>
</tr>
<tr>
<td>indicating value '2'</td>
</tr>
<tr>
<td>and containing header_fields[0]</td>
</tr>
<tr>
<td>containing type</td>
</tr>
<tr>
<td>indicating 'signer_info'</td>
</tr>
<tr>
<td>and containing signer {}</td>
</tr>
<tr>
<td>containing type</td>
</tr>
<tr>
<td>indicating 'certificate'</td>
</tr>
<tr>
<td>and containing certificate (CERT_AT_A) {}</td>
</tr>
<tr>
<td>containing subject_info.subject_type</td>
</tr>
<tr>
<td>indicating 'authorization_ticket' (2)</td>
</tr>
<tr>
<td>and containing subject_attributes['verification key'] (KEY)</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>and containing header_fields [1] {}</td>
</tr>
<tr>
<td>containing type</td>
</tr>
<tr>
<td>indicating 'generation_time'</td>
</tr>
<tr>
<td>containing generation_time</td>
</tr>
<tr>
<td>indicating CURRENT_TIME</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>and containing header_fields[2] {}</td>
</tr>
<tr>
<td>containing type</td>
</tr>
<tr>
<td>indicating 'its_aid'</td>
</tr>
<tr>
<td>containing its_aid</td>
</tr>
<tr>
<td>indicating 'AID_CAM'</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>and containing payload_field {}</td>
</tr>
<tr>
<td>containing type</td>
</tr>
<tr>
<td>indicating 'signed'</td>
</tr>
<tr>
<td>containing data</td>
</tr>
<tr>
<td>indicating length &gt; 0</td>
</tr>
<tr>
<td>containing CAM payload</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>and containing trailer_fields {}</td>
</tr>
<tr>
<td>containing single instance of type TrailerField {}</td>
</tr>
<tr>
<td>containing type</td>
</tr>
<tr>
<td>indicating 'signature'</td>
</tr>
<tr>
<td>containing signature</td>
</tr>
<tr>
<td>verifiable using KEY</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>} then {}</td>
</tr>
<tr>
<td>the IUT accepts the message</td>
</tr>
<tr>
<td>}</td>
</tr>
</tbody>
</table>
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 {
  the IUT being in the 'authorized' state
  the IUT already received a Secured message containing certificate (CERT_TS_AT_A)
  containing subject_info.subject_type
    indicating 'authorization_ticket' (2)
  and containing subject_attributes['verification key'] (KEY)
} ensure that {
  when {
    the IUT is receiving a SecuredMessage containing protocol_version
      indicating value '2'
    and containing header_fields[0]
      containing type
        indicating 'signer_info'
      and containing signer {
        containing type
          indicating 'certificate_digest_with_sha256'
        and containing digest
          referencing to certificate (CERT_TS_AT_A)
      }
    and containing header_fields [1] {
      containing type
        indicating 'generation_time'
      containing generation_time
        indicating CURRENT_TIME
    }
    and containing header_fields[2] {
      containing type
        indicating 'its_aid'
      containing its_aid
        indicating 'AID_CAM'
    }
    and containing payload_field {
      containing type
        indicating 'signed'
      containing data
        indicating length > 0
      containing CAM payload
    }
    and containing trailer_fields {
      containing single instance of type TrailerField {
        containing type
          indicating 'signature'
        containing signature
          verifiable using KEY
      }
    }
  } then {
    the IUT accepts the message
  }
}
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CAM_01_03_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT accepts a well-formed Secured CAM containing certificate chain in signer_info</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

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

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CAM_02_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards a Secured CAM containing protocol version set to a value less than 2</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 5.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage (CAM) containing protocol_version indicating 1
    containing header_fields['its_aid'] indicating 'AID_CAM'
  } then {
    the IUT discards a SecuredMessage
  }
}

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CAM_02_02_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards a Secured CAM containing protocol version set to a value greater than 2</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 5.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage (CAM) containing protocol_version indicating 3
    containing header_fields['its_aid'] indicating 'AID_CAM'
  } then {
    the IUT discards a SecuredMessage
  }
}
### 5.3.2.3 Check header fields

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CAM_04_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards a secured CAM if the header_fields contains more than one element of header field type: signer_info</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td>with {</td>
<td></td>
</tr>
<tr>
<td>the IUT being in the 'authorized' state</td>
<td></td>
</tr>
<tr>
<td>ensure that {</td>
<td></td>
</tr>
<tr>
<td>when {</td>
<td></td>
</tr>
<tr>
<td>the IUT is receiving a SecuredMessage (CAM)</td>
<td></td>
</tr>
<tr>
<td>containing header_fields[0].type indicating 'signer_info'</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields[1].type indicating 'signer_info'</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields[2].type indicating 'generation_time'</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields[3] {</td>
<td></td>
</tr>
<tr>
<td>containing type indicating 'its_aid'</td>
<td></td>
</tr>
<tr>
<td>containing its_aid indicating 'AID_CAM'</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>and not containing other header fields</td>
<td></td>
</tr>
<tr>
<td>then {</td>
<td></td>
</tr>
<tr>
<td>the IUT discards a SecuredMessage</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CAM_04_02_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards a secured CAM if the header_fields does not contain the header field type: signer_info</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td>with {</td>
<td></td>
</tr>
<tr>
<td>the IUT being in the 'authorized' state</td>
<td></td>
</tr>
<tr>
<td>ensure that {</td>
<td></td>
</tr>
<tr>
<td>when {</td>
<td></td>
</tr>
<tr>
<td>the IUT is receiving a SecuredMessage (CAM)</td>
<td></td>
</tr>
<tr>
<td>containing header_fields[0].type indicating 'generation_time'</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields[1] {</td>
<td></td>
</tr>
<tr>
<td>containing type indicating 'its_aid'</td>
<td></td>
</tr>
<tr>
<td>containing its_aid indicating 'AID_CAM'</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>and not containing other header fields</td>
<td></td>
</tr>
<tr>
<td>then {</td>
<td></td>
</tr>
<tr>
<td>the IUT discards a SecuredMessage</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>TP Id</td>
<td>TP_SEC_ITSS_RCV_CAM_04_03_BO</td>
</tr>
<tr>
<td>------------</td>
<td>---------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Summary</td>
<td>Check that IUT is able to receive a secured CAM if the signer_info header field is not encoded first</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td>Expected behaviour</td>
<td>with {</td>
</tr>
<tr>
<td></td>
<td>the IUT being in the 'authorized' state</td>
</tr>
<tr>
<td></td>
<td>the IUT is sending CAMs</td>
</tr>
<tr>
<td></td>
<td>} ensure that {</td>
</tr>
<tr>
<td></td>
<td>when {</td>
</tr>
<tr>
<td></td>
<td>the IUT is receiving a SecuredMessage (CAM) {</td>
</tr>
<tr>
<td></td>
<td>containing header_fields[0].type</td>
</tr>
<tr>
<td></td>
<td>indicating 'signer_info'</td>
</tr>
<tr>
<td></td>
<td>containing header_fields[1].type</td>
</tr>
<tr>
<td></td>
<td>indicating 'generation_time'</td>
</tr>
<tr>
<td></td>
<td>containing header_fields[2].type</td>
</tr>
<tr>
<td></td>
<td>indicating 'signer_info'</td>
</tr>
<tr>
<td></td>
<td>containing header_fields[3] {</td>
</tr>
<tr>
<td></td>
<td>containing type</td>
</tr>
<tr>
<td></td>
<td>indicating 'its_aid'</td>
</tr>
<tr>
<td></td>
<td>containing its_aid</td>
</tr>
<tr>
<td></td>
<td>indicating 'AID_CAM'</td>
</tr>
<tr>
<td></td>
<td>} and not containing other header fields</td>
</tr>
<tr>
<td></td>
<td>} then {</td>
</tr>
<tr>
<td></td>
<td>the IUT keeps sending CAMs</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CAM_04_04_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards a secured CAM if the header_fields contains more than one element of header field type: generation_time</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td>Expected behaviour</td>
<td>with {</td>
</tr>
<tr>
<td></td>
<td>the IUT being in the 'authorized' state</td>
</tr>
<tr>
<td></td>
<td>} ensure that {</td>
</tr>
<tr>
<td></td>
<td>when {</td>
</tr>
<tr>
<td></td>
<td>the IUT is receiving a SecuredMessage (CAM) {</td>
</tr>
<tr>
<td></td>
<td>containing header_fields[0].type</td>
</tr>
<tr>
<td></td>
<td>indicating 'signer_info'</td>
</tr>
<tr>
<td></td>
<td>containing header_fields[1].type</td>
</tr>
<tr>
<td></td>
<td>indicating 'generation_time'</td>
</tr>
<tr>
<td></td>
<td>containing header_fields[2].type</td>
</tr>
<tr>
<td></td>
<td>indicating 'generation_time'</td>
</tr>
<tr>
<td></td>
<td>containing header_fields[3] {</td>
</tr>
<tr>
<td></td>
<td>containing type</td>
</tr>
<tr>
<td></td>
<td>indicating 'its_aid'</td>
</tr>
<tr>
<td></td>
<td>containing its_aid</td>
</tr>
<tr>
<td></td>
<td>indicating 'AID_CAM'</td>
</tr>
<tr>
<td></td>
<td>} and not containing other header fields</td>
</tr>
<tr>
<td></td>
<td>} then {</td>
</tr>
<tr>
<td></td>
<td>the IUT discards a SecuredMessage</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td>TP Id</td>
<td>TP_SEC_ITSS_RCV_CAM_04_05_BO</td>
</tr>
<tr>
<td>----------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Summary</td>
<td>Check that IUT discards a secured CAM if the header_fields does not contain the element of header field of type: generation_time</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td>with {</td>
<td></td>
</tr>
<tr>
<td>the IUT being in the 'authorized' state</td>
<td></td>
</tr>
<tr>
<td>} ensure that {</td>
<td></td>
</tr>
<tr>
<td>when {</td>
<td></td>
</tr>
<tr>
<td>the IUT is receiving a SecuredMessage (CAM)</td>
<td></td>
</tr>
<tr>
<td>containing header_fields[0].type</td>
<td></td>
</tr>
<tr>
<td>indicating 'signer_info'</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields[1] {</td>
<td></td>
</tr>
<tr>
<td>containing type</td>
<td></td>
</tr>
<tr>
<td>indicating 'its_aid'</td>
<td></td>
</tr>
<tr>
<td>containing its_aid</td>
<td></td>
</tr>
<tr>
<td>indicating 'AID_CAM'</td>
<td></td>
</tr>
<tr>
<td>} and not containing other header fields</td>
<td></td>
</tr>
<tr>
<td>} then {</td>
<td></td>
</tr>
<tr>
<td>the IUT discards a SecuredMessage</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CAM_04_06_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards a secured CAM if the header_fields contain more than one element of header field of type: its_aid</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td>with {</td>
<td></td>
</tr>
<tr>
<td>the IUT being in the 'authorized' state</td>
<td></td>
</tr>
<tr>
<td>} ensure that {</td>
<td></td>
</tr>
<tr>
<td>when {</td>
<td></td>
</tr>
<tr>
<td>the IUT is receiving a SecuredMessage (CAM)</td>
<td></td>
</tr>
<tr>
<td>containing header_fields[0].type</td>
<td></td>
</tr>
<tr>
<td>indicating 'signer_info'</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields[1].type</td>
<td></td>
</tr>
<tr>
<td>indicating 'generation_time'</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields[2] {</td>
<td></td>
</tr>
<tr>
<td>containing type</td>
<td></td>
</tr>
<tr>
<td>indicating 'its_aid'</td>
<td></td>
</tr>
<tr>
<td>containing its_aid</td>
<td></td>
</tr>
<tr>
<td>indicating 'AID_CAM'</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields[3] {</td>
<td></td>
</tr>
<tr>
<td>containing type</td>
<td></td>
</tr>
<tr>
<td>indicating 'its_aid'</td>
<td></td>
</tr>
<tr>
<td>containing its_aid</td>
<td></td>
</tr>
<tr>
<td>indicating 'AID_DENM'</td>
<td></td>
</tr>
<tr>
<td>} and not containing other header fields</td>
<td></td>
</tr>
<tr>
<td>} then {</td>
<td></td>
</tr>
<tr>
<td>the IUT discards a SecuredMessage</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>TP Id</td>
<td>TP_SEC_ITSS_RCV_CAM_04_08_BO</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------</td>
</tr>
<tr>
<td>Summary</td>
<td>Check that IUT ignores the HeaderFields generation_time_standard_deviation of received Secured CAM</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

### Expected behaviour

with {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is receiving a SecuredMessage (CAM) containing header_fields[0].type indicating 'signer_info' containing header_fields[1] containing type indicating 'generation_time' containing generation_time indicating TIME_1 inside the validity period of the signer certificate
  } containing header_fields[2] containing type indicating 'generation_time_with_standard_deviation' containing generation_time_with_standard_deviation indicating TIME_2 outside the validity period of the signer certificate
  } and containing header_fields[3] containing type indicating 'its_aid' containing its_aid indicating 'AID_CAM'
  } and not containing other header fields
  then {
    the IUT discards a SecuredMessage
  }
Summary
Check that IUT ignores the HeaderFields generation_time_standard_deviation of received Secured CAM

