ETSI TS 103 096-2 V1.3.4 (2018-05)

Intelligent Transport Systems (ITS);

Testing;

Conformance test specifications for ITS Security;

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

**Technical Specification**

Reference

RTS/ITS-00543

Keywords

ITS, security, testing, TSS&TP

***ETSI***

650 Route des Lucioles

F-06921 Sophia Antipolis Cedex - FRANCE

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

Siret N° 348 623 562 00017 - NAF 742 C

Association à but non lucratif enregistrée à la

Sous-Préfecture de Grasse (06) N° 7803/88

***Important notice***

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

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

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

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

***Copyright Notification***

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.  
The content of the PDF version shall not be modified without the written authorization of ETSI.  
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2017.

All rights reserved.

**DECT**TM, **PLUGTESTS**TM, **UMTS**TM and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.  
**3GPP**TM and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and  
of the 3GPP Organizational Partners.  
**GSM**® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Intellectual Property Rights 5

Foreword 5

Modal verbs terminology 5

1 Scope 6

2 References 6

2.1 Normative references 6

2.2 Informative references 6

3 Definitions and abbreviations 7

3.1 Definitions 7

3.2 Abbreviations 7

4 Test Suite Structure (TSS) 8

4.1 Structure for Security tests 8

5 Test Purposes (TP) 8

5.1 Introduction 8

5.1.1 TP definition conventions 8

5.1.2 TP Identifier naming conventions 8

5.1.3 Rules for the behaviour description 8

5.1.4 Sources of TP definitions 9

5.1.5 Mnemonics for PICS reference 9

5 ITS-S Security 9

5.1 Overview 9

5.2 Sending behaviour 9

5.2.1 Check the message protocol version 9

5.2.4 CAM profile 10

5.2.4.1 Check that secured CAM is signed 10

5.2.4.2 Check secured CAM AID value 10

5.2.4.3 Check header fields 11

5.2.4.4 Check signer information 11

5.2.4.5 Check that IUT sends certificate to unknown ITS-S 13

5.2.4.6 Check that IUT restarts the timer when the certificate has been sent 14

5.2.4.7 Check sending certificate request for unknown certificate 14

5.2.4.8 Check that IUT sends AT certificate when requested 16

5.2.4.9 Check that IUT send AA certificate when requested 17

5.2.4.10 Check generation time 21

5.2.4.11 Check payload 21

5.2.4.12 Check signing permissions 22

5.2.4.13 Check signature 22

5.2.4.14 Check certificate consistency conditions 23

5.2.5 DENM profile 25

5.2.5.1 Check secured DENM is signed 25

5.2.5.2 Check secured DENM AID value 25

5.2.5.3 Check header fields 26

5.2.5.4 Check signer information 26

5.2.5.5 Check generation time 27

5.2.5.6 Check generation location 27

5.2.5.7 Check payload 30

5.2.5.8 Check signing permissions 30

5.2.5.9 Check signature 31

5.2.5.10 Check certificate consistency conditions 31

5.2.6 Generic signed message profile 33

5.2.6.1 Check that secured message is signed 33

5.2.6.2 Check secured AID value 33

5.2.6.2 Check header field 34

5.2.6.3 Check that signer info is a certificate or digest 34

5.2.6.4 Check generation time 35

5.2.6.6 Check payload 35

5.2.5.8 Check signing permissions 36

5.2.6.7 Check signature 36

5.2.7 Encrypted messages profile 37

5.2.8 Profiles for certificates 37

5.2.8.1 Check that certificate version is 3 37

5.2.8.2 Check basic certificate conformance to ETSI TS 103 097 37

5.2.8.3 Check the issuer reference of the certificate 38

5.2.8.4 Check rectangular region validity restriction 38

5.2.8.5 Check polygonal region validity restriction 39

5.2.8.6 Check identified region validity restriction 39

5.2.8.7 Check time validity restriction in the chain 41

5.2.8.8 Check ECC point type of the certificate signature 41

5.2.8.9 Check ECC point type of the certificate public keys 42

5.2.8.10 Verify certificate signatures 43

5.2.8.11 Verify certificate permissions 43

5.2.8.12 AT and AA certificate profiles 45

Annex A (informative): Bibliography 46

History 47

# Intellectual Property Rights

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

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

# Foreword

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

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

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

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

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

# Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](https://portal.etsi.org/Services/editHelp!/Howtostart/ETSIDraftingRules.aspx) (Verbal forms for the expression of provisions).

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

# 1 Scope

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

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

# 2 References

## 2.1 Normative references

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

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

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

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

[1] ETSI TS 103 097 (V1.3.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".

[2] IEEE Std 1609.2™-2016: "IEEE Standard for Wireless Access in Vehicular Environments –Security Services for Applications and Management Messages", as amended by IEEE Std 1609.2a™-2017: "Standard for Wireless Access In Vehicular Environments – Security Services for Applications and Management Messages Amendment 1".

[3] ETSI TS 103 096-1 (V1.4.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)".

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

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

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

## 2.2 Informative references

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

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

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

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

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

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

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

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

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

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

# 3 Definitions and abbreviations

## 3.1 Definitions

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

## 3.2 Abbreviations

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

AA Authorization Authority

AID Application Identifier

AID\_CAM ITS Application Identifier for CAM

AID\_DENM Application Identifier for DENM

AID\_GN Application Identifier for general GeoNetworking messages

AT Authorization Ticket

ATS Abstract Test Suite

BO Exceptional Behaviour

BV Valid Behaviour

CAM Co-operative Awareness Messages

CAN Controller Area Network

CERT Certificate

DE Data Element

DENM Decentralized Environmental Notification Message

EA Enrolment Authority

ECC Elliptic Curve Cryptography

GN GeoNetworking

ITS Intelligent Transportation Systems

ITS-S Intelligent Transport System - Station

IUT Implementation under Test

MSG Message

PICS Protocol Implementation Conformance Statement

SSP Service Specific Permissions

TP Test Purposes

TSS Test Suite Structure

# 4 Test Suite Structure (TSS)

## 4.1 Structure for Security tests

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

Table 1: TSS for Security

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

# 5 Test Purposes (TP)

## 5.1 Introduction

### 5.1.1 TP definition conventions

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

### 5.1.2 TP Identifier naming conventions

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

Table 2: TP naming convention

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

### 5.1.3 Rules for the behaviour description

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

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

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

### 5.1.4 Sources of TP definitions

All TPs have been specified according to ETSI TS 103 097 [1] and IEEE 1609.2™[2]

### 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' as defined in IEEE Std 1609.2 [2], ETSI TS 103 096-1 [3] and ETSI TS 102 871‑1 [4] shall be used to determine the test applicability.

Table 3: Mnemonics for PICS reference

|  |  |  |
| --- | --- | --- |
|  | Mnemonic | PICS item |
| 1 | PICS\_GN\_SECURITY | A.2/1 [4] |
| 2 | PICS\_SEC\_CERTIFICATE\_SELECTION | A.8/1 [3] |
| 3 | PICS\_SEC\_CIRCULAR\_REGION | S1.2.2.5.1.1 [2] |
| 4 | PICS\_SEC\_RECTANGULAR\_REGION | S1.2.2.5.1.2 [2] |
| 5 | PICS\_SEC\_POLYGONAL\_REGION | S1.2.2.5.1.3 [2] |
| 6 | PICS\_SEC\_IDENTIFIED\_REGION | S1.2.2.5.1.4 [2] |
| 7 | PICS\_SEC\_ITS\_AID\_OTHER | A.7/1 [3] |
| 8 | PICS\_SEC\_SHA256 | S1.2.2.1.1 [2] |
| 9 | PICS\_SEC\_SHA384 | S1.2.2.1.2 [2] |
| 10 | PICS\_SEC\_BRAINPOOL\_P256R1 | S1.2.2.4.1.2 [2] |
| 11 | PICS\_SEC\_BRAINPOOL\_P384R1 | S1.2.2.4.2 [2] |

# 5 ITS-S Security

## 5.1 Overview

Void.

## 5.2 Sending behaviour

### 5.2.1 Check the message protocol version

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_MSG\_01\_BV |
| **Summary** | Check that the IUT sends a secured message containing protocol version set to 3 |
| **Reference** | ETSI TS 103 097 [1], clause 5.1 IEEE1609.2[2], clause 6.3.2 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| **Expected behaviour** | |
| with     the IUT being in the 'authorized' state ensure that     when         the IUT is requested to send a secured message     then         the IUT sends a EtsiTs103097Data             containing protocolVersion                  indicating value '3' | |

### 5.2.4 CAM profile

#### 5.2.4.1 Check that secured CAM is signed

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_01\_BV |
| **Summary** | Check that IUT sends the secured CAM using SignedData container |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.1 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send a secured CAM     then         the IUT sends a message of type EtsiTs103097Data  containing content               containing signedData | |

#### 5.2.4.2 Check secured CAM AID value

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_02\_BV |
| **Summary** | Check that IUT sends the secured CAM containing the HeaderInfo field psid set to 'AID\_CAM' |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.1 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send a secured CAM     then         the IUT sends a message of type EtsiTs103097Data  containing content              containing signedData              containing tbsData              containing headerInfo                   containing psid                      indicating 'AID\_CAM' | |

#### 5.2.4.3 Check header fields

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_03\_BV |
| **Summary** | Check that IUT sends the secured CAM with the HeaderInfo containing generationTime and doesn’t containing expiryTime, generationLocation, encryptionKey, p2pcdLearningRequest, missingCrlIdentifier. |
| **Reference** | ETSI TS 103 097 [1], clauses 5.2, 7.1.1 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send a secured CAM     then         the IUT sends a message of type EtsiTs103097Data  containing content              containing signedData              containing tbsData              containing headerInfo              containing generationTime               and not containing expiryTime  and not containing generationLocation,           and not containing encryptionKey  and not containing p2pcdLearningRequest  and not containing missingCrlIdentifier | |

#### 5.2.4.4 Check signer information

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_04\_BV |
| **Summary** | Check that IUT sends the secured CAM containing signer containing either certificate or digest;  Check that signing certificate has permissions to sign CAM messages |
| **Reference** | ETSI TS 103 097 [1], clauses 5.2, 7.1.1  IEEE 1609.2 [2], clause 6.3.4 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send a secured CAM      then  the IUT sends a message of type EtsiTs103097Data  containing content              containing signedData              containing signer                containing digest                or containing certificate  containing toBeSigned  containing appPermissions  containing the item of type PsidSsp  containing psid  indicating AID\_CAM | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TP Id** | | TP\_SEC\_ITSS\_SND\_CAM\_05\_BV | | |
| **Summary** | | Check that IUT calculate the digest of certificate using proper hash algorithm;  Check that IUT canonicalize certificates before hash calculation | | |
| **Reference** | | ETSI TS 103 097 [1], clauses 5.2, 7.1.1  IEEE 1609.2 [2], clause 6.3.4 | | |
| **PICS Selection** | | PICS\_GN\_SECURITY AND ***X\_PICS*** | | |
| Expected behaviour | | | | |
| with     the IUT is authorized with AT certificate (***X\_CERTIFICATE***)      and the IUT is configured to send more than one CAM per second     and the IUT having sent a secured CAM  containing signer  containing certificate  indicating ***X\_CERTIFICATE***  containing verifyKeyIndicator  containing verificationKey  containing ***X\_KEY***  ensure that     when         the IUT is requested to send a subsequent secured CAM  containing signer  containing digest      then  the IUT sends a message of type EtsiTs103097Data  containing content              containing signedData              containing signer                containing digest  indicating last 8 bytes of the Hash value calculated using ***X\_HASH*** algorithm | | | | |
| **Permutation table** | | | | |
| **XX** | ***X\_CERTIFICATE*** | ***X\_KEY*** | ***X\_HASH*** | ***X\_PICS*** |
| A | CERT\_IUT\_A\_AT | ecdsaNistP256 | SHA-256 |  |
| AN | CERT\_IUT\_A\_N\_AT | ecdsaNistP256 | SHA-256 |  |
| B | CERT\_IUT\_A\_B\_AT | ecdsaBrainpoolP256r1 | SHA-256 | PICS\_SEC\_BRAINPOOL\_P256R1 |
| BN | CERT\_IUT\_A\_B\_N\_AT | ecdsaBrainpoolP256r1 | SHA-256 | PICS\_SEC\_BRAINPOOL\_P256R1 |
| C | CERT\_IUT\_A\_B3\_AT | ecdsaBrainpoolP384r1 | SHA-384 | PICS\_SEC\_SHA384 AND PICS\_SEC\_BRAINPOOL\_P384R1 |
| CN | CERT\_IUT\_A\_B3\_N\_AT | ecdsaBrainpoolP384r1 | SHA-384 | PICS\_SEC\_SHA384 AND PICS\_SEC\_BRAINPOOL\_P384R1 |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_06\_BV |
| **Summary** | Check that IUT sends the secured CAM containing the signing certificate when over the time of one second no other secured CAM contained the certificate was sent |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.1 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)      and the IUT is configured to send more than one CAM per second     and the IUT having sent a secured CAM  containing generationTime  indicating TIME\_LAST  ensure that     when         the IUT is sending secured CAM as a message of type EtsiTs103097Data          containing signer             containing certificate      then         this message is        containing headerInfo  containing generationTime            indicating TIME (TIME >= TIME\_LAST + 1sec) | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_07\_BV |
| **Summary** | Check that IUT sends the secured CAM containing the signing certificate when the timeout of one second has been expired after the previous CAM containing the certificate |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.1 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)      and the IUT is configured to send more than one CAM per second     and the IUT having sent a secured CAM  containing signer  containing certificate      and containing generationTime             indicating TIME\_LAST ensure that     when         the IUT is sending a secured CAM as a message of type EtsiTs103097Data    containing generationTime       indicating TIME >= TIME\_LAST + 1sec      then         this message is      containing certificate | |

#### 5.2.4.5 Check that IUT sends certificate to unknown ITS-S

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_08\_BV |
| **Summary** | Check that IUT sends the secured CAM containing the signing certificate when the IUT received a CAM from an unknown ITS-S |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.1 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)      and the IUT is configured to send more than one CAM per second     and the IUT having already sent secured CAM  containing certificate  at TIME\_1      and the IUT having received a message of type EtsiTs103097Data         containing signedData      containing signer  containing digest  indicating HashedId8 value                  referencing an unknown certificate (CERT\_TS\_B\_AT)          at TIME\_2 (TIME\_1 < TIME\_2 < TIME\_1+1sec) ensure that     when         the IUT is requested to send secured CAM                     at TIME\_3 (TIME\_1 < TIME\_2 < TIME\_3 < TIME\_1 + 1sec)     then          the IUT sends a message of type EtsiTs103097Data             containing signedData              containing signer                      containing certificate | |

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

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_09\_TI |
| **Summary** | Check that IUT restarts the certificate sending timer when the signing certificate was sent |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.1 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)      and the IUT is configured to send more than one CAM per second     and the IUT having already sent secured CAM         containing signer              containing certificate  at TIME\_1      and the IUT having received a secured CAM         containing signer              containing digest               indicating HashID8 value              referencing an unknown certificate         at TIME\_2 (TIME\_1 + 0.3sec)     and the IUT having sent secured CAM          containing signer              containing certificate  at TIME\_3 (TIME\_3 > TIME\_2)  ensure that     when         the IUT is sending the next secured CAM      containing signedData          containing signer                   containing certificate  at TIME\_4      then         the difference between TIME\_4 and TIME\_3 is about 1sec | |

#### 5.2.4.7 Check sending certificate request for unknown certificate

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_10\_BV |
| **Summary** | Check that the IUT sends certificate request when it receives secured CAM containing digest of unknown certificate as a message signer |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.1  IEEE 1609.2 [2], clauses 6.3.9, 8.2.4.1.2 |
| **PICS Selection** | PICS\_GN\_SECURITY, PICS\_SEC\_P2P\_AT\_DISTRIBUTION |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)      and the IUT has receiving a EtsiTs103097Data      containing signer           containing digest               indicating HashedId8 value DIGEST\_A                  referencing an unknown certificate (CERT\_TS\_B\_AT) ensure that     when         the IUT is requested to send a secured CAM     then         the IUT sends a message of type EtsiTs103097Data          containing headerInfo  containing inlineP2pcdRequest           containing HashedId3 value                 indicating last 3 octets of DIGEST\_A | |

|  |  |  |  |
| --- | --- | --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_11\_BV***\_XX*** | | |
| **Summary** | Check that the IUT sends certificate request when it receives secured CAM containing certificate signed by unknown AA certificate | | |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.1  IEEE 1609.2 [2], clauses 6.3.9, 8.2.4.1.2 | | |
| **PICS Selection** | PICS\_GN\_SECURITY  AND PICS\_SEC\_P2P\_AA\_DISTRIBUTION  AND ***X\_PICS*** | | |
| Expected behaviour | | | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)      and the IUT has receiving a message of type EtsiTs103097Data         containing signer              containing certificate               containing issuer  containing ***X\_FIELD\_1***                  indicating HashedId8 value DIGEST                  referencing an unknown certificate ensure that     when         the IUT is requested to send secured CAM     then         the IUT sends a message of type EtsiTs103097Data             containing signedData              containing tbsData              containing headerInfo  containing inlineP2pcdRequest                      containing HashedId3 value                          indicating last 3 octets of DIGEST | | | |
| **Permutation table** | | | |
| **XX** | | **X\_FIELD\_1** | **X\_PICS** |
| A | | sha256AndDigest |  |
| B | | sha384AndDigest | PICS\_SEC\_SHA384 |

#### 5.2.4.8 Check that IUT sends AT certificate when requested

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_12\_BV |
| **Summary** | Check that IUT sends the secured CAM containing the signing certificate when it received a CAM containing a request for unrecognized certificate that matches with the currently used AT certificate ID of the IUT |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.1  IEEE 1609.2 [2], clauses 6.3.9, 8.2.4.2.3 |
| **PICS Selection** | PICS\_GN\_SECURITY  AND PICS\_SEC\_P2P\_AT\_DISTRIBUTION |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)      and the IUT is configured to send more than one CAM per second     and the IUT having already sent secured CAM          containing signer              containing certificate  at TIME\_1      and the IUT having received a secured CAM          containing headerInfo  containing inlineP2pcdRequest          containing HashedId3 value              indicating last 3 octets of currently used AT 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 of type EtsiTs103097Data             containing signer                 and containing certificate                     referenced by the requested digest | |