Reference
ETSI TS 103 097 [1], clause 7.1

PICS Selection
PICS_GN_SECURITY

Expected behaviour

with {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is receiving a SecuredMessage (CAM)
      containing header_fields[0].type
        indicating 'signer_info'
      containing header_fields[1] {
        containing type
          indicating 'generation_time'
        containing generation_time
          indicating TIME_1 outside the validity period of the signer certificate
      }
      containing header_fields[2] {
        containing type
          indicating 'generation_time_with_standard_deviation'
        containing generation_time_with_standard_deviation
          indicating TIME_2 inside the validity period of the signer certificate
      }
      and containing header_fields[3] {
        containing type
          indicating 'its_aid'
        containing its_aid
          indicating 'AID_CAM'
      }
      and not containing other header fields
  } then {
    the IUT discards a SecuredMessage
  }
}
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CAM_04_10_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT ignores the HeaderFields expiry_time of received Secured CAM</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is receiving a SecuredMessage (CAM)
    containing header_fields[0].type
      indicating 'signer_info'
    containing header_fields[1]
      containing type
        indicating 'generation_time'
      containing_generation_time
        indicating TIME_1 (TIME_1 < CURRENT_TIME - 1min )
    } containing header_fields[2] 
      containing type
        indicating 'expiration'
      containing expiry_time
        indicating TIME_2 (TIME_1 < TIME_2 < CURRENT_TIME)
    and containing header_fields[3] 
      containing type
        indicating 'its_aid'
      containing its_aid
        indicating 'AID_CAM'
    } and not containing other header fields
  } then {
    the IUT accepts a SecuredMessage
  }
}
5.3.2.4 Check signer info

### 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

#### Expected behaviour

```plaintext
with {
    the IUT being in the 'authorized' state
} ensure that {
    when {
        the IUT is receiving a SecuredMessage (CAM) {
            containing header_fields['signer_info'] {
                containing signer.type indicating 'self'
            }
            and containing header_fields['generation_time']
            and containing header_fields['its_aid'] indicating 'AID_CAM'
            and not containing other header fields
        }
    }
    then {
        the IUT discards a SecuredMessage
    }
}
```
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CAM_05_02_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards a secured CAM if the header_fields contains a signer of type certificate_digest_with_other_algorithm</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td>with {</td>
</tr>
<tr>
<td></td>
<td>the IUT being in the 'authorized' state</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>ensure that {</td>
</tr>
<tr>
<td></td>
<td>when {</td>
</tr>
<tr>
<td></td>
<td>the IUT is receiving a SecuredMessage (CAM) {</td>
</tr>
<tr>
<td></td>
<td>containing header_fields['signer_info']</td>
</tr>
<tr>
<td></td>
<td>containing signer {</td>
</tr>
<tr>
<td></td>
<td>containing type</td>
</tr>
<tr>
<td></td>
<td>indicating 'certificate_digest_with_other_algorithm'</td>
</tr>
<tr>
<td></td>
<td>and containing header_fields['generation_time']</td>
</tr>
<tr>
<td></td>
<td>and containing header_fields['its_aid']</td>
</tr>
<tr>
<td></td>
<td>indicating 'AID_CAM'</td>
</tr>
<tr>
<td></td>
<td>and not containing other header fields</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>then {</td>
</tr>
<tr>
<td></td>
<td>the IUT discards a SecuredMessage</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CAM_05_03_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards a secured CAM if the header_fields contains a signer of type certificate_chain and the chain is empty</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td>with {</td>
</tr>
<tr>
<td></td>
<td>the IUT being in the 'authorized' state</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>ensure that {</td>
</tr>
<tr>
<td></td>
<td>when {</td>
</tr>
<tr>
<td></td>
<td>the IUT is receiving a SecuredMessage (CAM) {</td>
</tr>
<tr>
<td></td>
<td>containing header_fields['signer_info']</td>
</tr>
<tr>
<td></td>
<td>containing signer {</td>
</tr>
<tr>
<td></td>
<td>containing type</td>
</tr>
<tr>
<td></td>
<td>indicating 'certificate_chain'</td>
</tr>
<tr>
<td></td>
<td>containing certificates</td>
</tr>
<tr>
<td></td>
<td>indicating length = 0</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>and containing header_fields['generation_time']</td>
</tr>
<tr>
<td></td>
<td>and containing header_fields['its_aid']</td>
</tr>
<tr>
<td></td>
<td>indicating 'AID_CAM'</td>
</tr>
<tr>
<td></td>
<td>and not containing other header fields</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>then {</td>
</tr>
<tr>
<td></td>
<td>the IUT discards a SecuredMessage</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td>TP Id</td>
<td>TP_SEC_ITSS_RCV_CAM_05_04_BO</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-------------------------------------------------------</td>
</tr>
<tr>
<td>Summary</td>
<td>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</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
with {
    the IUT being in the 'authorized' state
}
ensure that {
    when {
        the IUT is receiving a SecuredMessage (CAM) {
            containing header_fields['signer_info']
            containing signer {
                containing type
                indicating 'certificate_chain'
                containing certificates
                indicating length = 1
            }
            and containing header_fields['generation_time']
            and containing header_fields['its_aid']
                indicating 'AID_CAM'
                and not containing other header fields
        } then {
            the IUT discards a SecuredMessage
        }
    }
}```
### 5.3.2.5 Check generation time

<table>
<thead>
<tr>
<th><strong>TP Id</strong></th>
<th>TP_SEC_ITSS_RCV_CAM_06_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards message containing generation_time before the certificate validity period</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clauses 5.4 and 7.1</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

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

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

with {
    the IUT being in the 'authorized' state
} ensure that {
    when {
        the IUT is receiving a SecuredMessage (CAM) containing header_fields['its_aid'] indicating AID_DENM
        and containing payload_field {
            containing type indicating 'signed'
            containing data containing CAM payload
        }
    } then {
        the IUT discards the message
    }
}
5.3.2.7 Check payload

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CAM_09_02_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards the Secured CAM containing empty payload of type 'signed'</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields['its_aid']
      indicating 'AID_CAM'
      and containing payload_field {
        containing type
        indicating 'signed'
        containing data
        indicating length 0
      }
    }
  } then {
    the IUT discards the message
  }
}

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CAM_09_03_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards the Secured CAM containing non-empty payload of type 'unsecured'</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

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

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CAM_09_05_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards the Secured CAM containing non-empty payload of type 'signed_external'</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td>Expected behaviour</td>
<td>with {</td>
</tr>
<tr>
<td></td>
<td>the IUT being in the 'authorized' state</td>
</tr>
<tr>
<td></td>
<td>} ensure that {</td>
</tr>
<tr>
<td></td>
<td>when {</td>
</tr>
<tr>
<td></td>
<td>the IUT is receiving a SecuredMessage {</td>
</tr>
<tr>
<td></td>
<td>containing header_fields['its_aid']</td>
</tr>
<tr>
<td></td>
<td>indicating 'AID_CAM'</td>
</tr>
<tr>
<td></td>
<td>and containing payload_field {</td>
</tr>
<tr>
<td></td>
<td>containing type</td>
</tr>
<tr>
<td></td>
<td>indicating 'signed_external'</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>} then {</td>
</tr>
<tr>
<td></td>
<td>the IUT discards the message</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>
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 {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields['its_aid']
        indicating 'AID_CAM'
      and containing payload_field {
        containing type
          indicating 'signed_and_encrypted'
    }
  }
} then {
  the IUT discards the message
}

5.3.2.8 Check presence of trailer field

TP 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 {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields['its_aid']
        indicating 'AID_CAM'
      and containing trailer_fields
        not containing any instance of type TrailerField {
          containing type
            indicating 'signature'
    }
  }
} then {
  the IUT discards the message
}
### 5.3.2.9 Check signature

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CAM_11_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>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</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
with { the IUT being in the 'authorized' state }
ensure that {
    when {
        the IUT is receiving a SecuredMessage {
            containing header_fields['its_aid'] {
                containing signer {
                    containing type indicating 'certificate'
                    containing certificate
                    containing subject_info.subject_type indicating 'authorization_ticket' (2)
                    and containing subject_attributes['verification key'] containing key (KEY)
                }
            }
            containing header_fields['its_aid'] indicating 'AID_CAM'
            containing trailer_fields {
                containing single instance of type TrailerField {
                    containing type indicating 'signature'
                    containing signature NOT verifiable using KEY
                }
            }
        } then {
            the IUT discards the message
        }
    }
}
```
### 5.3.2.10 Check signing certificate type

**TP Id**
TP_SEC_ITSS_RCV_CAM_12_01_BO

**Summary**
Check that IUT discards a Secured CAM if the signer certificate of the message contains the subject type "enrolment Credential".

**Reference**
ETSI TS 103 097 [1], clauses 7.1 and 7.4

**PICS Selection**
PICS_GN_SECURITY

**Expected behaviour**

```plaintext
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_EC_A)
               containing subject_info.subject_type
               indicating 'enrolment_credentials'
            }
            containing header_fields ['its_aid']
            indicating 'AID_CAM'
            containing trailer_fields {
               containing single instance of type TrailerField {
                  containing type
                  indicating 'signature'
                  containing signature
                  NOT verifiable using KEY
               }
            }
         }
      }
   } then {
      the IUT discards the message
   }
}
```
**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], clauses 7.1 and 7.4

**PICS Selection**  
PICS_GN_SECURITY

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info'] {
        containing signer.type
          indicating 'certificate'
        containing signer.certificate {CERT_TS_AA_A}
        containing subject_info.subject_type
          indicating 'authorization_authority'
      }  
      containing header_fields['its_aid']
        indicating 'AID_CAM'
  } then {
    the IUT discards the message
  }
}


5.3.3 DENM Profile

5.3.3.1 Check that IUT accepts well-formed Secured DENM

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC.ITSS.RCV_DENM.01_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT accepts a well-formed Secured DENM signed with the certificate without region validity restriction</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```
with {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is receiving a SecuredMessage
    containing header_fields[0]
    containing type indicating 'signer_info'
    and containing signer {
      containing type
      indicating 'certificate'
      and containing certificate (CERT_TS_AT_A) {
        containing subject_info.subject_type
        indicating 'authorization_ticket' (2)
        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'
    containing generation_time
    indicating CURRENT_TIME
    and containing header_fields [2]
    containing type indicating 'generation_location'
    containing generation_location
    and containing header_fields[3]
    containing type indicating 'its_aid'
    containing its_aid
    indicating 'AID_DENM'
    and containing payload_field {
      containing type indicating 'signed'
      containing data
      indicating length > 0
      containing DENM payload
    }
    and containing trailer_fields {
      containing single instance of type TrailerField {
        containing type
        indicating 'signature'
        containing signature
        verifiable using KEY
      }
    }
  }
} then {
  the IUT accepts the message
} 
```
**Summary**

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

**Reference**

ETSI TS 103 097 [1], clause 7.2

**PICS Selection**

PICS_GN_SECURITY

**Expected behaviour**

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

ensure that {
  when {
    the IUT is receiving a SecuredMessage
      and containing header_fields[0]
        containing type
          indicating 'signer_info'
        and containing signer {
          containing type
            indicating 'certificate'
          and containing certificate (CERT_AT_B) {
            containing subject_info.subject_type
              indicating 'authorization_ticket' (2)
            and containing subject_attributes['verification key'] (KEY)
            and containing validity_restrictions['region'] {
              containing region{
                containing region_type
                  indicating 'circle'
                and containing circular_region
                  indicating REGION
              }
            }
            and containing header_fields [1]
              containing type
                indicating 'generation_time'
            containing generation_time
              indicating CURRENT_TIME
            and containing header_fields [2]
              containing type
                indicating 'generation_location'
            containing generation_location
              indicating position inside the REGION
            and containing header_fields[3]
              containing type
                indicating 'its_aid'
            containing its_aid
              indicating 'AID_DENM'
          and not containing any other header_fields
          and containing payload_fields {
            containing type
              indicating 'signed'
            containing data
              indicating length > 0
            containing DENM payload
          }
        }
    and containing trailer_fields {
      containing single instance of type TrailerField {
        containing type
          indicating 'signature'
        containing signature
          verifiable using KEY
      }
    }
  } then {
    the IUT accepts the message
  }
}
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_01_03_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT accepts a well-formed Secured DENM signed with the certificate with a rectangular region validity restriction</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