#### 5.2.4.9 Check that IUT send AA certificate when requested

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_13\_BV |
| **Summary** | Check that IUT sends the secured CAM containing the AA certificate in the requestedCertificate headerInfo field when it received a CAM containing a request for unrecognized certificate that matches with the currently used AA certificate ID of the IUT |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.1  IEEE 1609.2 [2], clauses 6.3.9, 8.2.4.2.3 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_P2P\_AT\_DISTRIBUTION |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  issued by the AA certificate (CERT\_IUT\_A\_AA)     and the IUT is configured to send more than one CAM per second     and the IUT having already sent a secured CAM          containing signer              containing certificate  at TIME\_1      and the IUT having received a secured CAM  containing headerInfo  containing inlineP2pcdRequest       containing HashedId3 value      indicating last 3 octets of the digest of CERT\_IUT\_A\_AA  at TIME\_2 (TIME\_1 < TIME\_2 < TIME\_1+1sec)  ensure that     when         the IUT is requested to send a secured CAM             at TIME\_3 (TIME\_1 < TIME\_2 < TIME\_3 < TIME\_1+1sec)     then         the IUT sends a SecuredMessage of type EtsiTs103097Data          containing headerInfo       containing requestedCertificate  indicating requested AA certificate CERT\_IUT\_A\_AA | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_14\_BV |
| **Summary** | Check that IUT sends the secured CAM containing the AA certificate in the requestedCertificate headerInfo field when it received a CAM containing a request for unrecognized certificate that matches with the known AA certificate ID which is not currently used by the IUT |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.1  IEEE 1609.2 [2], clauses 6.3.9, 8.2.4.2.3 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_P2P\_AA\_DISTRIBUTION |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)      and the IUT is configured to send more than one CAM per second      and the IUT is configured to know the AA certificate (CERT\_TS\_B\_AA)      and the IUT has already sent secured CAM          containing signer                  containing certificate  at TIME\_1      and the IUT having received a secured CAM         containing headerInfo  containing inlineP2pcdRequest           containing HashedId3 value           indicating last 3 octets of the digest of CERT\_TS\_B\_AA  which is not an issuer of currently used AT certificate  at TIME\_2 (TIME\_1 < TIME\_2 < TIME\_1+1sec)  ensure that     when         the IUT is requested to send a secured CAM             at TIME\_3 (TIME\_1 < TIME\_2 < TIME\_3 < TIME\_1+1sec)     then         the IUT sends a SecuredMessage of type EtsiTs103097Data  containing headerInfo       containing requestedCertificate  indicating requested AA certificate (CERT\_TS\_B\_AA) | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_15\_BV |
| **Summary** | Check that the IUT doesn't send a secured CAM containing the AA certificate in the requestedCertificate headerInfo field when it was previously requested and already received from another ITS-S |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.1  IEEE 1609.2 [2], clauses 6.3.9, 8.2.4.2.3 |
| **PICS Selection** | PICS\_GN\_SECURITY, PICS\_SEC\_P2P\_AA\_DISTRIBUTION |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)   issued by the AA certificate (CERT\_IUT\_A\_AA)     and the IUT is configured to send more than one CAM per second     and the IUT having already sent secured CAM          containing signer              containing certificate  at TIME\_1      and the IUT having received a secured CAM       containing headerInfo  containing inlineP2pcdRequest     containing HashedId3 value       indicating last 3 octets of the digest of CERT\_IUT\_A\_AA      at TIME\_2 (TIME\_1 < TIME\_2 < TIME\_1+0.8sec)      and the IUT having received a secured CAM          containing headerInfo       containing requestedCertificate  indicating requested AA certificate (CERT\_IUT\_A\_AA)  at TIME\_3 (TIME\_2 < TIME\_3 < TIME\_2+0.1sec)  ensure that      when         the IUT is requested to send a secured CAM             at TIME\_4 (TIME\_3 < TIME\_4 < TIME\_1+0.9sec)     then         the IUT sends a SecuredMessage of type EtsiTs103097Data          containing headerInfo       does not containing requestedCertificate | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_16\_BV |
| **Summary** | Check that the IUT doesn't send a secured CAM containing the AA certificate in the requestedCertificate headerInfo field when it contains certificate in the signer field |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.1  IEEE 1609.2 [2], clauses 6.3.9, 8.2.4.2.3 |
| **PICS Selection** | PICS\_GN\_SECURITY, PICS\_SEC\_P2P\_AA\_DISTRIBUTION |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)   issued by the AA certificate (CERT\_IUT\_A\_AA)     and the IUT is configured to send more than one CAM per second     and the IUT having already sent a secured CAM          containing signer              containing certificate  at TIME\_1      and the IUT having received a SecuredMessage   containing headerInfo  containing inlineP2pcdRequest           containing HashedId3 value       indicating last 3 octets of the digest of CERT\_IUT\_A\_AA  at TIME\_2 (TIME2 = TIME\_1+0.9sec)  ensure that      when         the IUT is requested to send a secured CAM             at TIME\_3 (TIME\_2 < TIME\_3 < TIME\_1+1sec)     then         the IUT sends a SecuredMessage of type EtsiTs103097Data          containing signer              containing certificate          and containing headerInfo           does not containing requestedCertificate | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_17\_BV |
| **Summary** | Check that the IUT send a secured CAM containing the AA certificate in the requestedCertificate headerInfo field with the next CAM containing digest as a signer info |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.1  IEEE 1609.2 [2], clauses 6.3.9, 8.2.4.2.3 |
| **PICS Selection** | PICS\_GN\_SECURITY, PICS\_SEC\_P2P\_AA\_DISTRIBUTION |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)   issued by the AA certificate (CERT\_IUT\_A\_AA)     and the IUT is configured to send more than one CAM per second     and the IUT having already sent secured CAM          containing signer              containing certificate  at TIME\_1      and the IUT having received a SecuredMessage of type EtsiTs103097Data         containing headerInfo  containing inlineP2pcdRequest                  containing HashedId3 value       indicating last 3 octets of the digest of CERT\_IUT\_A\_AA  at TIME\_2 (TIME\_1+0.9sec < TIME2 < TIME\_1+1sec)  ensure that      when         the IUT is sending a first subsequent secured CAM          containing signer              containing digest      then         this message          containing headerInfo       containing requestedCertificate  indicating requested AA certificate CERT\_IUT\_A\_AA | |

#### 5.2.4.10 Check generation time

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_18\_BV |
| **Summary** | Check that IUT sends the secured CAM containing generation time and this time is inside the validity period of the signing certificate;  Check that message generation time value is realistic |
| **Reference** | ETSI TS 103 097 [1], clauses 7.1.1  IEEE 1609.2 [2], clauses 5.2.3.2.2, 5.2.4.2.2, 5.2.4.2.3 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send CAM              containing certificate     then         the IUT sends a SecuredMessage of type EtsiTs103097Data  containing headerInfo               containing generationTime           indicating GEN\_TIME (CUR\_TIME - 5min <= GEN\_TIME <= CUR\_TIME + 5min)          and containing signer                  containing certificate                  containing toBeSigned                       containing validityPeriod  containing start                           indicating value X\_START\_VALIDITY (X\_START\_VALIDITY <= GEN\_TIME)                              and containing duration                                 indicating value > GEN\_TIME - X\_START\_VALIDITY | |

#### 5.2.4.11 Check payload

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_19\_BV |
| **Summary** | Check that IUT sends the secured CAM containing the 'data' field in signed data payload, containing the EtsiTs103097Data of type unsecured, contained the CAM payload |
| **Reference** | ETSI TS 103 097 [1], clauses 5.2, 7.1.1 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send a secured CAM     then         the IUT sends a message of type EtsiTs103097Data          contains content          contains signedData              containing tbsData               containing payload               containing data               containing content               containing unsecuredData                   containing not-empty data | |

#### 5.2.4.12 Check signing permissions

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_20\_BV |
| **Summary** | Check that the IUT sends the secured CAM signed with the certificate containing appPermisions allowing to sign CA messages |
| **Reference** | ETSI TS 103 097 [1], clauses 7.2.1  IEEE 1609.2 [2], clauses 5.2.3.2.2 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send a secured CAM     then         the IUT sends a message of type EtsiTs103097Data         containing signer               containing certificate               containing appPermissions               containing an item of type PsidSsp                   containing psid = AID\_CAM | |

#### 5.2.4.13 Check signature

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TP Id** | | TP\_SEC\_ITSS\_SND\_CAM\_21\_BV\_***XX*** | | | |
| **Summary** | | Check that IUT sends the secured CAM containing signature;  check that the signature is calculated over the right fields and using right hash algorythm by cryptographically verifying the signature | | | |
| **Reference** | | ETSI TS 103 097 [1], clauses 5.2, 7.1.1  IEEE 1609.2 [2], clauses 5.3.1, 6.3.4, 6.3.29, 6.3.30, 6.3.31 | | | |
| **PICS Selection** | | PICS\_GN\_SECURITY AND ***X\_PICS*** | | | |
| Expected behaviour | | | | | |
| with     the IUT is authorized with AT certificate (***X\_CERTIFICATE***)   containing verifyKeyIndicator  containing verificationKey  containing ***X\_KEY***  indicating KEY  ensure that     when         the IUT is requested to send a secured CAM     then         the IUT sends a message of type EtsiTs103097Data          containing signedData          containing signer  containing digest                    referencing the certificate ***X\_CERTIFICATE***                  or containing certificate  indicating ***X\_CERTIFICATE***               and containing signature               containing ***X\_SIGNATURE***                  verifiable using KEY | | | | | |
| **Permutation table** | | | | | |
| **XX** | ***X\_CERTIFICATE*** | | ***X\_KEY*** | ***X\_SIGNATURE*** | ***X\_PICS*** |
| A | CERT\_IUT\_A\_AT | | ecdsaNistP256 | ecdsaNistP256Signature |  |
| B | CERT\_IUT\_A\_B\_AT | | ecdsaBrainpoolP256r1 | ecdsaBrainpoolP256r1Signature | PICS\_SEC\_BRAINPOOL\_P256R1 |
| C | CERT\_IUT\_A\_B3\_AT | | ecdsaBrainpoolP384r1 | ecdsaBrainpoolP384r1Signature | PICS\_SEC\_SHA384 AND PICS\_SEC\_BRAINPOOL\_P384R1 |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_22\_BV |
| **Summary** | Check that IUT sends the secured CAM containing signature containing the ECC point of type set to either compressed\_lsb\_y\_0, compressed\_lsb\_y\_1 or x\_coordinate\_only |
| **Reference** | ETSI TS 103 097 [1], clauses 5.2, 7.1.1  IEEE 1609.2 [2], clauses 6.3.30, 6.3.31 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send a secured CAM     then         the IUT sends a message of type EtsiTs103097Data          containing signedData               containing signature  containing one of the ecdsaNistP256Signature  or containing ecdsaBrainpoolP256r1Signature  or containing ecdsaBrainpoolP384r1Signature  containing rSig  containing x-only  or containing compressed-y-0  or containing compressed-y-1 | |

#### 5.2.4.14 Check certificate consistency conditions

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_23\_BV |
| **Summary** | Check that IUT doesn’t send secured CAMs if IUT is authorized with AT certificate doesn’t allowing sending messages in this location |
| **Reference** | IEEE 1609.2 [2], clauses 5.2.3.2.2 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_C1\_AT)   containing region  indicating rectangular region  not containing current IUT position  and the IUT has no other installed AT certificates  ensure that     when         the IUT is requested to send a secured CAM     then         the IUT doesn’t send CAM | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_24\_BV |
| **Summary** | Check that IUT doesn’t send the secured CAM if IUT is configured to use an AT certificate without region validity restriction and generation location is outside of the region of the issuing AA certificate |
| **Reference** | IEEE 1609.2 [2], clauses 5.2.3.2.2 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT has been authorized with the AT certificate (CERT\_IUT\_CA3\_AT)  not containing region  and issued by the AA certificate (CERT\_IUT\_C3\_AA)  containing region  indicating rectangular region  not containing current IUT position  ensure that     when         the IUT is requested to send a secured CAM     then         the IUT doesn’t send CAM | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_25\_BV |
| **Summary** | Check that IUT doesn’t send secured CAMs if all AT certificates installed on the IUT was expired. |
| **Reference** | IEEE 1609.2 [2], clauses 5.2.3.2.2 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A1\_AT)   containing validityPeriod  indicating start + duration < CURRENT\_TIME  and the IUT has no other installed AT certificates  ensure that     when         the IUT is requested to send a secured CAM     then         the IUT doesn’t send CAM | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_26\_BV |
| **Summary** | Check that IUT doesn’t send secured CAMs if all AT certificates installed on the IUT have the starting time in the future. |
| **Reference** | IEEE 1609.2 [2], clauses 5.2.3.2.2 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A2\_AT)   containing validityPeriod  indicating start > CURRENT\_TIME  and the IUT has no other installed AT certificates  ensure that     when         the IUT is requested to send a secured CAM     then         the IUT doesn’t send CAM | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CAM\_27\_BV |
| **Summary** | Check that IUT doesn’t send secured CAMs if IUT doesn’t possess an AT certificate allowing sending CAM by its appPermissions |
| **Reference** | IEEE 1609.2 [2], clauses 5.2.3.2.2 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A3\_AT)   containing appPermissions  not containing PsidSSP  containing psid  indicating AID\_CAM  and the IUT has no other installed AT certificates  ensure that     when         the IUT is requested to send a secured CAM     then         the IUT doesn’t send CAM | |

### 5.2.5 DENM profile

#### 5.2.5.1 Check secured DENM is signed

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_DENM\_01\_BV |
| **Summary** | Check that IUT sends the secured DENM using SignedData container |
| **Reference** | ETSI TS 103 097 [1], clauses 7.1.2 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send a secured DENM     then         the IUT sends a EtsiTs103097Data  containing content               containing signedData | |

#### 5.2.5.2 Check secured DENM AID value

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_DENM\_02\_BV |
| **Summary** | Check that IUT sends the secured DENM containing the HeaderInfo field psid set to 'AID\_DENM' |
| **Reference** | ETSI TS 103 097 [1], clauses 7.1.2 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send a secured DENM     then         the IUT sends a EtsiTs103097Data  containing content              containing signedData              containing tbsData              containing headerInfo                   containing psid                      indicating 'AID\_DENM' | |

#### 5.2.5.3 Check header fields

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_DENM\_03\_BV |
| **Summary** | Check that IUT sends the secured DENM with the HeaderInfo containing generationTime and generationLocation and doesn’t containing expiryTime, encryptionKey, p2pcdLearningRequest, missingCrlIdentifier, inlineP2pcdRequest, requestedCertificate. |
| **Reference** | ETSI TS 103 097 [1], clause 5.2, 7.1.2 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send a secured DENM     then         the IUT sends a EtsiTs103097Data  containing content              containing signedData              containing tbsData              containing headerInfo              containing generationTime  and containing generationLocation,               and not containing expiryTime           and not containing encryptionKey  and not containing p2pcdLearningRequest  and not containing missingCrlIdentifier  and not containing inlineP2pcdRequest  and not containing requestedCertificate | |

#### 5.2.5.4 Check signer information

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_DENM\_04\_BV |
| **Summary** | Check that IUT sends the secured DENM containing signer containing certificate |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.2  IEEE 1609.2 [2], clause 6.3.4 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send a secured DENM     then  the IUT sends a EtsiTs103097Data  containing content              containing signedData              containing signer                containing certificate  containing toBeSigned  containing appPermissions  containing the item of type PsidSsp  containing psid  indicating AID\_DENM | |

#### 5.2.5.5 Check generation time

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_DENM\_05\_BV |
| **Summary** | Check that IUT sends the secured DENM containing generation time and this time is inside the validity period of the signing certificate;  Check that message generation time value is realistic |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.2  IEEE 1609.2 [2], clauses 5.2.3.2.2, 5.2.4.2.2, 5.2.4.2.3 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send a secured DENM     then          the IUT sends a message of type EtsiTs103097Data  containing headerInfo               containing generationTime           indicating GEN\_TIME (CUR\_TIME - 10min <= GEN\_TIME <= CUR\_TIME + 10min)          and containing signer                  containing certificate                  containing toBeSigned                       containing validityPeriod  containing start                           indicating value X\_START\_VALIDITY (X\_START\_VALIDITY <= GEN\_TIME)                              and containing duration                                 indicating value > GEN\_TIME - X\_START\_VALIDITY | |

#### 5.2.5.6 Check generation location

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_DENM\_06\_BV |
| **Summary** | Check that IUT sends the secured DENM containing generation location when signing certificate chain doesn’t have any region restriction |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.2  IEEE 1609.2 [2], clause 5.2.3.2.2 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_CERTIFICATE\_SELECTION |
| Expected behaviour | |
| with     the IUT has been authorized with the AT certificate (CERT\_IUT\_A\_AT)  containing toBeSigned  not containing region  and issuied by the certificate AA (CERT\_IUT\_A\_AA)  containing toBeSigned  not containing region  and issuied by the certificate RCA (CERT\_IUT\_A\_RCA)  containing toBeSigned  not containing region ensure that     when         the IUT is requested to send a secured DENM     then         the IUT sends a message of type EtsiTs103097Data  containing headerInfo               containing generationLocation | |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TP Id** | | TP\_SEC\_ITSS\_SND\_DENM\_07\_BV***\_XX*** | | |
| **Summary** | | Check that IUT sends the secured DENM containing generation location which is inside the circular region defined by the validity restriction of the certificate pointed by the message signer | | |
| **Reference** | | ETSI TS 103 097 [1], clause 7.1.2  IEEE 1609.2 [2], clause 5.2.3.2.2 | | |
| **PICS Selection** | | PICS\_GN\_SECURITY AND PICS\_SEC\_CERTIFICATE\_SELECTION AND ***X\_PICS*** | | |
| Expected behaviour | | | | |
| with     the IUT has been authorized with the AT certificate (***X\_AT\_CERTIFICATE***)  containing toBeSigned  containing region  containing ***X\_FIELD***  indicating REGION ensure that     when         the IUT is requested to send a secured DENM     then         the IUT sends a message of type EtsiTs103097Data  containing headerInfo               containing generationLocation                      indicating value inside the REGION | | | | |
| **Permutation Table** | | | | |
| ***\_XX*** | ***X\_FIELD*** | | ***X\_AT\_CERTIFICATE*** | ***X\_PICS*** |
| B | circularRegion | | CERT\_IUT\_B\_AT | PICS\_SEC\_CIRCULAR\_REGION |
| C | rectangularRegion | | CERT\_IUT\_C\_AT | PICS\_SEC\_RECTANGULAR\_REGION |
| D | polygonalRegion | | CERT\_IUT\_D\_AT | PICS\_SEC\_POLYGONAL\_REGION |
| E | identifiedRegion | | CERT\_IUT\_E\_AT | PICS\_SEC\_IDENTIFIED\_REGION |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_DENM\_08\_BV |
| **Summary** | Check that IUT sends the secured DENM containing generation location which is inside the region defined by the validity restriction of the certificate pointed by the message signer |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.2  IEEE 1609.2 [2], clause 5.2.3.2.2 |
| **PICS Selection** | PICS\_GN\_SECURITY AND NOT PICS\_SEC\_CERTIFICATE\_SELECTION |
| Expected behaviour | |
| with     the IUT has been authorized with some AT certificate  containing toBeSigned  containing region  ensure that     when         the IUT is requested to send a secured DENM     then         the IUT sends a message of type EtsiTs103097Data  containing headerInfo               containing generationLocation                      indicating value inside the REGION | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_DENM\_09\_BV |
| **Summary** | Check that IUT sends the secured DENM containing generation location which is inside the identified region defined by the validity restriction of the AA certificate used to sign the certificate pointed by the message signer doesn’t containing any region restriction |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.2  IEEE 1609.2 [2], clause 5.2.3.2.2, 6.4.8 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_CERTIFICATE\_SELECTION |
| Expected behaviour | |
| with     the IUT has been authorized with the AT certificate (CERT\_IUT\_CA1\_AT)  containing toBeSigned  not containing region  and issuied by the certificate AA (CERT\_IUT\_CC\_AA)  containing toBeSigned  containing circularRegion  indicating REGION  and issuied by the certificate RCA (CERT\_IUT\_C\_RCA)  containing toBeSigned  containing circularRegion  indicating REGION  ensure that     when         the IUT is requested to send a secured DENM     then         the IUT sends a message of type EtsiTs103097Data  containing headerInfo               containing generationLocation                      indicating value inside the REGION | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_DENM\_10\_BV |
| **Summary** | Check that IUT sends the secured DENM containing generation location which is inside the identified region defined by the validity restriction of the root certificate when subordinate AA and AT certificates don’t contain any region restriction |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.2  IEEE 1609.2 [2], clause 5.2.3.2.2, 6.4.8 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_CERTIFICATE\_SELECTION |
| Expected behaviour | |
| with     the IUT has been authorized with the AT certificate (CERT\_IUT\_CA2\_AT)  containing toBeSigned  not containing region  and issuied by the certificate AA (CERT\_IUT\_CA\_AA)  containing toBeSigned  not containing region  and issuied by the certificate RCA (CERT\_IUT\_C\_RCA)  containing toBeSigned  containing circularRegion  indicating REGION  ensure that     when         the IUT is requested to send a secured DENM     then         the IUT sends a message of type EtsiTs103097Data  containing headerInfo               containing generationLocation                      indicating value inside the REGION | |