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

ensure that {
  when {
    the IUT is receiving a SecuredMessage
      containing protocol_version
        indicating value '2'
      and containing header_fields[0]
        containing type
          indicating 'signer_info'
      and containing signer {
        containing type
          indicating 'certificate'
        and containing certificate (CERT_AT_C) {
          containing subject_info.subject_type
            indicating 'authorization_ticket' (2)
        }
      }
      and containing 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
  }
}
TP Id | TP_SEC_ITSS_RCV_DENM_01_04_BV
---|---
Summary | Check that IUT accepts a well-formed Secured DENM signed with the certificate with a polygonal region validity restriction
Reference | ETSI TS 103 097 [1], clause 7.2
PICS Selection | PICS_GN_SECURITY

Expected behaviour

with {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is receiving a SecuredMessage
    containing protocol_version
      indicating value '2'
    and containing header_fields[0]
      containing type
        indicating 'signer_info'
      and containing signer {
        containing type
          indicating 'certificate'
        and containing certificate (CERT_AT_D) {
          containing subject_info.subject_type
            indicating 'authorization_ticket' (2)
          and containing subject_attributes['verification key'] (KEY)
          and containing validity_restrictions['region'] {
            containing region{
              containing region_type
                indicating 'polygon'
            and containing polygonal_region
              indicating REGION
            }
          }
        }
      }
    and containing header_fields [1]
      containing type
        indicating 'generation_time'
      containing generation_time
        indicating CURRENT_TIME
    and containing header_fields [2]
      containing type
        indicating 'generation_location'
      containing generation_location
        indicating position inside the REGION
    and containing header_fields[3]
      containing type
        indicating 'its_aid'
      containing its_aid
        indicating 'AID_DENM'
    and not containing any other header_fields
    and containing payload_field {
      containing type
        indicating 'signed'
      containing data
        indicating length > 0
      containing DENM payload
    }
    and containing trailer_fields {
      containing single instance of type TrailerField {
        containing type
          indicating 'signature'
        containing signature
          verifiable using KEY
      }
    }
  } then {
    the IUT accepts the message
  }
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_01_05_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT accepts a well-formed Secured DENM signed with the certificate with a identified region validity restriction</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

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

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

### 5.3.3.2 Check the message protocol version

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_02_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards a Secured DENM containing protocol version set to a value less than 2</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 5.2</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td>with {}</td>
<td></td>
</tr>
<tr>
<td>the IUT being in the 'authorized' state</td>
<td></td>
</tr>
<tr>
<td>ensure that {}</td>
<td></td>
</tr>
<tr>
<td>when {}</td>
<td></td>
</tr>
<tr>
<td>the IUT is receiving a SecuredMessage (DENM)</td>
<td></td>
</tr>
<tr>
<td>containing protocol_version indicating 1</td>
<td></td>
</tr>
<tr>
<td>containing header_fields['its_aid'] indicating 'AID_DENM'</td>
<td></td>
</tr>
<tr>
<td>} then {}</td>
<td></td>
</tr>
<tr>
<td>the IUT discards a SecuredMessage</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_02_02_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards a Secured DENM containing protocol version set to a value greater than 2</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 5.2</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td>with {}</td>
<td></td>
</tr>
<tr>
<td>the IUT being in the 'authorized' state</td>
<td></td>
</tr>
<tr>
<td>ensure that {}</td>
<td></td>
</tr>
<tr>
<td>when {}</td>
<td></td>
</tr>
<tr>
<td>the IUT is receiving a SecuredMessage (DENM)</td>
<td></td>
</tr>
<tr>
<td>containing protocol_version indicating 3</td>
<td></td>
</tr>
<tr>
<td>containing header_fields['its_aid'] indicating 'AID_DENM'</td>
<td></td>
</tr>
<tr>
<td>} then {}</td>
<td></td>
</tr>
<tr>
<td>the IUT discards a SecuredMessage</td>
<td></td>
</tr>
</tbody>
</table>
### 5.3.3.3 Check header fields

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

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_04_02_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards a secured DENM if the header_fields does not contain the header field type: signer_info</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td>Expected behaviour</td>
<td>with {</td>
</tr>
<tr>
<td></td>
<td>the IUT being in the 'authorized' state</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>ensure that {</td>
</tr>
<tr>
<td></td>
<td>when {</td>
</tr>
<tr>
<td></td>
<td>the IUT is receiving a SecuredMessage (DENM)</td>
</tr>
<tr>
<td></td>
<td>containing header_fields[0].type</td>
</tr>
<tr>
<td></td>
<td>indicating 'generation_time'</td>
</tr>
<tr>
<td></td>
<td>and containing header_fields[1].type</td>
</tr>
<tr>
<td></td>
<td>indicating 'generation_location'</td>
</tr>
<tr>
<td></td>
<td>and containing header_fields[2]</td>
</tr>
<tr>
<td></td>
<td>containing type</td>
</tr>
<tr>
<td></td>
<td>indicating 'its_aid'</td>
</tr>
<tr>
<td></td>
<td>containing its_aid</td>
</tr>
<tr>
<td></td>
<td>indicating 'AID_DENM'</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>and not containing other header fields</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>then {</td>
</tr>
<tr>
<td></td>
<td>the IUT discards a SecuredMessage</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td>TP Id</td>
<td>TP_SEC_ITSS_RCV_DENM_04_04_BO</td>
</tr>
<tr>
<td>-------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Summary</td>
<td>Check that IUT discards a secured DENM if the header_fields contains more than one element of header field type: generation_time</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
with {
    the IUT being in the 'authorized' state
} ensure that {
    when {
        the IUT is receiving a SecuredMessage (DENM) 
            containing header_fields[0].type 
                indicating 'signer_info' 
            and header_fields[1].type 
                indicating 'generation_time' 
            and header_fields[2].type 
                indicating 'generation_time' 
            and header_fields[3].type 
                indicating 'generation_location' 
            and 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 
        }
    }
}
```

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_04_05_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards a secured DENM if the message does not contain the header field of type generation_time</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

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

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_04_07_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards a secured DENM if the header_fields contains more than one element of header field of type generation_location</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td>with {</td>
<td></td>
</tr>
<tr>
<td>the IUT being in the 'authorized' state</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>ensure that {</td>
<td></td>
</tr>
<tr>
<td>when {</td>
<td></td>
</tr>
<tr>
<td>the IUT is receiving a SecuredMessage (DENM)</td>
<td></td>
</tr>
<tr>
<td>containing header_fields[0].type indicating 'signer_info'</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields[1].type indicating 'generation_time'</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields[2].type indicating 'generation_location'</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields[3].type indicating 'generation_location'</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields[4] {</td>
<td></td>
</tr>
<tr>
<td>containing type</td>
<td></td>
</tr>
<tr>
<td>indicating 'its_aid'</td>
<td></td>
</tr>
<tr>
<td>containing its_aid</td>
<td></td>
</tr>
<tr>
<td>indicating 'AID_DENM'</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>and not containing other header fields</td>
<td></td>
</tr>
<tr>
<td>} then {</td>
<td></td>
</tr>
<tr>
<td>the IUT discards a SecuredMessage</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>TP Id</td>
<td>TP_SEC_ITSS_RCV_DENM_04_08_BO</td>
</tr>
<tr>
<td>-------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Summary</td>
<td>Check that IUT discards a secured DENM if the message does not contain the header field of type <code>generation_location</code></td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

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

ensure that {
    when {
        the IUT is receiving a SecuredMessage (DENM)
        containing header_fields[0].type indicating 'signer_info'
        containing header_fields[1].type indicating 'generation_time'
        and containing header_fields[2] {
            containing type indicating 'its_aid'
            containing its_aid indicating 'AID_DENM'
        }
        and not containing other header fields
    } then {
        the IUT discards a SecuredMessage
    }
}
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_04_10_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT ignores the HeaderFields generation_time_standard_deviation of received Secured CAM</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>
| Expected behaviour | with {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is receiving a SecuredMessage (DENM)
    containing header_fields[0].type
    indicating 'signer_info'
    containing signer
    containing certificate
    indicating CERT_TS_AT_A
    and containing header_fields[1] {
      containing type
      indicating 'generation_time_with_standard_deviation'
      containing generation_time_with_standard_deviation
      indicating TIME_2 inside the validity period of CERT_TS_AT_A
    }
    and containing header_fields[2] {
      containing type
      indicating 'generation_time'
      containing generation_time
      indicating TIME_1 outside the validity period of CERT_TS_AT_A
    }
    and containing header_fields[3].type
    indicating 'generation_location'
    and containing header_fields[4] {
      containing type
      indicating 'its_aid'
      containing its_aid
      indicating 'AID_DENM'
    }
    and not containing other header fields
  } then {
    the IUT discards a SecuredMessage
} |
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_04_11_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT ignores the HeaderFields <code>generation_time_standard_deviation</code> of received Secured CAM</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

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

Expected behaviour

with {
  \text{the IUT being in the 'authorized' state}
} ensure that {
  when {
    \text{the IUT is receiving a SecuredMessage (DENM)}
    containing header_fields[0].type
      indicating 'signer_info'
    containing header_fields[1]{
      containing type
        indicating 'generation_time'
      containing generation_time
        indicating TIME_1 ( TIME_1 < CURRENT_TIME - 1min )
    } and containing header_fields[2] {
      containing type
        indicating 'expiration'
      containing expiry_time
        indicating TIME_2 ( TIME_1 < TIME_2 < CURRENT_TIME )
    } and containing header_fields[3].type
      indicating 'generation_location'
    and containing header_fields[4] {
      containing type
        indicating 'its_aid'
      containing its_aid
        indicating 'AID_DENM'
    } and not containing other header fields
  } then {
    \text{the IUT accepts a SecuredMessage}
  }
}

5.3.3.4 Check signer info

Check that IUT discards a secured DENM if the header_fields contains a signer of type 'self'

Expected behaviour

with {
  \text{the IUT being in the 'authorized' state}
} ensure that {
  when {
    \text{the IUT is receiving a SecuredMessage (DENM)}
      containing header_fields['signer_info']
    containing signer.type
      indicating 'self'
    and containing header_fields['generation_time']
    and containing header_fields['generation_location']
    and containing header_fields['its_aid']
      indicating 'AID_DENM'
    and not containing other header fields
  } then {
    \text{the IUT discards a SecuredMessage}
  }
}
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_05_02_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards a secured DENM if the header_fields contains a signer of type 'certificate_digest_with_other_algorithm'</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
with {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is receiving a SecuredMessage (DENM) {
      containing header_fields['signer_info']
      containing signer.type
      indicating 'certificate_digest_with_other_algorithm'
      and containing header_fields['generation_time']
      and containing header_fields['generation_location']
      and containing header_fields['its_aid']
      indicating 'AID_DENM'
      and not containing other header fields
    } then {
      the IUT discards a SecuredMessage
    }
  }
}
```