#### 5.2.5.7 Check payload

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_DENM\_11\_BV |
| **Summary** | Check that IUT sends the secured DENM containing the 'data' field in signed data payload, containing the EtsiTs103097Data of type unsecured, contained the DENM payload |
| **Reference** | ETSI TS 103 097 [1], clauses 5.2, 7.1.2 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with         the IUT has been authorized with the AT certificate (CERT\_IUT\_A\_AT) ensure that     when         the IUT is requested to send a secured DENM     then         the IUT sends a message of type EtsiTs103097Data          contains content          contains signedData              containing tbsData               containing payload               containing data               containing content               containing unsecuredData                   containing not-empty data | |

#### 5.2.5.8 Check signing permissions

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_DENM\_12\_BV |
| **Summary** | Check that the IUT sends the secured DENM signed with the certificate containing appPermisions allowing to sign DEN messages |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.2  IEEE 1609.2 [2], clauses 5.2.3.2.2 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT has been authorized with the AT certificate (CERT\_IUT\_A\_AT) ensure that     when         the IUT is requested to send a secured DENM     then         the IUT sends a message of type EtsiTs103097Data         containing signer               containing certificate               containing appPermissions               containing an item of type PsidSsp                   containing psid = AID\_DENM | |

#### 5.2.5.9 Check signature

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TP Id** | | TP\_SEC\_ITSS\_SND\_DENM\_13\_BV | | | |
| **Summary** | | Check that IUT sends the secured DENM containing signature; check that the signature is calculated over the right fields and using right hash algorythm by cryptographically verifying the signature | | | |
| **Reference** | | ETSI TS 103 097 [1], clauses 5.2, 7.1.2  IEEE 1609.2 [2], clauses 5.3.1, 6.3.4, 6.3.29, 6.3.30, 6.3.31 | | | |
| **PICS Selection** | | PICS\_GN\_SECURITY AND ***X\_PICS*** | | | |
| Expected behaviour | | | | | |
| with     the IUT is authorized with AT certificate (***X\_CERTIFICATE***)  containing verifyKeyIndicator  containing verificationKey  containing ***X\_KEY***  indicating KEY  ensure that     when         the IUT is requested to send a secured DENM     then         the IUT sends a message of type EtsiTs103097Data          containing signedData          containing signer                  containing certificate  indicating ***X\_CERTIFICATE***  containing verifyKeyIndicator  containing verificationKey  containing ***X\_KEY***  indicating KEY               and containing signature               containing ***X\_SIGNATURE***                  verifiable using KEY | | | | | |
| **Permutation table** | | | | | |
| **XX** | ***X\_CERTIFICATE*** | | ***X\_KEY*** | ***X\_SIGNATURE*** | ***X\_PICS*** |
| A | CERT\_IUT\_A\_AT | | ecdsaNistP256 | ecdsaNistP256Signature |  |
| B | CERT\_IUT\_A\_B\_AT | | ecdsaBrainpoolP256r1 | ecdsaBrainpoolP256r1Signature | PICS\_SEC\_BRAINPOOL\_P256R1 |
| C | CERT\_IUT\_A\_B3\_AT | | ecdsaBrainpoolP384r1 | ecdsaBrainpoolP384r1Signature | PICS\_SEC\_SHA384 AND PICS\_SEC\_BRAINPOOL\_P384R1 |

#### 5.2.5.10 Check certificate consistency conditions

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_DENM\_14\_BV |
| **Summary** | Check that IUT doesn’t send secured DENMs if IUT doesn’t possess an AT certificate allowing sending messages in this location |
| **Reference** | IEEE 1609.2 [2], clauses 5.2.3.2.2 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT has been authorized with the AT certificate (CERT\_IUT\_C1\_AT)  containing region  indicating rectangular region  not containing current IUT position  ensure that     when         the IUT is requested to send a secured DENM     then         the IUT doesn’t send DENM | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_DENM\_15\_BV |
| **Summary** | Check that IUT doesn’t send the secured DENM if IUT is configured to use an AT certificate without region validity restriction and generation location is outside of the region of the issuing AA certificate |
| **Reference** | IEEE 1609.2 [2], clauses 5.2.3.2.2 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT has been authorized with the AT certificate (CERT\_IUT\_CA3\_AT)  not containing region  and issued by the AA certificate (CERT\_IUT\_C3\_AA)  containing region  indicating rectangular region  not containing current IUT position  ensure that     when         the IUT is requested to send a secured DENM     then         the IUT doesn’t send DENM | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_DENM\_16\_BV |
| **Summary** | Check that IUT doesn’t send secured DENMs if all AT certificates installed on the IUT are expired. |
| **Reference** | IEEE 1609.2 [2], clauses 5.2.3.2.2 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A1\_AT)   containing validityPeriod  indicating start + duration < CURRENT\_TIME  and the IUT has no other installed AT certificates  ensure that     when         the IUT is requested to send a secured DENM     then         the IUT doesn’t send DENM | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_DENM\_17\_BV |
| **Summary** | Check that IUT doesn’t send secured DENMs if all AT certificates installed on the IUT have the starting time in the future. |
| **Reference** | IEEE 1609.2 [2], clauses 5.2.3.2.2 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT has been authorized with the AT certificate (CERT\_IUT\_A2\_AT)  containing validityPeriod  indicating start > CURRENT\_TIME  and IUT has no other certificates installed  ensure that     when         the IUT is requested to send a secured DENM     then         the IUT doesn’t send DENM | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_DENM\_18\_BV |
| **Summary** | Check that IUT doesn’t send secured DENMs if IUT doesn’t possess an AT certificate allowing sending DENM by its appPermissions |
| **Reference** | IEEE 1609.2 [2], clauses 5.2.3.2.2 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT has been authorized with the AT certificate (CERT\_IUT\_A4\_AT)  containing appPermissions  not containing PsidSSP  containing psid  indicating AID\_DENM  and IUT has no other certificates installed  ensure that     when         the IUT is requested to send a secured DENM     then         the IUT doesn’t send DENM | |

### 5.2.6 Generic signed message profile

#### 5.2.6.1 Check that secured message is signed

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_GENMSG\_01\_BV |
| **Summary** | Check that IUT sends the secured message using signedData container |
| **Reference** | ETSI TS 103 097 [1], clauses 7.1.3 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_ITS\_AID\_OTHER |
| Expected behaviour | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send a secured Beacon     then         the IUT sends a message of type EtsiTs103097Data  containing content               containing signedData | |

#### 5.2.6.2 Check secured AID value

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_GENMSG\_02\_BV |
| **Summary** | Check that the sent Secured Message contains HeaderField its\_aid that is set to other value then AID\_CAM and AID\_DENM |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.3 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_ITS\_AID\_OTHER |
| Expected behaviour | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send a secured Beacon     then         the IUT sends a message of type EtsiTs103097Data  containing content              containing signedData              containing tbsData              containing headerInfo                   containing psid                      indicating AID\_GNMGMT | |

#### 5.2.6.2 Check header field

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_GENMSG\_03\_BV |
| **Summary** | Check that IUT sends the secured GeoNetworking message with the headerInfo containing generationTime |
| **Reference** | ETSI TS 103 097 [1], clauses 5.2, 7.1.3 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_ITS\_AID\_OTHER |
| Expected behaviour | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send a secured Beacon     then         the IUT sends a message of type EtsiTs103097Data  containing content              containing signedData              containing tbsData              containing headerInfo              containing generationTime  and not containing p2pcdLearningRequest  and not containing missingCrlIdentifier | |

#### 5.2.6.3 Check that signer info is a certificate or digest

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_GENMSG\_04\_BV |
| **Summary** | Check that IUT sends the secured GeoNetworking message containing certificate or digest as a signer |
| **Reference** | ETSI TS 103 097 [1], clauses 5.2, 7.1.3  IEEE 1609.2 [2], clause 6.3.4 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_ITS\_AID\_OTHER |
| Expected behaviour | |
| with     the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send a secured Beacon     then  the IUT sends a message of type EtsiTs103097Data  containing content              containing signedData              containing signer                containing digest                or containing certificate  containing toBeSigned  containing appPermissions  containing the item of type PsidSsp  containing psid  indicating AID\_GNMGMT | |