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_05_03_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards a secured DENM if the header_fields contains a signer of type 'certificate_chain'</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
with {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is receiving a SecuredMessage (DENM) {
      containing header_fields['signer_info']
      containing signer {
        containing type
        indicating 'certificate_chain'
      }
      and containing header_fields['generation_time']
      and containing header_fields['generation_location']
      and containing header_fields['its_aid']
      indicating 'AID_DENM'
      and not containing other header fields
    } then {
      the IUT discards a SecuredMessage
    }
  }
}
```
5.3.3.5 Check generation time

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_06_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards message containing generation_time before the certificate validity period</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 5.4 and 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is receiving a SecuredMessage (DENM) {
      containing header_fields[0] {
        containing type
        indicating 'signer_info'
        and containing signer {
          containing type
          indicating 'certificate'
          and containing certificate (CERT_TS_AT_A) {
            containing validity_restrictions['time_start_and_end'] {
              containing start_validity
              indicating TIME_CERT_TS_AT_START
              and containing end_validity
              indicating TIME_CERT_TS_AT_END
            }
          }
        }
      }
      and containing header_fields [1] {
        containing type
        indicating 'generation_time'
        containing generation_time
        indicating TIME_1 < TIME_CERT_TS_AT_START
      }
      and containing header_fields [2] {
        containing type
        indicating 'generation_location'
      }
      and containing header_fields[3] {
        containing type
        indicating 'its_aid'
        containing its_aid
        indicating 'AID_DENM'
      }
    }
  } then {
    the IUT discards the message
  }
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_06_02_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards message containing generation_time after the certificate validity period</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clauses 5.4 and 7.2</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

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

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_07_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards secured DENM when its_aid value is not AID_DENM</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage (DENM)
    containing header_fields['its_aid']
    indicating AID_CAM
    and containing payload_field {
      containing type
      indicating 'signed'
      containing data
      containing DENM payload
    }
  } then {
    the IUT discards the message
  }
}

### 5.3.3.7 Check generation location

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_08_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards Secured DENM if the HeaderField generation_location is outside of the circular validity region of the signing certificate</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY, PICS_USE_CIRCULAR_REGION</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage
    and containing header_fields ['signer_info'].type
    indicating certificate
    and containing header_fields ['signer_info'].certificate (CERT_TS_AT_B)
    containing validity_restrictions ['region'] {
      containing region{
        containing region_type
        indicating 'circle'
        containing circular_region
        indicating REGION
      }
    }
    and containing header_fields ['generation_location']
    containing generation_location
    indicating value outside of the REGION
    and containing header_fields['its_aid']
    indicating 'AID_DENM'
  } then {
    the IUT discards the message
  }
}
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ISSS_RCV_DENM_08_02_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards Secured DENM if the HeaderField generation_location is outside of the rectangular validity region of the signing certificate</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td>with {</td>
<td></td>
</tr>
<tr>
<td>the IUT being in the 'authorized' state</td>
<td></td>
</tr>
<tr>
<td>} ensure that {</td>
<td></td>
</tr>
<tr>
<td>when {</td>
<td></td>
</tr>
<tr>
<td>the IUT is receiving a SecuredMessage</td>
<td></td>
</tr>
<tr>
<td>containing header_fields ['signer_info'].type</td>
<td></td>
</tr>
<tr>
<td>indicating certificate</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields ['signer_info'].certificate (CERT_TS_AT_C)</td>
<td></td>
</tr>
<tr>
<td>containing validity_restrictions ['region'] {</td>
<td></td>
</tr>
<tr>
<td>containing region{</td>
<td></td>
</tr>
<tr>
<td>containing region_type</td>
<td></td>
</tr>
<tr>
<td>indicating 'rectangle'</td>
<td></td>
</tr>
<tr>
<td>containing rectangular_regions</td>
<td></td>
</tr>
<tr>
<td>indicating REGION</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>} and containing header_fields ['generation_location']</td>
<td></td>
</tr>
<tr>
<td>containing generation_location</td>
<td></td>
</tr>
<tr>
<td>indicating value outside of the REGION</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields ['its_aid']</td>
<td></td>
</tr>
<tr>
<td>indicating 'AID_DENM'</td>
<td></td>
</tr>
<tr>
<td>} then {</td>
<td></td>
</tr>
<tr>
<td>the IUT discards the message</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>TP Id</td>
<td>TP_SEC_ISSS_RCV_DENM_08_03_BO</td>
</tr>
<tr>
<td>Summary</td>
<td>Check that IUT discards Secured DENM if the HeaderField generation_location is outside of the polygonal validity region of the signing certificate</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td>with {</td>
<td></td>
</tr>
<tr>
<td>the IUT being in the 'authorized' state</td>
<td></td>
</tr>
<tr>
<td>} ensure that {</td>
<td></td>
</tr>
<tr>
<td>when {</td>
<td></td>
</tr>
<tr>
<td>the IUT is receiving a SecuredMessage</td>
<td></td>
</tr>
<tr>
<td>containing header_fields ['signer_info'].type</td>
<td></td>
</tr>
<tr>
<td>indicating certificate</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields ['signer_info'].certificate (CERT_TS_AT_D)</td>
<td></td>
</tr>
<tr>
<td>containing validity_restrictions ['region'] {</td>
<td></td>
</tr>
<tr>
<td>containing region{</td>
<td></td>
</tr>
<tr>
<td>containing region_type</td>
<td></td>
</tr>
<tr>
<td>indicating 'polygon'</td>
<td></td>
</tr>
<tr>
<td>containing polygonal_region</td>
<td></td>
</tr>
<tr>
<td>indicating REGION</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>} and containing header_fields ['generation_location']</td>
<td></td>
</tr>
<tr>
<td>containing generation_location</td>
<td></td>
</tr>
<tr>
<td>indicating value outside of the REGION</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields ['its_aid']</td>
<td></td>
</tr>
<tr>
<td>indicating 'AID_DENM'</td>
<td></td>
</tr>
<tr>
<td>} then {</td>
<td></td>
</tr>
<tr>
<td>the IUT discards the message</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>TP Id</td>
<td>TP_SEC_ITSS_RCV_DENM_08_04_BO</td>
</tr>
<tr>
<td>--------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Summary</td>
<td>Check that IUT discards Secured DENM if the HeaderField generation_location is outside of the identified validity region of the signing certificate</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td>with {}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the IUT being in the 'authorized' state</td>
</tr>
<tr>
<td></td>
<td>ensure that {}</td>
</tr>
<tr>
<td></td>
<td>when {}</td>
</tr>
<tr>
<td></td>
<td>the IUT is receiving a SecuredMessage</td>
</tr>
<tr>
<td></td>
<td>containing header_fields ['signer_info'].type indicating certificate</td>
</tr>
<tr>
<td></td>
<td>and containing header_fields ['signer_info'].certificate (CERT_TS_AT_E)</td>
</tr>
<tr>
<td></td>
<td>containing validity_restrictions ['region']</td>
</tr>
<tr>
<td></td>
<td>containing region</td>
</tr>
<tr>
<td></td>
<td>containing region_type indicating 'id_region'</td>
</tr>
<tr>
<td></td>
<td>and containing identified_region</td>
</tr>
<tr>
<td></td>
<td>indicating REGION</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>and containing header_fields ['generation_location']</td>
</tr>
<tr>
<td></td>
<td>containing generation_location</td>
</tr>
<tr>
<td></td>
<td>indicating value outside of the REGION</td>
</tr>
<tr>
<td></td>
<td>and containing header_fields['its_aid']</td>
</tr>
<tr>
<td></td>
<td>indicating 'AID_DENM'</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>then {}</td>
</tr>
<tr>
<td></td>
<td>the IUT discards the message</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>

5.3.3.8 Check Payload

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_09_02_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards the Secured DENM containing empty payload of type 'signed'</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td>with {}</td>
<td></td>
</tr>
<tr>
<td></td>
<td>the IUT being in the 'authorized' state</td>
</tr>
<tr>
<td></td>
<td>ensure that {}</td>
</tr>
<tr>
<td></td>
<td>when {}</td>
</tr>
<tr>
<td></td>
<td>the IUT is receiving a SecuredMessage</td>
</tr>
<tr>
<td></td>
<td>containing header_fields['its_aid']</td>
</tr>
<tr>
<td></td>
<td>indicating 'AID_DENM'</td>
</tr>
<tr>
<td></td>
<td>and containing payload_field</td>
</tr>
<tr>
<td></td>
<td>containing type indicating 'signed'</td>
</tr>
<tr>
<td></td>
<td>containing data indicating length 0</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>then {}</td>
</tr>
<tr>
<td></td>
<td>the IUT discards the message</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>
TP Id | TP_SEC_ITSS_RCV_DENM_09_03_BO  
---|---
Summary | Check that IUT discards the Secured DENM containing non-empty payload of type 'unsecured'  
Reference | ETSI TS 103 097 [1], clause 7.2  
PICS Selection | PICS_GN_SECURITY

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields['its_aid']
      indicating 'AID_DENM'
      and containing payload_field {
        containing type
        indicating 'unsecured'
      }
    }
  }
  then {
    the IUT discards the message
  }
}

TP Id | TP_SEC_ITSS_RCV_DENM_09_04_BO  
---|---
Summary | Check that IUT discards the Secured DENM containing non-empty payload of type 'encrypted'  
Reference | ETSI TS 103 097 [1], clause 7.2  
PICS Selection | PICS_GN_SECURITY

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields['its_aid']
      indicating 'AID_DENM'
      and containing payload_field {
        containing type
        indicating 'encrypted'
      }
    }
  }
  then {
    the IUT discards the message
  }
}

TP Id | TP_SEC_ITSS_RCV_DENM_09_05_BO  
---|---
Summary | Check that IUT discards the Secured DENM containing non-empty payload of type 'signed_external'  
Reference | ETSI TS 103 097 [1], clause 7.2  
PICS Selection | PICS_GN_SECURITY

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields['its_aid']
      indicating 'AID_DENM'
      and containing payload_field {
        containing type
        indicating 'signed_external'
      }
    }
  }
  then {
    the IUT discards the message
  }
}
### 5.3.3.9 Check presence of trailer field

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_10_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards the Secured DENM if the message does not contain the trailer field of type 'signature'.</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields['its_aid']
        indicating 'AID_DENM'
        and containing payload_field {
          containing type
            indicating 'signed_and_encrypted'
        }
    }
  } then {
    the IUT discards the message
  }
}
```
### Check that IUT discards the Secured DENM containing more than one instance of TrailerField of type 'signature'

**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 {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields['its_aid']
      indicating 'AID_DENM'
      and containing trailer_fields[0]
      containing type
      indicating 'signature'
      and containing trailer_fields[1]
      containing type
      indicating 'signature'
    } then {
      the IUT discards the message
    }
  }
}

### Check signature

**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], clause 7.2

**PICS Selection**
PICS_GN_SECURITY

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields['its_aid']
      indicating 'AID_DENM'
      and containing trailer_fields['signature']
      containing type
      indicating 'signature'
      and containing trailer_fields['verification_key']
      containing key (KEY)
    } then {
      the IUT discards the message
    }
  }
}
### 5.3.3.11 Check signing certificate type

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_12_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards a Secured DENM if the signer certificate of the message contains the subject type 'enrolment_credential'</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
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_EA_A)
            containing subject_info.subject_type
                indicating 'enrolment_credentials'
        }
        containing header_fields['its_aid']
            indicating 'AID_DENM'
    } then {
        the IUT discards the message
    }
}
```

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_DENM_12_02_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards a Secured DENM if the signer certificate of the message contains the subject type &quot;authorization_authority&quot;</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.2</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
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
    }
}
```
### 5.3.4 Generic Signed Message Profile

#### 5.3.4.1 Check that IUT accepts well-formed GN Beacon message

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_GENMSG_01_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT accepts a well-formed Secured GN Beacon signed with the certificate without region validity restriction</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
with {
    the IUT being in the 'authorized' state
}
ensure that {
    when {
        the IUT is receiving a SecuredMessage
            containing protocol_version
                indicating value '2'
            and containing header_fields[0]
                containing type
                    indicating 'signer_info'
                and containing signer {
                    containing type
                        indicating 'certificate'
                    and containing certificate (CERT_TS_AT_A) {
                        containing subject_info.subject_type
                            indicating 'authorization_ticket' (2)
                        and containing subject_attributes['verification key'] (KEY)
                        and not containing validity_restrictions['region']
                    }
                }
            and containing header_fields [1] {
                containing type
                    indicating 'generation_time'
                containing generation_time
                    indicating CURRENT_TIME
            }
            and containing header_fields [2] {
                containing type
                    indicating 'generation_location'
                containing generation_location
            }
            and containing header_fields[3] {
                containing type
                    indicating 'its_aid'
                containing its_aid
                    indicating 'AID_BEACON'
            }
        and containing payload_field {
            containing type
                indicating 'signed'
            containing data
                indicating length > 0
        }
        and containing trailer_fields {
            containing single instance of type TrailerField {
                containing type
                    indicating 'signature'
                containing signature
                    verifiable using KEY
            }
        }
    then {
        the IUT accepts the message
    }
}
```
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_GENMSG_01_02_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT accepts a well-formed Secured GN Beacon signed with the certificate with a circular region validity restriction</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

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

**Reference**
ETSI TS 103 097 [1], clause 7.3

**PICS Selection**
PICS_GN_SECURITY

**Expected behaviour**

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

<table>
<thead>
<tr>
<th>Expected behaviour</th>
</tr>
</thead>
<tbody>
<tr>
<td>with {</td>
</tr>
<tr>
<td>the IUT being in the 'authorized' state</td>
</tr>
<tr>
<td>} ensure that {</td>
</tr>
<tr>
<td>when {</td>
</tr>
<tr>
<td>the IUT is receiving a SecuredMessage</td>
</tr>
<tr>
<td>containing protocol_version</td>
</tr>
<tr>
<td>indicating value '2'</td>
</tr>
<tr>
<td>and containing header_fields[0]</td>
</tr>
<tr>
<td>indicating 'signer_info'</td>
</tr>
<tr>
<td>and containing signer {</td>
</tr>
<tr>
<td>containing type</td>
</tr>
<tr>
<td>indicating 'certificate'</td>
</tr>
<tr>
<td>and containing certificate (CERT_TS_AT_D) {</td>
</tr>
<tr>
<td>containing subject_info.subject_type</td>
</tr>
<tr>
<td>indicating 'authorization_ticket' (2)</td>
</tr>
<tr>
<td>and containing subject_attributes['verification key'] (KEY)</td>
</tr>
<tr>
<td>and containing validity_restrictions['region'] {</td>
</tr>
<tr>
<td>containing region(</td>
</tr>
<tr>
<td>containing region_type</td>
</tr>
<tr>
<td>indicating 'polygon'</td>
</tr>
<tr>
<td>and containing polygonal_region</td>
</tr>
<tr>
<td>indicating REGION</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>and containing header_fields[1] {</td>
</tr>
<tr>
<td>containing type</td>
</tr>
<tr>
<td>indicating 'generation_time'</td>
</tr>
<tr>
<td>containing generation_time</td>
</tr>
<tr>
<td>indicating CURRENT_TIME</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>and containing header_fields[2] {</td>
</tr>
<tr>
<td>containing type</td>
</tr>
<tr>
<td>indicating 'generation_location'</td>
</tr>
<tr>
<td>containing generation_location</td>
</tr>
<tr>
<td>indicating position inside the REGION</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>and containing header_fields[3] {</td>
</tr>
<tr>
<td>containing type</td>
</tr>
<tr>
<td>indicating 'its_aid'</td>
</tr>
<tr>
<td>containing its_aid</td>
</tr>
<tr>
<td>indicating 'AID_BEACON'</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>and containing payload_field {</td>
</tr>
<tr>
<td>containing type</td>
</tr>
<tr>
<td>indicating 'signed'</td>
</tr>
<tr>
<td>containing data</td>
</tr>
<tr>
<td>indicating length &gt; 0</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>and containing trailer_fields {</td>
</tr>
<tr>
<td>containing single instance of type TrailerField {</td>
</tr>
<tr>
<td>containing type</td>
</tr>
<tr>
<td>indicating 'signature'</td>
</tr>
<tr>
<td>containing signature</td>
</tr>
<tr>
<td>verifiable using KEY</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td>then {</td>
</tr>
<tr>
<td>the IUT accepts the message</td>
</tr>
<tr>
<td>}</td>
</tr>
<tr>
<td><strong>TP Id</strong></td>
</tr>
<tr>
<td>-----------</td>
</tr>
<tr>
<td><strong>Summary</strong></td>
</tr>
<tr>
<td><strong>Reference</strong></td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is receiving a SecuredMessage
    containing protocol_version
    indicating value '2'
    and containing header_fields[0]
    indicating 'signer_info'
    and containing signer {
      containing type
      indicating 'certificate'
      and containing certificate (CERT_TS_AT_E) {
        containing subject_info.subject_type
        indicating 'authorization_ticket' (2)
        and containing subject_attributes['verification key'] (KEY)
        and containing validity_restrictions['region'] {
          containing region{
            containing region_type
            indicating 'id_region'
            and containing identified_region
            indicating REGION
          }
        }
      }
    }
    and containing header_fields [1] {
      containing type
      indicating 'generation_time'
      containing generation_time
      indicating CURRENT_TIME
    }
    and containing header_fields [2] {
      containing type
      indicating 'generation_location'
      containing generation_location
      indicating position inside the REGION
    }
    and containing header_fields[3] {
      containing type
      indicating 'its_aid'
      containing its_aid
      indicating 'AID_BEACON'
    }
    and containing payload_field {
      containing type
      indicating 'signed'
      containing data
      indicating length > 0
    }
    and containing trailer_fields {
      containing single instance of type TrailerField {
        containing type
        indicating 'signature'
        containing signature
        verifiable using KEY
      }
    }
  }
} then {
  the IUT accepts the message
}
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_GENMSG_01_06_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT accepts a well-formed Secured GN Message containing payload of type signed_external</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      and containing header_fields[0] {
        containing type
          indicating 'signer_info'
          and containing signer.type
          indicating 'certificate'
          and containing signer.certificate
            indicating CERT_TS_AT_A
      }
      and containing header_fields['its_aid']
        indicating 'AID_BEACON'
      and containing payload_field
        containing type
          indicating 'signed_external'
    }
  }
  then {
    the IUT accepts the message
  }
}

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_GENMSG_01_07_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT accepts a well-formed Secured GN Message containing payload of type signed_and_encrypted</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      and containing header_fields[0] {
        containing type
          indicating 'signer_info'
          and containing signer.type
          indicating 'certificate'
          and containing signer.certificate
            indicating CERT_TS_AT_A
      }
      and containing header_fields['its_aid']
        indicating 'AID_BEACON'
      and containing payload_field
        containing type
          indicating 'signed_and_encrypted'
    }
  }
  then {
    the IUT accepts the message
  }
}
### 5.3.4.2 Check the message protocol version

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_GENMSG_02_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards a Secured GN Message containing protocol version set to a value less than 2</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 5.2</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>with {</td>
</tr>
<tr>
<td></td>
<td>the IUT being in the 'authorized' state</td>
</tr>
<tr>
<td></td>
<td>} ensure that {</td>
</tr>
<tr>
<td></td>
<td>when {</td>
</tr>
<tr>
<td></td>
<td>the IUT is receiving a SecuredMessage</td>
</tr>
<tr>
<td></td>
<td>containing protocol_version</td>
</tr>
<tr>
<td></td>
<td>indicating 1</td>
</tr>
<tr>
<td></td>
<td>and containing header_fields['its_aid']</td>
</tr>
<tr>
<td></td>
<td>indicating 'AID_BEACON'</td>
</tr>
<tr>
<td></td>
<td>} then {</td>
</tr>
<tr>
<td></td>
<td>the IUT discards a SecuredMessage</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_GENMSG_02_02_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards a Secured GN Message containing protocol version set to a value greater than 2</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 5.2</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>with {</td>
</tr>
<tr>
<td></td>
<td>the IUT being in the 'authorized' state</td>
</tr>
<tr>
<td></td>
<td>} ensure that {</td>
</tr>
<tr>
<td></td>
<td>when {</td>
</tr>
<tr>
<td></td>
<td>the IUT is receiving a SecuredMessage</td>
</tr>
<tr>
<td></td>
<td>containing protocol_version</td>
</tr>
<tr>
<td></td>
<td>indicating 3</td>
</tr>
<tr>
<td></td>
<td>and containing header_fields['its_aid']</td>
</tr>
<tr>
<td></td>
<td>indicating 'AID_BEACON'</td>
</tr>
<tr>
<td></td>
<td>} then {</td>
</tr>
<tr>
<td></td>
<td>the IUT discards a SecuredMessage</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>
### 5.3.4.3 Check header fields

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV GENMSG_04_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards a secured GN Beacon if the header_fields contains more than one element of header field type: signer_info</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.3</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
with {
    the IUT being in the 'authorized' state
} ensure that {
    when {
        the IUT is receiving a SecuredMessage
        containing header_fields[0].type indicating 'signer_info'
        and containing header_fields[1].type indicating 'signer_info'
        and containing header_fields[2].type indicating 'generation_time'
        and containing header_fields[3].type indicating 'generation_location'
        and containing header_fields['its_aid'] indicating 'AID_BEACON'
        and not containing other header fields
    } then {
        the IUT discards a SecuredMessage
    }
}
```

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV GENMSG_04_02_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards a secured GN Beacon if the header_fields does not contain the header field type: signer_info</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.3</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
with {
    the IUT being in the 'authorized' state
} ensure that {
    when {
        the IUT is receiving a SecuredMessage
        containing header_fields[0].type indicating 'generation_time'
        and containing header_fields[1].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
    }
}
```
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_GENMSG_04_04_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards a secured GN Beacon if</td>
</tr>
<tr>
<td></td>
<td>the header_fields contains more than one element</td>
</tr>
<tr>
<td></td>
<td>of header field type: generation_time</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.3</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Expected behaviour</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>with {</td>
<td></td>
</tr>
<tr>
<td>the IUT being in the 'authorized' state</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>ensure that {</td>
<td></td>
</tr>
<tr>
<td>when {</td>
<td></td>
</tr>
<tr>
<td>the IUT is receiving a</td>
<td></td>
</tr>
<tr>
<td>SecuredMessage</td>
<td></td>
</tr>
<tr>
<td>containing header_fields[0].type</td>
<td></td>
</tr>
<tr>
<td>indicating 'signer_info'</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields[1].type</td>
<td></td>
</tr>
<tr>
<td>indicating 'generation_time'</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields[2].type</td>
<td></td>
</tr>
<tr>
<td>indicating 'generation_time'</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields[3].type</td>
<td></td>
</tr>
<tr>
<td>indicating 'generation_location'</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields['its_aid'] indicating 'AID_BEACON'</td>
<td></td>
</tr>
<tr>
<td>and not containing other header fields</td>
<td></td>
</tr>
<tr>
<td>} then {</td>
<td></td>
</tr>
<tr>
<td>the IUT discards a SecuredMessage</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_GENMSG_04_05_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that IUT discards a secured GN Beacon if</td>
</tr>
<tr>
<td></td>
<td>the message does not contain the header field of</td>
</tr>
<tr>
<td></td>
<td>type 'generation_time'</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.3</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Expected behaviour</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>with {</td>
<td></td>
</tr>
<tr>
<td>the IUT being in the 'authorized' state</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
<tr>
<td>ensure that {</td>
<td></td>
</tr>
<tr>
<td>when {</td>
<td></td>
</tr>
<tr>
<td>the IUT is receiving a</td>
<td></td>
</tr>
<tr>
<td>SecuredMessage</td>
<td></td>
</tr>
<tr>
<td>containing header_fields[0].type</td>
<td></td>
</tr>
<tr>
<td>indicating 'signer_info'</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields[1].type</td>
<td></td>
</tr>
<tr>
<td>indicating 'generation_location'</td>
<td></td>
</tr>
<tr>
<td>and containing header_fields['its_aid'] indicating 'AID_BEACON'</td>
<td></td>
</tr>
<tr>
<td>and not containing other header fields</td>
<td></td>
</tr>
<tr>
<td>} then {</td>
<td></td>
</tr>
<tr>
<td>the IUT discards a SecuredMessage</td>
<td></td>
</tr>
<tr>
<td>}</td>
<td></td>
</tr>
</tbody>
</table>
### TP Id: TP_SEC_ITSS_RCV_GENMSG_04_06_BO

**Summary:** Check that IUT discards a secured GN Beacon if the header_fields contains more than one element of type: generation_location

**Reference:** ETSI TS 103 097 [1], clause 7.3

**PICS Selection:** PICS_GN_SECURITY

**Expected behaviour**

```python
with {
    the IUT being in the 'authorized' state
}
ensure that {
    when {
        the IUT is receiving a SecuredMessage
            containing header_fields[0].type
                indicating 'signer_info'
            and containing header_fields[1].type
                indicating 'generation_time'
            and containing header_fields[2].type
                indicating 'generation_location'
            and containing header_fields[3].type
                indicating 'generation_location'
            and containing header_fields['its_aid']
                indicating 'AID_BEACON'
            and not containing other header fields
    } then {
        the IUT discards a SecuredMessage
    }
}
```

### TP Id: TP_SEC_ITSS_RCV_GENMSG_04_07_BO

**Summary:** Check that IUT discards a secured GN Beacon if the header_fields contains no element of header field type generation_location

**Reference:** ETSI TS 103 097 [1], clause 7.3

**PICS Selection:** PICS_GN_SECURITY

**Expected behaviour**