#### 5.2.6.4 Check generation time

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_GENMSG\_05\_BV |
| **Summary** | Check that IUT sends the secured GeoNetworking message containing generation time and this time is inside the validity period of the signing certificate;  Check that message generation time value is realistic |
| **Reference** | ETSI TS 103 097 [1], clauses 5.4 and 7.1.3 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_ITS\_AID\_OTHER |
| Expected behaviour | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send a secured Beacon             containing certificate     then          the IUT sends a message of type EtsiTs103097Data  containing headerInfo               containing generationTime           indicating GEN\_TIME (CUR\_TIME - 10min <= GEN\_TIME <= CUR\_TIME + 10min)          and containing signer                  containing certificate                  containing toBeSigned                       containing validityPeriod  containing start                           indicating value X\_START\_VALIDITY (X\_START\_VALIDITY <= GEN\_TIME)                              and containing duration                                 indicating value > GEN\_TIME - X\_START\_VALIDITY | |

#### 5.2.6.6 Check payload

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_GENMSG\_06\_BV |
| **Summary** | Check that IUT sends the secured message using the 'data' field in signed data payload, containing the EtsiTs103097Data of type unsecured, containing the data payload or using the extDataHash field containing the SHA256 hash of data payload |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.3 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_ITS\_AID\_OTHER |
| Expected behaviour | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that     when         the IUT is requested to send a secured Beacon     then         the IUT sends a message of type EtsiTs103097Data          contains content          contains signedData              containing tbsData               containing payload               containing data               containing content               containing unsecuredData                   containing not-empty data | |

TODO: add a message for externalPayload.

#### 5.2.5.8 Check signing permissions

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_GENMSG\_07\_BV |
| **Summary** | Check that the IUT sends the secured messages signed with the certificate containing appPermisions allowing to sign these messages |
| **Reference** | ETSI TS 103 097 [1], clause 7.1.3  IEEE 1609.2 [2], clauses 5.2.3.2.2 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_ITS\_AID\_OTHER |
| Expected behaviour | |
| with     the IUT has been authorized with the AT certificate (CERT\_IUT\_A\_AT) ensure that     when         the IUT is requested to send Beacon     then         the IUT sends a message of type EtsiTs103097Data         containing signer               containing certificate               containing appPermissions               containing an item of type PsidSsp                   containing psid = AID\_GNMGMT | |

#### 5.2.6.7 Check signature

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TP Id** | | TP\_SEC\_ITSS\_SND\_GENMSG\_08\_BV | | | |
| **Summary** | | Check that IUT sends the secured GeoNetworking message containing signature;  check that the signature is calculated over the right fields and using right hash algorythm by cryptographically verifying the signature | | | |
| **Reference** | | ETSI TS 103 097 [1], clauses 5.2, 7.1.3  IEEE 1609.2 [2], clauses 5.3.1, 6.3.4, 6.3.29, 6.3.30, 6.3.31 | | | |
| **PICS Selection** | | PICS\_GN\_SECURITY AND PICS\_SEC\_ITS\_AID\_OTHER AND ***X\_PICS*** | | | |
| Expected behaviour | | | | | |
| with     the IUT is authorized with AT certificate (***X\_CERTIFICATE***)   containing verifyKeyIndicator  containing verificationKey  containing ***X\_KEY***  indicating KEY  ensure that     when         the IUT is requested to send a secured Beacon     then         the IUT sends a message of type EtsiTs103097Data          containing signedData          containing signer  containing digest                    referencing the certificate ***X\_CERTIFICATE***                  or containing certificate  indicating ***X\_CERTIFICATE***               and containing signature               containing ***X\_SIGNATURE***                  verifiable using KEY | | | | | |
| **Permutation table** | | | | | |
| **XX** | ***X\_CERTIFICATE*** | | ***X\_KEY*** | ***X\_SIGNATURE*** | ***X\_PICS*** |
| A | CERT\_IUT\_A\_AT | | ecdsaNistP256 | ecdsaNistP256Signature |  |
| B | CERT\_IUT\_A\_B\_AT | | ecdsaBrainpoolP256r1 | ecdsaBrainpoolP256r1Signature | PICS\_SEC\_BRAINPOOL\_P256R1 |
| C | CERT\_IUT\_A\_B3\_AT | | ecdsaBrainpoolP384r1 | ecdsaBrainpoolP384r1Signature | PICS\_SEC\_SHA384 AND PICS\_SEC\_BRAINPOOL\_P384R1 |

### 5.2.7 Encrypted messages profile

#### 5.2.7.1 Check encrypted message generation

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_ENC\_01\_BV |
| **Summary** | Check that the IUT can generate encrypted message |
| **Reference** | ETSI TS 103 097 [1], clauses 5.3 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_ENCRYPTION\_SUPPORT |
| Expected behaviour | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that       when         the IUT is requested to send an encrypted message     then         the IUT sends a message of type EtsiTs103097Data          containing encryptedData | |

#### 5.2.7.2 Check recipient information

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_ENC\_02\_BV |
| **Summary** | Check that the encrypted message contains at least one RecipientInfo |
| **Reference** | IEEE 1609.2 [2], clause 6.3.31 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_ENCRYPTION\_SUPPORT |
| Expected behaviour | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that       when         the IUT is requested to send an encrypted message     then         the IUT sends a message of type EtsiTs103097Data          containing encryptedData  containing recipients  containing at least one item of type RecipientInfo | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TP Id** | | TP\_SEC\_ITSS\_SND\_ENC\_03\_BV\_***XX*** | | | |
| **Summary** | | Check that when the certRecipInfo is used to specify the RecipientInfo then the recipientId contains the HashID8 of the receiver's certificate and the encKey contains encrypted symmetric kay that can be used to decrypt cyphertext | | | |
| **Reference** | | IEEE 1609.2 [2], clauses 5.3.4, 5.3.5, 6.3.31, 6.3.34 | | | |
| **PICS Selection** | | PICS\_GN\_SECURITY AND PICS\_SEC\_ENCRYPTION\_SUPPORT AND ***X\_PICS*** | | | |
| Expected behaviour | | | | | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that       when         the IUT is requested to send an encrypted message  to the receipient authorized with the certificate ***X\_REC\_CERT***  containing encryptionKey  containing publicKey  containing ***X\_REC\_KEY***      then         the IUT sends a message of type EtsiTs103097Data          containing encryptedData  containing recipients  containing an item of type RecipientInfo  containing certRecipInfo  containing recipientId  indicating HashID8 of the certificate ***X\_REC\_CERT***  and containing encKey  containing ***X\_ENC\_KEY***  containing v  indicating sender public key  and containing c  indicating encoded symmetric key ***ENC\_SYM\_KEY***  and containing t  indicating the authentication tag  and containing ciphertext  which can be decrypted using decrypted ***ENC\_SYM\_KEY*** | | | | | |
| **Permutation table** | | | | | |
| **XX** | ***X\_REC\_CERT*** | | ***X\_REC\_KEY*** | ***X\_ENC\_KEY*** | ***X\_PICS*** |
| A | CERT\_TS\_A\_AA | | eciesNistP256 | eciesNistP256 |  |
| B | CERT\_TS\_A\_AA\_B | | eciesBrainpoolP256r1 | eciesBrainpoolP256r1 | PICS\_SEC\_BRAINPOOL\_P256R1 |

#### 5.2.7.3 Check encrypted data content

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_ENC\_04\_BV |
| **Summary** | Check that the ciphertext of encrypted message contains encrypted EtsiTs103097Data structure |
| **Reference** | IEEE 1609.2 [2], clauses 6.3.31  ETSI TS 103 097 [1], clause 7.1.4 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_ENCRYPTION\_SUPPORT |
| Expected behaviour | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that       when         the IUT is requested to send an encrypted message      then         the IUT sends a message of type EtsiTs103097Data          containing encryptedData  containing ciphertext  containing encrypted data  containing COER encoded data  containing structure of type EtsiTs103097Data | |

#### 5.2.7.4 Check encrypted and signed data

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_ENC\_05\_BV |
| **Summary** | Check that when the IUT sends SignedAndEcrypted message then it sends the EtsiTs103097Data-Encrypted message containing the EtsiTs103097Data-Signed structure as the ToBeSignedDataContent |
| **Reference** | IEEE 1609.2 [2], clauses 6.3.31  ETSI TS 103 097 [1], clause 7.1.5 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_ENCRYPTION\_SUPPORT |
| Expected behaviour | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT)  ensure that       when         the IUT is requested to send an encrypted and signed message      then         the IUT sends a message of type EtsiTs103097Data          containing encryptedData  containing ciphertext  containing encrypted data  containing COER encoded data  containing structure of type EtsiTs103097Data  containing signedData | |

### 5.2.8 Profiles for certificates

#### 5.2.8.1 Check that certificate version is 3

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CERT\_01\_BV |
| **Summary** | Check that IUT certificate is explicit and has version 3 |
| **Reference** | ETSI TS 103 097 [1], clauses 6  IEEE 1609.2 [2], clause 6.4.3 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| ensure that       when         the AA is issued the certificate      then      this certificate is of type EtsiTs103097Certificate       containing version       indicating 3          and containing type          indicating ‘explicit’     and containing toBeSigned  containing verifyKeyIndicator  containing verificationKey | |

#### 5.2.8.2 Check basic certificate conformance to ETSI TS 103 097

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CERT\_03\_BV |
| **Summary** | Check that IUT certificate is conformed to ETSI TS 103 097 clause 6. |
| **Reference** | ETSI TS 103 097 [1], clauses 6 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| ensure that      when         the AA is issued the certificate      then      this certificate is of type EtsiTs103097Certificate  containing toBeSigned       containing id  indicating ‘none’  or indicating ‘name’          and containing cracaId  indicating ‘000000'H          and containing crlSeries  indicating ‘0'D          and not containing certRequestPermissions          and not containing canRequestRollover          and containing signature | |