```python
with {
    the IUT being in the 'authorized' state
}
ensure that {
    when {
        the IUT is receiving a SecuredMessage
            containing header_fields[0].type
                indicating 'signer_info'
            and containing header_fields[1].type
                indicating 'generation_time'
            and containing header_fields['its_aid']
                indicating 'AID_BEACON'
            and not containing other header fields
    } then {
        the IUT discards a SecuredMessage
    }
}
```
5.3.4.4 Check signer info

---

**TP Id**  
TP_SEC_LTSS_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
}
ensure that {
when {
the IUT is receiving a SecuredMessage {
containing header_fields['signer_info']
containing signer.type
indicating 'self'
and containing header_fields['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_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 
- the IUT being in the 'authorized' state

ensure that 
- when 
  - the IUT is receiving a SecuredMessage 
    - containing header_fields['signer_info']
      - containing signer.type
        - indicating 'certificate_digest_with_other_algorithm'
      and containing header_fields['generation_time']
      and containing header_fields['generation_location']
      and containing header_fields['its_aid']
        - indicating 'AID_BEACON'
      and not containing other header fields
  then 
  - the IUT discards a SecuredMessage

---

### TP Id
TP_SEC_ITSS_RCV_GENMSG_05_03_BO

### Summary
Check that IUT discards a secured GN Beacon if the header_fields contains a signer of type 'certificate_chain'.

### Reference
ETSI TS 103 097 [1], clause 7.3

### PICS Selection
PICS_GN_SECURITY

### Expected behaviour

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_chain'
      and containing header_fields['generation_time']
      and containing header_fields['generation_location']
      and containing header_fields['its_aid']
        - indicating 'AID_BEACON'
      and not containing other header fields
  then 
  - the IUT discards a SecuredMessage

5.3.4.5 Check generation time

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_GENMSG_06_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards message containing generation_time before the certificate validity period</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 5.4 and 7.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

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

ensure that {
    when {
        the IUT is receiving a SecuredMessage {
            containing header_fields[0] {
                containing type
                    indicating 'signer_info'
                and containing signer {
                    containing type
                        indicating 'certificate'
                    and containing certificate (CERT_TS_AT_A) {
                        containing validity_restrictions['time_start_and_end'] {
                            containing start_validity
                                indicating TIME_CERT_TS_AT_START
                            and containing end_validity
                                indicating TIME_CERT_TS_AT_END
                        }
                    }
                }
            }
        } and containing header_fields[1] {
            containing type
                indicating 'generation_time'
            containing generation_time
                indicating TIME_1 < TIME_CERT_TS_AT_START
        }
        } and containing header_fields[2] {
            containing type
                indicating 'generation_location'
        }
        } and containing header_fields['its_aid'] {
            indicating 'AID_BEACON'
        }
    }
    then {
        the IUT discards the message
    }
}
Summary
Check that IUT discards message containing generation_time after the certificate validity period.

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

PI
CS Selection
PICS_GN_SECURITY

Expected behaviour

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

**TP Id** | TP_SEC_ITSS_RCV_GENMSG_08_01_BO
---|---
**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, PICS_USE_CIRCULAR_REGION

**Expected behaviour**

with {  
  the IUT being in the 'authorized' state  
}  
ensure that {  
  when {  
    the IUT is receiving a SecuredMessage  
    and containing header_fields ['signer_info'] {  
      containing type  
      indicating certificate  
      and containing certificate (CERT_TS_AT_B)  
      containing validity_restrictions ['region']  
      containing region{  
        containing region_type  
        indicating 'circle'  
        containing circular_region  
        indicating REGION  
      }  
    }  
    and containing header_fields ['generation_location']  
    containing generation_location  
    indicating value outside of the REGION  
    and containing header_fields['its_aid']  
    indicating 'AID_BEACON'  
  } then {  
    the IUT discards the message  
  }  
}

---

**TP Id** | TP_SEC_ITSS_RCV_GENMSG_08_02_BO
---|---
**Summary** | Check that IUT discards Secured GN Message if the HeaderField generation_location is outside of the rectangular validity region of the signing certificate
**Reference** | ETSI TS 103 097 [1], clause 7.3
**PICS Selection** | PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION

**Expected behaviour**

with {  
  the IUT being in the 'authorized' state  
}  
ensure that {  
  when {  
    the IUT is receiving a SecuredMessage  
    and containing header_fields ['signer_info'] {  
      containing type  
      indicating certificate  
      and containing certificate (CERT_TS_AT_C)  
      containing validity_restrictions ['region']  
      containing region{  
        containing region_type  
        indicating 'rectangle'  
        containing rectangular_regions  
        indicating REGION  
      }  
    }  
    and containing header_fields ['generation_location']  
    containing generation_location  
    indicating value outside of the REGION  
    and containing header_fields['its_aid']  
    indicating 'AID_BEACON'  
  } 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, PICS_USE_POLYGONAL_REGION

**Expected behaviour**

```plaintext
with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage
    and containing header_fields ['signer_info'] {
      containing type
      indicating certificate
      and containing certificate (CERT_TS_AT_D)
      containing validity_restrictions ['region']
      containing region {
        containing region_type
        indicating 'polygon'
        containing polygonal_region
        indicating REGION
      }
    }
    and containing header_fields ['generation_location']
    containing generation_location
    indicating value outside of the REGION
    and containing header_fields ['its_aid']
    indicating 'AID_BEACON'
  } then {
    the IUT discards the message
  }
}
```

### TP 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, PICS_USE_IDENTIFIED_REGION

**Expected behaviour**

```plaintext
with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage
    containing header_fields ['signer_info'] {
      containing type
      indicating certificate
      and containing certificate (CERT_TS_AT_E)
      containing validity_restrictions ['region']
      containing region {
        containing region_type
        indicating 'id_region'
        and containing identified_region
        indicating REGION
      }
    }
    and containing header_fields ['generation_location']
    containing generation_location
    indicating value outside of the REGION
    and containing header_fields ['its_aid']
    indicating 'AID_BEACON'
  } then {
    the IUT discards the message
  }
}
```
5.3.4.7 Check Payload

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_GENMSG_09_02_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards the Secured GN Message containing empty payload of type 'signed'</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
with {
    the IUT being in the 'authorized' state
} ensure that {
    when {
        the IUT is receiving a SecuredMessage {
            containing header_fields['its_aid']
            indicating 'AID_BEACON'
            and containing payload_field {
                containing type
                indicating 'signed'
                containing data
                indicating length 0
            }
        }
    }
    then {
        the IUT discards the message
    }
}
```

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_GENMSG_09_03_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards the Secured GN Message containing payload element of type 'unsecured'</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
with {
    the IUT being in the 'authorized' state
} ensure that {
    when {
        the IUT is receiving a SecuredMessage {
            containing header_fields['its_aid']
            indicating 'AID_BEACON'
            and containing payload_field {
                containing type
                indicating 'unsecured'
            }
        }
    }
    then {
        the IUT discards the message
    }
}
```
### 5.3.4.8 Check presence of trailer field

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_GENMSG_10_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards the Secured GN Message if the message does not contain the trailer field of type 'signature'</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.3</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td>Expected behaviour</td>
<td>with {</td>
</tr>
<tr>
<td></td>
<td>the IUT being in the 'authorized' state</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>ensure that {</td>
</tr>
<tr>
<td></td>
<td>when {</td>
</tr>
<tr>
<td></td>
<td>the IUT is receiving a SecuredMessage {</td>
</tr>
<tr>
<td></td>
<td>containing header_fields['its_aid']</td>
</tr>
<tr>
<td></td>
<td>indicating 'AID_BEACON'</td>
</tr>
<tr>
<td></td>
<td>and containing trailer_fields</td>
</tr>
<tr>
<td></td>
<td>not containing any instance of type TrailerField {</td>
</tr>
<tr>
<td></td>
<td>containing type</td>
</tr>
<tr>
<td></td>
<td>indicating 'signature'</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>then {</td>
</tr>
<tr>
<td></td>
<td>the IUT discards the message</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>

```c
with {  
  the IUT being in the 'authorized' state  
}  
ensure that {  
  when {  
    the IUT is receiving a SecuredMessage {  
      containing header_fields['its_aid']  
        indicating 'AID_BEACON'  
      and containing trailer_fields  
        not containing any instance of type TrailerField {  
          containing type  
            indicating 'signature'  
        }  
    }  
  }  
  then {  
    the IUT discards the message  
  }  
```

### 5.3.4.8 Check presence of trailer field

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

```c
with {  
  the IUT being in the 'authorized' state  
}  
ensure that {  
  when {  
    the IUT is receiving a SecuredMessage {  
      containing header_fields['its_aid']  
        indicating 'AID_BEACON'  
      and containing payload_field {  
        containing type  
          indicating 'encrypted'  
      }  
    }  
  }  
  then {  
    the IUT discards the message  
  }  
```

```c
with {  
  the IUT being in the 'authorized' state  
}  
ensure that {  
  when {  
    the IUT is receiving a SecuredMessage {  
      containing header_fields['its_aid']  
        indicating 'AID_BEACON'  
      and containing payload_field {  
        containing type  
          indicating 'encrypted'  
      }  
    }  
  }  
  then {  
    the IUT discards the message  
  }  
```
### TP Id

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_GENMSG_10_02_BO</th>
</tr>
</thead>
</table>

### 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 {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields['its_aid']
          indicating 'AID_Beacon'
    }
    and containing trailer_fields
      containing 2 instances of type TrailerField {
        containing type
          indicating 'signature'
      }
  }
} then {
  the IUT discards the message
}

## 5.3.4.9 Check signature

### TP Id

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_GENMSG_11_01_BO</th>
</tr>
</thead>
</table>

### Summary

Check that the IUT discards Secured GN Message containing signature that is not verified using the verification key from the certificate contained in the message's signer info

### Reference

ETSI TS 103 097 [1], clause 7.3

### PICS Selection

PICS_GN_SECURITY

### Expected behaviour

with {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields['its_aid']
          indicating 'AID_Beacon'
    }
    and containing header_fields ['signer_info'] {
      containing signer {
        containing type
          indicating 'certificate'
        containing certificate
          containing subject_info.subject_type
            indicating 'authorization_ticket' (2)
          containing subject_attributes['verification_key'] (KEY)
      }
      and containing payload_field {
        containing type
          indicating 'signed'
      }
      and containing trailer_fields {
        containing single instance of type TrailerField {
          containing type
            indicating 'signature'
          containing signature
            NOT verifiable using KEY
        }
      }
    }
} then {
  the IUT discards the message
}
5.3.4.10 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 7.3

**PICS Selection**: PICS_GN_SECURITY

**Expected behaviour**

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

ensure that {
  when {
    the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info'] {
        containing signer.type indicating 'certificate'
          containing signer.certificate.subject_info.subject_type indicating 'enrolment_credentials'
      }
      and containing header_fields['its_aid'] indicating 'AID_BEACON'
  } then {
    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 7.3

**PICS Selection**: PICS_GN_SECURITY

**Expected behaviour**

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

ensure that {
  when {
    the IUT is receiving a SecuredMessage
      containing header_fields ['signer_info'] {
        containing signer.type indicating 'certificate'
          containing signer.certificate.subject_info.subject_type indicating 'authorization_authority'
      }
      and containing header_fields['its_aid'] indicating 'AID_BEACON'
  } then {
    the IUT discards the message
  }
}
5.3.5 Profiles for certificates

5.3.5.1 Check that certificate version is 2

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

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_01_02_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards the AT certificate with version 1</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 6.1 and 7.4</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>
| Expected behaviour     | with {
|                        |   the IUT being in the 'authorized' state
|                        | } ensure that {
|                        | with {
|                        |   the IUT is receiving a SecuredMessage {
|                        |     containing header_fields ['signer_info'] {
|                        |       containing signer {
|                        |         containing type
|                        |           indicating 'certificate'
|                        |         containing certificate (CERT_TS_01_02_BO_AT)
|                        |         containing version
|                        |           indicating '1'
|                        |     }
|                        | }
|                        | } then {
|                        |   the IUT discards the message
|                        | }
5.3.5.2 Check that enrolment certificate is not used for sign other certificates

Void.

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

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

Void.

5.3.5.5 Check the certificate signature

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_05_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards the message when signing AT certificate has a not valid signature</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 6.1 and 7.4</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**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_A_AT) {
            containing signer_info.digest referencing to a CERT_TS_A_AA
            containing signature
            NOT verifiable with CERT_TS_A_AA.subject_attributes['verification_key'].key
          }
        }
      }
    }
  }
  then {
    the IUT discards the message
  }
}

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_05_02_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that IUT discards the message when the issuing AA certificate of the signing AT certificate has a not valid signature</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 6.1 and 7.4</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**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_chain'
          containing certificates[0] (CERT_TS_A_AA) {
            containing signer_info.digest referencing to a CERT_ROOT
            containing signature
            not verifiable with CERT_ROOT.subject_attributes['verification_key'].key
          }
          containing certificates[1] (CERT_TS_A_AT) {
            containing signer_info.digest referencing to a CERT_TS_A_AA
          }
        }
      }
    }
  }
  then {
    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 its signing certificate contains the same circular region validity restriction as its issuing certificate

**Reference**  ETSI TS 103 097 [1], clause 7.4

**PICS Selection**  PICS_GN_SECURITY, PICS_USE_CIRCULAR_REGION

**Expected behaviour**

```
with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_06_01_BV_AT) {
            containing validity_restrictions['region'] {
              containing region_type
                indicating 'circle'
              containing circular_region
                indicating CURCULAR_REGION_AA
            }
            containing signer_info.digest
              referencing to a CERT_TS_B_AA
          }
        }
      }
    }
  }
  then {
    the IUT accepts the message
  }
}
```

**TP Id**  TP_SEC_ITSS_RCV_CERT_06_02_BV

**Summary**  Check that the IUT accepts a message when its signing certificate contains the validity restriction with circular region which is fully inside in the validity region of its issuing certificate

**Reference**  ETSI TS 103 097 [1], clause 7.4

**PICS Selection**  PICS_GN_SECURITY, PICS_USE_CIRCULAR_REGION

**Expected behaviour**

```
with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_06_02_BV_AT) {
            containing validity_restrictions['region'] {
              containing region_type
                indicating 'circle'
              containing circular_region
                indicating CURCULAR_REGION_AT
            }
            containing signer_info.digest
              referencing to a CERT_TS_B_AA
          }
        }
      }
    }
  }
  then {
    the IUT accepts the message
  }
}
```
TP Id | TP_SEC_ITSS_RCV_CERT_06_03_BO
--- | ---
Summary | Check that the IUT discards a message when its signing certificate does not contain the validity restriction of type 'region' but its issuing certificate contains the circular region validity restriction
Reference | ETSI TS 103 097 [1], clause 7.4
PICS Selection | PICS_GN_SECURITY, PICS_USE_CIRCULAR_REGION

**Expected behaviour**

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

ensure that {
  
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_06_03_BO_AT) {
            not containing validity_restrictions['region']
            and containing signer_info.digest
            referencing to a CERT_TS_B_AA
          }
          }
        }
    }
  }
}

} then {
  the IUT discards the message
}

---

TP Id | TP_SEC_ITSS_RCV_CERT_06_04_BO
--- | ---
Summary | Check that the IUT discards a message when the circular validity region of the signing certificate is outside of the validity region of the issuing certificate
Reference | ETSI TS 103 097 [1], clause 7.4
PICS Selection | PICS_GN_SECURITY, PICS_USE_CIRCULAR_REGION

**Expected behaviour**

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

ensure that {
  
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_06_04_BO_AT) {
            containing validity_restrictions['region'] {
              containing region_type
                indicating 'circle'
              containing circular_region
                indicating CURCULAR_REGION_AT
            }
            containing signer_info.digest
            referencing to a CERT_TS_06_04_BO_AA
            containing validity_restrictions['region'] {
              containing region_type
                indicating 'circle'
              containing circular_region
                indicating CURCULAR_REGION_AA_OUTSIDE
            }
          }
          }
        }
    }
  }
}

} then {
  the IUT discards the message
}

---
**TP Id**

TP_SEC_ITSS_RCV_CERT_06_05_BO

**Summary**

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

**Reference**

ETSI TS 103 097 [1], clause 7.4

**PICS Selection**

PICS_GN_SECURITY, PICS_USE_CIRCULAR_REGION

**Expected behaviour**

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

ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_06_05_BO_AT) {
            containing validity_restrictions['region'] {
              containing region_type
                indicating 'circle'
              containing circular_region
                indicating CURCULAR_REGION_AT
            }
            containing signer_info.digest
              referencing to a CERT_TS_06_05_BO_AA
              containing validity_restrictions['region'] {
                containing region_type
                  indicating 'circle'
                containing circular_region
                  indicating CURCULAR_REGION_AA_INTERSECT
            }
          }
        }
      }
    }
  }
  then {
    the IUT discards the message
  }
}
### 5.3.5.7 Check rectangular region of subordinate certificate

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_07_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that the IUT accepts a message when its signing certificate contains the same validity restriction with rectangular regions as its issuing certificate</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.4</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
            containing certificate (CERT_TS_07_01_BV_AT) {
              containing validity_restrictions ['region'] {
                containing region_type
                  indicating 'rectangle'
                  containing rectangular_region[0]
                    indicating RECT_REGION_AA
                }
                containing signer_info.digest
                  referencing to a CERT_TS_C_AA
              }
          }
        }
    }
  }
  then {
    the IUT accepts the message
  }
}
```

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_07_02_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that the IUT accepts a message when its signing certificate contains the rectangular validity region which is fully inside of the validity region of its issuing certificate</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.4</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
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_AT_07_02_NB) {
              containing validity_restrictions ['region'] {
                containing region_type
                  indicating 'rectangle'
                  containing rectangular_region[0]
                    indicating RECT_REGION_TS_AT
                }
                containing signer_info.digest
                  referencing to a CERT_TS_AA_C
              }
          }
        }
    }
  }
  then {
    the IUT accepts the message
  }
}
```
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_07_03_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that the IUT discards a message when the signing certificate does not contain a region validity restriction but its issuing certificate contains the rectangular region validity restriction.</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.4</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>with {</td>
</tr>
<tr>
<td></td>
<td>the IUT being in the 'authorized' state }</td>
</tr>
<tr>
<td></td>
<td>ensure that {</td>
</tr>
<tr>
<td></td>
<td>when {</td>
</tr>
<tr>
<td></td>
<td>the IUT is receiving a SecuredMessage {</td>
</tr>
<tr>
<td></td>
<td>containing header_fields ['signer_info'] {</td>
</tr>
<tr>
<td></td>
<td>containing signer {</td>
</tr>
<tr>
<td></td>
<td>containing type</td>
</tr>
<tr>
<td></td>
<td>indicating 'certificate'</td>
</tr>
<tr>
<td></td>
<td>containing certificate (CERT_TS_07_03_BO_AT) {</td>
</tr>
<tr>
<td></td>
<td>not containing validity_restrictions['region']</td>
</tr>
<tr>
<td></td>
<td>containing signer_info.digest</td>
</tr>
<tr>
<td></td>
<td>referencing to a CERT_TS_C_AA</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>} then {</td>
</tr>
<tr>
<td></td>
<td>the IUT discards the message</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_07_04_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that the IUT discards a message when the rectangular validity region of the message signing certificate is outside of the validity region of its issuing certificate.</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.4</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION</td>
</tr>
<tr>
<td><strong>Expected behaviour</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>with {</td>
</tr>
<tr>
<td></td>
<td>the IUT being in the 'authorized' state }</td>
</tr>
<tr>
<td></td>
<td>ensure that {</td>
</tr>
<tr>
<td></td>
<td>when {</td>
</tr>
<tr>
<td></td>
<td>the IUT is receiving a SecuredMessage {</td>
</tr>
<tr>
<td></td>
<td>containing header_fields ['signer_info'] {</td>
</tr>
<tr>
<td></td>
<td>containing signer {</td>
</tr>
<tr>
<td></td>
<td>containing type</td>
</tr>
<tr>
<td></td>
<td>indicating 'certificate'</td>
</tr>
<tr>
<td></td>
<td>containing certificate (CERT_TS_07_04_BO_AT) {</td>
</tr>
<tr>
<td></td>
<td>containing validity_restrictions['region'] {</td>
</tr>
<tr>
<td></td>
<td>containing region_type</td>
</tr>
<tr>
<td></td>
<td>indicating 'rectangle'</td>
</tr>
<tr>
<td></td>
<td>containing rectangular_region[0]</td>
</tr>
<tr>
<td></td>
<td>indicating RECT_REGION_AT</td>
</tr>
<tr>
<td></td>
<td>containing signer_info.digest</td>
</tr>
<tr>
<td></td>
<td>referencing to a CERT_TS_07_04_BO_AA</td>
</tr>
<tr>
<td></td>
<td>containing validity_restrictions['region'] {</td>
</tr>
<tr>
<td></td>
<td>containing region_type</td>
</tr>
<tr>
<td></td>
<td>indicating 'rectangle'</td>
</tr>
<tr>
<td></td>
<td>containing rectangular_region[0]</td>
</tr>
<tr>
<td></td>
<td>indicating RECT_REGION_AA_OUTSIDE</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>} then {</td>
</tr>
<tr>
<td></td>
<td>the IUT discards the message</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>
Summary
Check that the IUT discards a message when the rectangular validity region of the message signing certificate is not fully covered by the validity region of the issuing certificate.

Reference
ETSI TS 103 097 [1], clause 7.4

PICS Selection
PICS_GN_SECURITY, PICS_USE_RECTANGULAR_REGION

Expected behaviour

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_07_05_BO_AT) {
            containing validity_restrictions['region'] {
              containing region_type
                indicating 'rectangle'
              containing rectangular_region[0]
                indicating RECT_REGION_AT
            }
            containing signer_info.digest
              referencing to a CERT_TS_07_05_BO_AA
              containing validity_restrictions['region'] {
                containing region_type
                  indicating 'rectangle'
                containing rectangular_region[0]
                  indicating RECT_REGION_AA_INTERSECT
              }
          }
        }
      }
    }
  }
} then {
  the IUT discards the message
}
5.3.5.8 Check polygonal region of subordinate certificate

**TP Id**  | **TP_SEC_ITSS_RCV_CERT_08_01_BV**
---|---
**Summary** | Check that the IUT accepts a message when its signing certificate contains the same polygonal region validity restriction as its issuing certificate
**Reference** | ETSI TS 103 097 [1], clause 7.4
**PICS Selection** | PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage { containing header_fields ['signer_info'] { containing signer { containing type indicating 'certificate' containing certificate (CERT_TS_08_01_BV_AT) { containing validity_restrictions['region'] { containing region_type indicating 'polygon' containing polygonal_region indicating POLYGON_REGION_AA } containing signer_info.digest referencing to a CERT_TS_D_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 its signing certificate contains the validity restriction with the polygonal region which is fully inside in the validity region of its issuing certificate
**Reference** | ETSI TS 103 097 [1], clause 7.4
**PICS Selection** | PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage { containing header_fields ['signer_info'] { containing signer { containing type indicating 'certificate' containing certificate (CERT_TS_08_02_BV_AT) { containing validity_restrictions['region'] { containing region_type indicating 'polygon' containing polygonal_region indicating POLYGON_REGION_AT } containing signer_info.digest referencing to a CERT_TS_D_AA } } } then { the IUT accepts the message }
  }
}
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC ITSS RCV CERT_08_03_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the IUT discards a message when its signing certificate does not contain a region validity restriction but its issuing certificate contains the polygonal region validity restriction</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.4</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
    the IUT being in the 'authorized' state
} ensure that {
    when {
        the IUT is receiving a SecuredMessage {
            containing header_fields ['signer_info'] {
                containing signer {
                    containing type
                        indicating 'certificate'
                    containing certificate (CERT_TS_08_03_BO_AT) {
                        not containing validity_restrictions['region']
                        containing signer_info.digest
                            referencing to a CERT_TS_D_AA
                    }
                }
            }
        } then {
            the IUT discards the message
        }
    }
}

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC ITSS RCV CERT_08_04_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the IUT discards a message when signing certificate contains a polygonal region validity restriction containing less than 3 points</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 4.2.24 and 7.4</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
    the IUT being in the 'authorized' state
} ensure that {
    when {
        the IUT is receiving a SecuredMessage {
            containing header_fields ['signer_info'] {
                containing signer {
                    containing type
                        indicating 'certificate'
                    containing certificate (CERT_TS_08_04_BO_AT) {
                        containing validity_restrictions['region'] {
                            containing region_type
                                indicating 'polygon'
                            containing polygonal_region
                                containing length
                                    indicating 2
                        containing signer_info.digest
                            referencing to a CERT_TS_D_AA
                    }
                }
            }
        } then {
            the IUT discards the message
        }
    }
}
TP Id: TP_SEC_ITSS_RCV_CERT_08_05_BO

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

Reference: ETSI TS 103 097 [1], clause 7.4

PICS Selection: PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION

**Expected behaviour**

```plaintext
with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_08_05_BO_AT) {
            containing region_type
              indicating 'polygon'
            containing polygonal_region
              indicating POLYGON_REGION_AT
          }
          containing signer_info.digest
            referencing to a CERT_TS_08_05_BO_AA
            containing validity_restrictions['region'] {
              containing region_type
                indicating 'polygon'
              containing polygonal_region
                indicating POLYGON_REGION_AA_OUTSIDE
            }
        }
      }
    }
  }
}
then {
  the IUT discards the message
}
```
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_08_06_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>Check that the IUT discards a message when the polygonal validity region of the message signing certificate is not fully covered by the validity region of its issuing certificate</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clause 7.4</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY, PICS_USE_POLYGONAL_REGION</td>
</tr>
</tbody>
</table>

**Expected behaviour**

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

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC.ITSS.RCV.CERT_09_01_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the IUT accepts a message when its signing certificate contains the region validity restriction with the same identified region as the issuing certificate and without local area definition</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 4.2.26 and 7.4</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION</td>
</tr>
</tbody>
</table>
| Expected behaviour | with { the IUT being in the 'authorized' state } ensure that { when { the IUT is receiving a SecuredMessage { containing header_fields ['signer_info'] { containing signer { containing type indicating 'certificate' containing certificate (CERT_TS_09_01_BV_AT) { containing validity_restrictions['region'] { containing region_type indicating 'id' containing id_region { containing region_dictionary indicating 'iso_3166_1' (0) containing region_identifier indicating ID_REGION_AT containing local_region indicating 0 } containing signer_info.digest referencing to a CERT_AA_ES_TS } } } } then { the IUT accepts the message } } } }
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_09_02_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the IUT accepts a message when its signing certificate contains the identified region validity restriction with the same identified region as in the issuing certificate but with the local area definition</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 4.2.26 and 7.4</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION</td>
</tr>
</tbody>
</table>

**Expected behaviour**