#### 5.2.8.3 Check the issuer reference of the certificate

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TP Id** | | | TP\_SEC\_ITSS\_SND\_CERT\_04\_BV\_***XX*** | | |
| **Summary** | | | Check that the certificate issuer of certificates is referenced using digest;  check that right digest field is used to reference to the certificate | | |
| **Reference** | | | IEEE 1609.2 [2], clause 6.4.3 | | |
| **PICS Selection** | | | PICS\_GN\_SECURITY AND ***X\_PICS*** | | |
| Expected behaviour | | | | | |
| with  the CA is authorized with certificate C\_ISSUER  ensure that      when         the CA is issued the certificate      then      this certificate is of type EtsiTs103097Certificate  containing issuer  containing self  or containing ***X\_DIGEST***  indicating last 8 bytes of the hash of the certificate calculated using ***X\_ALGORITHM***  referenced to certificate  containing toBeSigned  containing verifyKeyIndicator  containing verificationKey  containing ***X\_KEY*** | | | | | |
| **cPermutation table** | | | | | |
| **XX** | ***X\_DIGEST*** | ***X\_ALGORITM*** | | ***X\_KEY*** | ***X\_PICS*** |
| A | sha256AndDigest | SHA-256 | | ecdsaNistP256 or ecdsaBrainpoolP256r1 | PICS\_SEC\_SHA256  AND PICS\_SEC\_BRAINPOOL\_P256R1 |
| B | sha384AndDigest | SHA-384 | | ecdsaBrainpoolP384r1 | PICS\_SEC\_SHA384 AND PICS\_SEC\_BRAINPOOL\_P384R1 |

#### 5.2.8.4 Check rectangular region validity restriction

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CERT\_05\_BV |
| **Summary** | Check that the rectangular certificate validity region of the subordinate certificate is well formed and inside the validity region of the issuing certificate |
| **Reference** | IEEE 1609.2 [2], clause 6.4.20, 6.4.17,5.1.2.4 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_RECTANGULAR\_REGION |
| Expected behaviour | |
| with  the CA is authorized with AA certificate  containing toBeSigned  containing region  indicating REGION  ensure that     when         the IUT issued the AT certificate      then      this AT certificate is of type EtsiTs103097Certificate  containing toBeSigned  containing region  containing rectangularRegion  containing items of type RectangularRegion  containing northwest  indicating a point inside the REGION  and containing southeast  indicating a point on the south from northwest  and inside the REGION | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CERT\_06\_BV |
| **Summary** | Check that the IUT supports at least 8 entries in the rectangular certificate validity region in the AT certificate |
| **Reference** | IEEE 1609.2 [2], clause 6.4.17 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_RECTANGULAR\_REGION |
| Expected behaviour | |
| With  the IUT is authorized with AT certificate (CERT\_IUT\_C\_AT\_8)  containing toBeSigned  containing region  containing rectangularRegion  containing 8 entries  containing one entry (***ENTRY***)  containing current IUT position  ensure that     when         the IUT is requested to send a secured DENM     then         the IUT sends a message of type EtsiTs103097Data  containing headerInfo               containing generationLocation               indicating position inside the ***ENTRY*** | |

#### 5.2.8.5 Check polygonal region validity restriction

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CERT\_07\_BV |
| **Summary** | Check that the polygonal certificate validity region contains at least three points;  Check that the polygonal certificate validity region does not contain intersections;  Check that the polygonal certificate validity region is inside the validity region of the issuing certificate; |
| **Reference** | IEEE 1609.2 [2], clause 6.4.21, 6.4.17,5.1.2.4 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_POLYGONAL\_REGION |
| Expected behaviour | |
| with  the CA is authorized with AA certificate  containing toBeSigned  containing region  indicating REGION  ensure that     when         the IUT issued the AT certificate      then      this AT certificate is of type EtsiTs103097Certificate  containing toBeSigned  containing region  containing polygonalRegion  containing more then 2 items of type TwoDLocation  indicating points inside the REGION  and indicating unintercepting segments | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CERT\_08\_BV |
| **Summary** | Check that the IUT supports at least 8 points in the polygonal certificate validity region in the AT certificate |
| **Reference** | IEEE 1609.2 [2], clause 6.4.17 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_POLYGONAL\_REGION |
| Expected behaviour | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_D\_AT\_8)  containing toBeSigned  containing region  containing polygonalRegion  containing 8 entries  indicating polygon ***P***  and the IUT’s position is inside the polygon ***P***  ensure that     when         the IUT is requested to send a secured DENM     then         the IUT sends a message of type EtsiTs103097Data  containing headerInfo               containing generationLocation               indicating position inside the ***P*** | |

#### 5.2.8.6 Check identified region validity restriction

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CERT\_09\_BV |
| **Summary** | Check that the identified certificate validity region contains values that correspond to numeric country codes as defined by United Nations Statistics Division [6] in October 2013 |
| **Reference** | IEEE 1609.2 [2], clause 6.4.23 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_IDENTIFIED\_REGION |
| Expected behaviour | |
| ensure that     when         the IUT issued the certificate   containing toBeSigned  containing region  containing identifiedRegion      then      this certificate is of type EtsiTs103097Certificate  containing toBeSigned  containing region  containing identifiedRegion  containing 1 entry of type IdentifiedRegion  containing countryOnly  indicating integer representation of the identifier of country or area  or containing countryAndRegions  containing countryOnly  indicating integer representation of the identifier of country or area  or containing countryAndSubregions  containing country  indicating integer representation of the identifier of country or area | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CERT\_10\_BV |
| **Summary** | Check that the IUT supports at least 8 points in the polygonal certificate validity region in the AT certificate |
| **Reference** | IEEE 1609.2 [2], clause 6.4.17 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_IDENTIFIED\_REGION |
| Expected behaviour | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_E\_AT\_8)  containing toBeSigned  containing region  containing identifiedRegion  containing 8 entries  containing one of the items (***I***)  containing current IUT position  ensure that     when         the IUT is requested to send a secured DENM     then         the IUT sends a message of type EtsiTs103097Data  containing headerInfo               containing generationLocation               indicating position inside the ***I*** | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CERT\_11\_BV |
| **Summary** | Check that the identified region validity restriction of the subordinate certificate is included in the identified region validity restriction of the issuing certificate |
| **Reference** | IEEE 1609.2 [2], clause 6.4.17,5.1.2.4 |
| **PICS Selection** | PICS\_GN\_SECURITY AND PICS\_SEC\_IDENTIFIED\_REGION |
| Expected behaviour | |
| with  the CA is authorized with AA certificate  containing toBeSigned  containing region  containing identifiedRegion  containing countryOnly  indicating COUNTRY  or containing countryAndRegions  containing countryOnly  indicating COUNTRY  and containing regions  indicating REGIONS  or containing countryAndSubregions  containing country  indicating COUNTRY  and containing regionAndSubregions  indicating REGIONS and SUBREGIONS  ensure that     when         the IUT issued the certificate   containing toBeSigned  containing region  containing identifiedRegion      then      this certificate is of type EtsiTs103097Certificate  containing toBeSigned  containing region  containing identifiedRegion  containing countryOnly  indicating value = COUNTRY  or containing countryAndRegions  containing countryOnly  indicating value = COUNTRY  and containing regions  containing region identifiers contained in REGIONS  or containing countryAndSubregions  containing country  indicating value = COUNTRY  and containing regionAndSubregions  containing region identifiers contained in REGIONS  and containing subRegion identifiers contained in SUBREGIONS for every region | |

#### 5.2.8.7 Check time validity restriction in the chain

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CERT\_12\_BV |
| **Summary** | Check that the validityPeriod of the subordinate certificate is inside the vlidityPeriod of the issuing certificate |
| **Reference** | IEEE 1609.2 [2], clause 5.1.2.4 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with  the CA is authorized with AA certificate  containing toBeSigned  containing validityPeriod  containing start  indicating X\_START\_VALIDITY\_AA  containing duration  indicating X\_START\_DURATION\_AA  ensure that     when         the IUT issued the certificate      then      this certificate is of type EtsiTs103097Certificate  containing toBeSigned  containing validityPeriod  containing start  indicating X\_START\_VALIDITY\_AT ( X\_START\_VALIDITY\_AT >= X\_START\_VALIDITY\_AA )  containing duration  indicating value <= X\_START\_VALIDITY\_AT + X\_DURATION\_AT - X\_START\_VALIDITY\_AA | |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **TP Id** | | TP\_SEC\_ITSS\_SND\_CERT\_13\_BV\_***XX*** | |
| **Summary** | | Check that the certificate signature contains ECC point of type set to either compressed\_lsb\_y\_0, compressed\_lsb\_y\_1 or x\_coordinate\_only | |
| **Reference** | | IEEE 1609.2 [2], clause 6.3.29, 6.3.30, 6.3.31 | |
| **PICS Selection** | | PICS\_GN\_SECURITY AND  ***X\_PICS*** | |
| Expected behaviour | | | |
| ensure that     when         the IUT issued the certificate      then      this certificate is of type EtsiTs103097Certificate  containing signature               and containing signature               containing ***X\_SIGNATURE***  containing rSig  containing x-only  or containing compressed-y-0  or containing compressed-y-1 | | | |
| **Permutation table** | | | |
| **XX** | ***X\_SIGNATURE*** | | ***X\_PICS*** |
| A | ecdsaNistP256Signature | |  |
| B | ecdsaBrainpoolP256r1Signature | | PICS\_SEC\_BRAINPOOL\_P256R1 |
| C | ecdsaBrainpoolP384r1Signature | | PICS\_SEC\_SHA384 AND PICS\_SEC\_BRAINPOOL\_P384R1 |

#### 5.2.8.9 Check ECC point type of the certificate public keys

|  |  |  |  |
| --- | --- | --- | --- |
| **TP Id** | | TP\_SEC\_ITSS\_SND\_CERT\_14\_BV | |
| **Summary** | | Check that the certificate verification key contains ECC point of type set to either compressed\_lsb\_y\_0, compressed\_lsb\_y\_1 or uncompressed | |
| **Reference** | | IEEE 1609.2 [2], clause 6.4.38 | |
| **PICS Selection** | | PICS\_GN\_SECURITY AND ***X\_PICS*** | |
| Expected behaviour | | | |
| ensure that     when         the IUT issued the certificate      then      this certificate is of type EtsiTs103097Certificate  containing toBeSigned  containing verifyKeyIndicator  containing verificationKey  containing ***X\_KEY***  containing uncompressed  or containing compressed-y-0  or containing compressed-y-1 | | | |
| **Permutation table** | | | |
| **XX** | ***X\_KEY*** | | ***X\_PICS*** |
| A | ecdsaNistP256 | |  |
| B | ecdsaBrainpoolP256r1 | | PICS\_SEC\_BRAINPOOL\_P256R1 |
| C | ecdsaBrainpoolP384r1 | | PICS\_SEC\_SHA384 AND PICS\_SEC\_BRAINPOOL\_P384R1 |

|  |  |  |  |
| --- | --- | --- | --- |
| **TP Id** | | TP\_SEC\_ITSS\_SND\_CERT\_15\_BV | |
| **Summary** | | Check that the certificate encryption key contains ECC point of type set to either compressed\_lsb\_y\_0, compressed\_lsb\_y\_1 or uncompressed | |
| **Reference** | | IEEE 1609.2 [2], clause 6.4.38 | |
| **PICS Selection** | | PICS\_GN\_SECURITY | |
| Expected behaviour | | | |
| ensure that     when         the IUT issued the certificate      then      this certificate is of type EtsiTs103097Certificate  containing toBeSigned  containing encryptionKey  containing publicKey  containing ***X\_KEY***  containing uncompressed  or containing compressed-y-0  or containing compressed-y-1 | | | |
| **Permutation table** | | | |
| **XX** | ***X\_KEY*** | | ***X\_PICS*** |
| A | eciesNistP256 | |  |
| B | eciesBrainpoolP256r1 | | PICS\_SEC\_BRAINPOOL\_P256R1 |

#### 5.2.8.10 Verify certificate signatures

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **TP Id** | | TP\_SEC\_ITSS\_SND\_CERT\_16\_BV | | |
| **Summary** | | Check the certificate signature | | |
| **Reference** | | ETSI TS 103 097 [1], clauses 6 | | |
| **PICS Selection** | | PICS\_GN\_SECURITY AND ***X\_PICS*** | | |
| Expected behaviour | | | | |
| With  the CA authorized with certificate  containing toBeSigned  containing verifyKeyIndicator  containing verificationKey  containing ***X\_KEY***  ensure that     when         the IUT issued the certificate      then      this certificate is of type EtsiTs103097Certificate  containing issuer  referencing the certificate  containing toBeSigned  containing verifyKeyIndicator  containing verificationKey  containing ***X\_KEY***  indicating KEY              and containing signature           containing ***X\_SIGNATURE***          verifiable using KEY | | | | |
| **Permutation table** | | | | |
| **XX** | ***X\_KEY*** | | ***X\_SIGNATURE*** | ***X\_PICS*** |
| A | ecdsaNistP256 | | ecdsaNistP256Signature |  |
| B | ecdsaBrainpoolP256r1 | | ecdsaBrainpoolP256r1Signature | PICS\_SEC\_BRAINPOOL\_P256R1 |
| C | ecdsaBrainpoolP384r1 | | ecdsaBrainpoolP384r1Signature | PICS\_SEC\_SHA384 AND PICS\_SEC\_BRAINPOOL\_P384R1 |

#### 5.2.8.11 Verify certificate permissions

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CERT\_17\_BV |
| **Summary** | Check that all PSID entries of the appPermissions component of the certificate are unique; |
| **Reference** | IEEE 1609.2 [2], clause 6.4.28, 5.1.2.4 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| ensure that     when         the CA issued the certificate  containing toBeSigned  containing appPermissions      then      this certificate is of type EtsiTs103097Certificate  containing toBeSigned  containing appPermissions  containing items of type PsidSsp  containing psid  indicating unique values in this sequence | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CERT\_18\_BV |
| **Summary** | Check that IUT supports at least 8 items in the appPermissions component of the certificate |
| **Reference** | IEEE 1609.2 [2], clause 6.4.8 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT\_A8)  containing toBeSigned  containing appPermissions  containing 8 entries  indicating the last item  containing psid  indicating the ‘AID\_CAM’  ensure that     when         the IUT is requested to send a secured CAM     then         the IUT sends a message of type EtsiTs103097Data  containing content              containing signedData              containing tbsData              containing headerInfo                   containing psid                      indicating 'AID\_CAM' | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CERT\_19\_BV |
| **Summary** | Check that all PSID entries of the certIssuePermissions component of the certificate are unique; |
| **Reference** | IEEE 1609.2 [2], clause 6.4.28, 5.1.2.4 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| ensure that     when         the IUT issued the certificate  containing toBeSigned  containing certIssuePermissions      then      this certificate is of type EtsiTs103097Certificate  containing toBeSigned  containing certIssuePermissions  containing items of type PsidGroupPermissions  and containing subjectPermissions  containing explicit  containing items of type PsidSspRange  containing psid  indicating unique values in this sequence | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CERT\_20\_BV |
| **Summary** | Check that IUT supports at least 8 items in the certIssuePermissions component of the certificate |
| **Reference** | IEEE 1609.2 [2], clause 6.4.8 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with  the IUT is authorized with AT certificate (CERT\_IUT\_A\_AT\_A8)  containing appPermissions  conformed to the certIssuePermissions  issued by AA certificate (CERT\_IUT\_A\_AA\_C8)  containing toBeSigned  containing certIssuePermissions  containing 8 entries  indicating the last item  containing psid  indicating the ‘AID\_CAM’  ensure that     when         the IUT is requested to send a secured CAM     then         the IUT sends a message of type EtsiTs103097Data  containing content              containing signedData              containing tbsData              containing headerInfo                   containing psid                      indicating 'AID\_CAM' | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CERT\_19\_BV |
| **Summary** | Check that all PSID entries of the appPermissions component of the certificate are also contained in the certIssuePermissions component in the issuing certificate; |
| **Reference** | IEEE 1609.2 [2], clause 6.4.28, 5.1.2.4 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| ensure that     when         the IUT issued the certificate  containing toBeSigned  containing appPermissions      then      this certificate is of type EtsiTs103097Certificate  containing issuer  referenced to the certificate  containing toBeSigned  containing certIssuePermissions  containing items of type PsidGroupPermissions  containing eeType  indicating app(0)  and containing subjectPermissions  containing explicit  containing items of type PsidSspRange  indicating X\_PSID\_RANGE\_LIST  or containing all  containing toBeSigned  containing appPermissions  containing items of type PsidSsp  containing psid  contained in the X\_PSID\_RANGE\_LIST  as a psid | |

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CERT\_20\_BV |
| **Summary** | Check that SSP field in each entry of the appPermissions component of the AT certificate is equal to or a subset of the SSP Range in the corresponding issung entry |
| **Reference** | IEEE 1609.2 [2], clause 6.4.28, 5.1.2.4 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| ensure that     when         the IUT issued the certificate  containing toBeSigned  containing appPermissions      then      this certificate is of type EtsiTs103097Certificate  containing issuer  referenced to the certificate  containing toBeSigned  containing certIssuePermissions  containing items of type PsidGroupPermissions  containing eeType  indicating app(0)  and containing subjectPermissions  containing explicit  containing items of type PsidSspRange  containing psid  indicating X\_PSID\_AA  containing sspRange  indicating X\_SSP\_AA [ X\_PSID\_AA ]  or containing all  containing toBeSigned  containing appPermissions  containing items of type PsidSsp  containing psid  indicating value equal to X\_PSID\_AA  containing ssp  indicating value permitted by X\_SSP\_AA [ X\_PSID\_AA ] | |

#### 5.2.8.12 AT and AA certificate profiles

|  |  |
| --- | --- |
| **TP Id** | TP\_SEC\_ITSS\_SND\_CERT\_AT\_01\_BV |
| **Summary** | Check that the IUT sign messages with Authorization Ticket certificate  Check that AT certificate certificate\_id is set to none  Check that AT certificate contains appPermission  Check that AT certificate doesn’t contain certIssuePermissions |
| **Reference** | ETSI TS 103 097 [1], clause 7.2.1 |
| **PICS Selection** | PICS\_GN\_SECURITY |
| Expected behaviour | |
| with     the IUT is in ‘authorized’ state      the IUT being requested to include certificate in the next CAM  ensure that     when         the IUT is requested to send a secured CAM      then  the IUT sends a message of type EtsiTs103097Data          containing signer  containing certificate  containing toBeSigned       containing id  indicating ‘none’  and containing appPermissions  and not containing certIssuePermissions | |

Annex A (informative):  
Bibliography

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

# History

|  |  |  |
| --- | --- | --- |
| **Document history** | | |
| V1.1.1 | July 2013 | Publication |
| V1.2.1 | September 2015 | Publication |
| V1.3.1 | March 2017 | Publication |
| V1.3.4 | May 2018 | STF538: Final draft |
|  |  |  |
|  |  |  |