```plaintext
with {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_09_01_BV_AT) {
            containing validity_restrictions['region'] {
              containing region_type
                indicating 'id'
              containing id_region {
                containing region_dictionary
                  indicating 'iso_3166_1' (0)
                containing region_identifier
                  indicating ID_REGION_AT
                containing local_region
                  indicating 1
              }
            }
          }
        }
      }
    }
  }
} then {
  the IUT accepts the message
}
```
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_09_03_BV</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the IUT accepts a message when its signing certificate contains the region validity restriction with the identified region which is fully covered by the identified validity region of the issuing certificate</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 4.2.26 and 7.4</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_09_03_BV_AT) {
            containing validity_restrictions ['region'] {
              containing region_type
                indicating 'id'
              containing id_region {
                containing region_dictionary
                  indicating 'un_stats' (1)
                containing region_identifier
                  indicating ID_REGION_AT
                containing local_region
                  indicating 0
              }
            }
          }
          containing signer_info.digest
            referencing to a CERT_TS_09_03_BV_AA {
              containing validity_restrictions ['region'] {
                containing region_type
                  indicating 'id'
                containing id_region {
                  containing region_dictionary
                    indicating 'un_stats' (1)
                  containing region_identifier
                    indicating ID_REGION_AA_UNSTATS
                  containing local_region
                    indicating 0
                }
              }
            }
        }
      }
    }
  }
} then {
  the IUT accepts the message
}
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_09_04_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the IUT discards a message when signing certificate does not contain a region validity restriction but the issuing certificate contains the identified region validity restriction</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 4.2.26 and 7.4</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION</td>
</tr>
</tbody>
</table>

### Expected behaviour

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

ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
          indicating 'certificate'
          containing certificate (CERT_TS_09_04_BO_AT) {
            not containing validity_restrictions['region']
          }
          containing signer_info.digest
          referencing to a CERT_TS_E_AA
        }
      }
    }
  }
  then {
    the IUT discards the message
  }
}
### TP Id

TP_SEC_ITSS_RCV_CERT_09_05_BO

### Summary

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

### Reference

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

### PICS Selection

PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION

### Expected behaviour

with {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
          indicating 'certificate'
          containing certificate (CERT_TS_09_05_BO_AT) {
            containing validity_restrictions['region'] {
              indicating 'id'
              containing id_region {
                containing region_dictionary indicating 'iso_3166_1' (0)
                containing region_identifier indicating ID_REGION_AT
                containing local_region
                indicating 0
              }
            }
            containing signer_info.digest
            referencing to a CERT_TS_09_05_BO_AA
            containing validity_restrictions['region'] {
              indicating 'id'
              containing id_region {
                containing region_dictionary indicating 'iso_3166_1' (0)
                containing region_identifier indicating ID_REGION_AA_OTHER
                containing local_region
                indicating 0
              }
            }
          }
        }
      }
    }
  }
} then {
  the IUT discards the message
}
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_09_06_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Summary</strong></td>
<td>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</td>
</tr>
<tr>
<td><strong>Reference</strong></td>
<td>ETSI TS 103 097 [1], clauses 4.2.26 and 7.4</td>
</tr>
<tr>
<td><strong>PICS Selection</strong></td>
<td>PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION</td>
</tr>
</tbody>
</table>
| **Expected behaviour** | with {
  the IUT being in the 'authorized' state
} ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'] {
        containing signer {
          containing type
            indicating 'certificate'
          containing certificate (CERT_TS_09_06_BO_AT) {
            containing validity_restrictions['region'] {
              containing region_type
                indicating 'id'
              containing id_region {
                containing region_dictionary
                  indicating 'iso_3166_1' (0)
                containing region_identifier
                  indicating ID_REGION_AA
                containing local_region
                  indicating 1
              }
            }
          }
        }
        containing signer_info.digest
          referencing to a CERT_TS_09_06_BO_AA
          containing validity_restrictions['region'] {
            containing region_type
              indicating 'id'
            containing id_region {
              containing region_dictionary
                indicating 'iso_3166_1' (0)
              containing region_identifier
                indicating ID_REGION_AA
              containing local_region
                indicating 2
            }
          }
      }
      } then {
        the IUT discards the message
      }
  } } |
<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_09_07_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the IUT discards a message when the identified region validity restriction of the signing certificate contains unknown area code</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 4.2.26 and 7.4</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY, PICS_USE_IDENTIFIED_REGION</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
| the IUT being in the 'authorized' state |
}

ensure that {
| when {
| the IUT is receiving a SecuredMessage {
| containing header_fields ['signer_info'] {
| containing signer {
| containing type indicating 'certificate' |
| containing certificate (CERT_TS_09_07_BO_AT) {
| containing validity_restrictions['region'] {
| indicating 'id' |
| containing id_region {
| containing region_dictionary indicating 'iso_3166_1' (0) |
| containing region_identifier indicating ID_REGION_UNKNOWN |
| containing local_region indicating 0 |
| }
| }
| containing signer_info.digest referencing to a CERT_TS_09_07_BO_AA |
| containing validity_restrictions['region'] {
| indicating 'id' |
| containing id_region {
| containing region_dictionary indicating 'iso_3166_1' (0) |
| containing region_identifier indicating ID_REGION_UNKNOWN |
| containing local_region indicating 0 |
| }
| }
| }
| }
| then {
| the IUT discards the message |
| }
### 5.3.5.10 Check time validity restriction presence

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_10_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the IUT discards a message when its signing certificate does not contain the time validity restriction</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 7.4 and 7.4.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td>Expected behaviour</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with {</td>
</tr>
<tr>
<td></td>
<td>the IUT being in the 'authorized' state</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>ensure that {</td>
</tr>
<tr>
<td></td>
<td>when {</td>
</tr>
<tr>
<td></td>
<td>the IUT is receiving a SecuredMessage</td>
</tr>
<tr>
<td></td>
<td>containing header_fields ['signer_info'] {</td>
</tr>
<tr>
<td></td>
<td>containing signer {</td>
</tr>
<tr>
<td></td>
<td>containing type indicating 'certificate'</td>
</tr>
<tr>
<td></td>
<td>containing certificate (CERT_TS_10_01_BO_AT) {</td>
</tr>
<tr>
<td></td>
<td>not containing validity_restrictions['time_start_and_end']</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>then {</td>
</tr>
<tr>
<td></td>
<td>the IUT discards the message</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_10_02_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the IUT discards a message when its signing certificate contains 'time_end' validity restriction</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clauses 7.4 and 7.4.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
<tr>
<td>Expected behaviour</td>
<td></td>
</tr>
<tr>
<td></td>
<td>with {</td>
</tr>
<tr>
<td></td>
<td>the IUT being in the 'authorized' state</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>ensure that {</td>
</tr>
<tr>
<td></td>
<td>when {</td>
</tr>
<tr>
<td></td>
<td>the IUT is receiving a SecuredMessage</td>
</tr>
<tr>
<td></td>
<td>containing header_fields ['signer_info'] {</td>
</tr>
<tr>
<td></td>
<td>containing signer {</td>
</tr>
<tr>
<td></td>
<td>containing type indicating 'certificate'</td>
</tr>
<tr>
<td></td>
<td>containing certificate (CERT_TS_10_02_BO_AT) {</td>
</tr>
<tr>
<td></td>
<td>containing validity_restrictions['time_end'] }</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
<tr>
<td></td>
<td>then {</td>
</tr>
<tr>
<td></td>
<td>the IUT discards the message</td>
</tr>
<tr>
<td></td>
<td>}</td>
</tr>
</tbody>
</table>
5.3.5.11 Check time validity restriction conforming to the issuing certificate

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_11_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the IUT discards a message when the validity period of the signing certificate ends after the period of its issuing certificate</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.4</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>
| 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_11_01_BO_AT) { 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 its signing certificate starts before its issuing certificate.

#### Reference
ETSI TS 103 097 [1], clause 7.4

#### PICS Selection
PICS_GN_SECURITY

#### Expected behaviour

<table>
<thead>
<tr>
<th>Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>the IUT being in the 'authorized' state</td>
<td>ensure that</td>
</tr>
<tr>
<td>the IUT is receiving a SecuredMessage</td>
<td>ensure that</td>
</tr>
<tr>
<td>containing header_fields ['signer_info'].signer.certificate (CERT_TS_11_02_BO_AT) 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</td>
<td>when</td>
</tr>
<tr>
<td>containing validity_restrictions['time_start_and_end'] containing start_validity indicating START_VALIDITY_AA - 1d containing end_validity indicating END_VALIDITY_AA</td>
<td>then</td>
</tr>
<tr>
<td>then</td>
<td>the IUT discards the message</td>
</tr>
</tbody>
</table>

### 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.

#### Reference
ETSI TS 103 097 [1], clause 7.4

#### PICS Selection
PICS_GN_SECURITY

#### Expected behaviour

<table>
<thead>
<tr>
<th>Condition</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>the IUT being in the 'authorized' state</td>
<td>ensure that</td>
</tr>
<tr>
<td>the IUT is receiving a SecuredMessage</td>
<td>ensure that</td>
</tr>
<tr>
<td>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 containing end_validity indicating END_VALIDITY_AA</td>
<td>when</td>
</tr>
<tr>
<td>containing validity_restrictions['time_start_and_end'] containing start_validity indicating START_VALIDITY_AA - 1d containing end_validity indicating END_VALIDITY_AA</td>
<td>then</td>
</tr>
<tr>
<td>then</td>
<td>the IUT discards the message</td>
</tr>
<tr>
<td>TP Id</td>
<td>TP_SEC_ITSS_RCV_CERT_11_04_BO</td>
</tr>
<tr>
<td>---------------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>Summary</td>
<td>Check that the IUT discards a message when the validity period of the issuing certificate of signing certificate is not started yet</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.4</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**Expected behaviour**

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a SecuredMessage {
      containing header_fields ['signer_info'].signer.certificate (CERT_TS_11_04_BO_AT)
      containing signer_info.digest
      referencing to CERT_TS_11_04_BO_AA
      containing validity_restrictions['time_start_and_end'] {
        containing start_validity
        indicating END_VALIDITY_AA
        containing end_validity
        indicating END_VALIDITY_AA + 365d
      }
      containing validity_restrictions['time_start_and_end'] {
        containing start_validity
        indicating START_VALIDITY_AA
        containing end_validity
        indicating END_VALIDITY_AA + 365d
      }
    }
  }
  then {
    the IUT discards the message
  }
}

---

5.3.5.12 Check AID subject attribute presence

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_12_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>Check that the IUT discards a message when its signing certificate does not contain the SSP-AID subject attribute</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.4.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

**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_12_01_BO_AT)
          not containing subject_attributes['its_aid_ssp_list']
        }
      }
    }
  }
  then {
    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 7.4.1  
**PICS Selection**  PICS_GN_SECURITY  

**Expected behaviour**  
with {  
  the IUT being in the 'authorized' state  
}  
ensure that {  
  when {  
    the IUT is receiving a Secured CAM {  
      containing header_fields ['its_aid'] {  
        containing its_aid  
        indicating 'AID_CAM' (16512)  
      }  
      containing header_fields ['signer_info'] {  
        containing signer {  
          containing type  
          indicating 'certificate'  
          containing certificate (CERT_TS_12_02_BO_AT) {  
            containing subject_attributes ['its_aid_ssp_list']  
            not containing an item  
            containing its_aid  
            indicating 'AID_CAM' (16512)  
          }  
        }  
      }  
    } then {  
      the IUT discards the message  
    }  
  }  
}  

**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 7.4.1  
**PICS Selection**  PICS_GN_SECURITY  

**Expected behaviour**  
with {  
  the IUT being in the 'authorized' state  
}  
ensure that {  
  when {  
    the IUT is receiving a Secured DENM {  
      containing header_fields ['its_aid'] {  
        containing its_aid  
        indicating 'AID_DENM' (16513)  
      }  
      containing header_fields ['signer_info'] {  
        containing signer {  
          containing type  
          indicating 'certificate'  
          containing certificate (CERT_TS_12_03_BO_AT) {  
            containing subject_attributes ['its_aid_ssp_list']  
            not containing an item  
            containing its_aid  
            indicating 'AID_DENM' (16513)  
          }  
        }  
      }  
    } then {  
      the IUT discards the message  
    }  
  }  
}
5.3.5.13 Check AID-SSP subject attribute value conforming to the issuing certificate

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_13_01_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>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</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.4.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

Expected behaviour

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a Secured CAM {
      containing header_fields ['signer_info'].signer.certificate (CERT_TS_13_01_BO_AT) {
        containing signer_info.digest
        referencing to CERT_TS_13_01_BO_AA
        containing subject_attributes['its_aid_list']
        not containing AID_CAM
        containing subject_attributes['its_aid_ssp_list']
        containing a record
        containing its_aid
        indicating AID_CAM
      }
    }
  } then {
    the IUT discards the message
  }
}

<table>
<thead>
<tr>
<th>TP Id</th>
<th>TP_SEC_ITSS_RCV_CERT_13_02_BO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summary</td>
<td>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 record with AID_DENM</td>
</tr>
<tr>
<td>Reference</td>
<td>ETSI TS 103 097 [1], clause 7.4.1</td>
</tr>
<tr>
<td>PICS Selection</td>
<td>PICS_GN_SECURITY</td>
</tr>
</tbody>
</table>

Expected behaviour

with {
  the IUT being in the 'authorized' state
}
ensure that {
  when {
    the IUT is receiving a Secured DENM {
      containing header_fields ['signer_info'].signer.certificate (CERT_TS_13_02_BO_AT) {
        containing signer_info.digest
        referencing to CERT_TS_13_02_BO_AA
        containing subject_attributes['its_aid_list']
        not containing AID_DENM
        containing subject_attributes['its_aid_ssp_list']
        containing a record
        containing its_aid
        indicating AID_DENM
      }
    }
  } then {
    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

<table>
<thead>
<tr>
<th>Document history</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>V1.1.1</strong></td>
</tr>
<tr>
<td><strong>V1.2.1</strong></td>
</tr>
</tbody>
</table>
