ETSI TS 103 096-2 V1.4.1 (2018-08)

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

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

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

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 specifications for ITS Security, as identified below:

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

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

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

Modal verbs terminology

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

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

1 Scope

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

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

2 References

2.1 Normative references

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

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

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

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

[1] ETSI TS 103 097 (V1.3.1): "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: " IEEE 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 (V1.4.1): "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] United Nations Statistics Division: "Composition of Macro Geographical (Continental) Regions, Geographical Sub-Regions, and Selected Economic and Other Groupings".

NOTE: Available at http://unstats.un.org/unsd/methods/m49/m49regin.htm.

2.2 Informative references

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

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

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

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

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

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

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

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

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

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

3 Definitions and abbreviations

3.1 Definitions

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

3.2 Abbreviations

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

AA	Authorization Authority
AID	Application Identifier
AID_CAM	ITS Application Identifier for CAM
AID_DENM	Application Identifier for DENM
AID_GN	Application Identifier for general GeoNetworking messages
AT	Authorization Ticket
ATS	Abstract Test Suite
BO	Exceptional Behaviour
BV	Valid Behaviour
CA	Certificate Authority
CAM	Co-operative Awareness Messages
CAN	Controller Area Network
CERT	Certificate
COER	Cannonical Octet Encoding Rules
DE	Data Element
DEN	Decentralized Environmental Notification
DENM	Decentralized Environmental Notification Message
EA	Enrolment Authority
ECC	Elliptic Curve Cryptography
GN	GeoNetworking
ITS	Intelligent Transport Systems
ITS-S	Intelligent Transport System - Station
IUT	Implementation under Test
MSG	Message
PICS	Protocol Implementation Conformance Statement
PSID	Provider Service Identifier
RCA	Root Certificate Authority
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 a 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 Std 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]

6 ITS-S Security

6.1 Overview

Void.

6.2 Sending behaviour

6.2.1 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 IEEE Std 1609.2 [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'	

6.2.2 CAM profile

6.2.2.1 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	

6.2.2.2 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'	

6.2.2.3 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 does not contain 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	

6.2.2.4 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 Std 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 Std 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 (uncompressed)	SHA-256	
B	CERT_IUT_A_B_AT	ecdsaBrainpoolP256r1	SHA-256	PICS_SEC_BRAINPOOL_P256R1
BN	CERT_IUT_A_B_N_AT	ecdsaBrainpoolP256r1 (uncompressed)	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 (uncompressed)	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 + 1 sec)

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 + 1 sec
   then
      this message is
         containing certificate
```

6.2.2.5 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+1 sec)
ensure that
   when
      the IUT is requested to send secured CAM
            at TIME_3 (TIME_1 < TIME_2 < TIME_3 < TIME_1 + 1 sec)
   then
      the IUT sends a message of type EtsiTs103097Data
         containing signedData
            containing signer
               containing certificate
```

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

TP Id	TP_SEC_ITSS_SND_CAM_09_BV
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 + 0,3 sec) 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 1 sec	

6.2.2.7 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 Std 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 Std 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

6.2.2.8 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 Std 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+1 sec) ensure that when the IUT is requested to send a CAM at TIME_3 (TIME_1 < TIME_2 < TIME_3 < TIME_1+1 sec) then the IUT sends a SecuredMessage of type EtsiTs103097Data containing signer and containing certificate referenced by the requested digest	

6.2.2.9 Check that IUT sends 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 Std 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+1 sec) ensure that when the IUT is requested to send a secured CAM at TIME_3 (TIME_1 < TIME_2 < TIME_3 < TIME_1+1 sec) 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 Std 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+1 sec)
ensure that
when
the IUT is requested to send a secured CAM
at TIME_3 (TIME_1 < TIME_2 < TIME_3 < TIME_1+1 sec)
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 does not 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 Std 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+0,8 sec)
  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+0,1 sec)
ensure that
  when
    the IUT is requested to send a secured CAM
      at TIME_4 (TIME_3 < TIME_4 < TIME_1+0,9 sec)
  then
    the IUT sends a SecuredMessage of type EtsiTs103097Data
      containing headerInfo
        does not contain requestedCertificate

TP Id	TP_SEC_ITSS_SND_CAM_16_BV
Summary	Check that the IUT does not 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 Std 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+0,9 sec)
ensure that
  when
    the IUT is requested to send a secured CAM
      at TIME_3 (TIME_2 < TIME_3 < TIME_1+1 sec)
  then
    the IUT sends a SecuredMessage of type EtsiTs103097Data
      containing signer
        containing certificate
      and containing headerInfo
        does not contain requestedCertificate

TP Id	TP_SEC_ITSS_SND_CAM_17_BV
Summary	Check that the IUT sends 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 Std 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+0,9 sec < TIME2 < TIME_1+1 sec)
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

6.2.2.10 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], clause 7.1.1 IEEE Std 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 - 5 min <= GEN_TIME <= CUR_TIME + 5 min) 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	

6.2.2.11 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	

6.2.2.12 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 appPermissions allowing to sign CA messages
Reference	ETSI TS 103 097 [1], clause 7.2.1 IEEE Std 1609.2 [2], clause 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	

6.2.2.13 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 algorithm by cryptographically verifying the signature
Reference	ETSI TS 103 097 [1], clauses 5.2, 7.1.1 IEEE Std 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 Std 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	

6.2.2.14 Check certificate consistency conditions

TP Id	TP_SEC_ITSS_SND_CAM_23_BV
Summary	Check that IUT does not send secured CAMs if IUT is authorized with AT certificate does not allow sending messages in this location
Reference	IEEE Std 1609.2 [2], clause 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 does not send CAM	

TP Id	TP_SEC_ITSS_SND_CAM_24_BV
Summary	Check that IUT does not 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 Std 1609.2 [2], clause 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 does not send CAM	

TP Id	TP_SEC_ITSS_SND_CAM_25_BV
Summary	Check that IUT does not send secured CAMs if all AT certificates installed on the IUT was expired
Reference	IEEE Std 1609.2 [2], clause 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 does not send CAM	

TP Id	TP_SEC_ITSS_SND_CAM_26_BV
Summary	Check that IUT does not send secured CAMs if all AT certificates installed on the IUT have the starting time in the future
Reference	IEEE Std 1609.2 [2], clause 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 does not send CAM	

TP Id	TP_SEC_ITSS_SND_CAM_27_BV
Summary	Check that IUT does not send secured CAMs if IUT does not possess an AT certificate allowing sending CAM by its appPermissions
Reference	IEEE Std 1609.2 [2], clause 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 does not send CAM	

6.2.3 DENM profile

6.2.3.1 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], clause 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	

6.2.3.2 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], clause 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'	

6.2.3.3 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 does not contain expiryTime, encryptionKey, p2pcdLearningRequest, missingCrlIdentifier, inlineP2pcdRequest, requestedCertificate
Reference	ETSI TS 103 097 [1], clauses 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	

6.2.3.4 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 Std 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	

6.2.3.5 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 Std 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 + 10 min) 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	

6.2.3.6 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 does not have any region restriction
Reference	ETSI TS 103 097 [1], clause 7.1.2 IEEE Std 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 issued by the certificate AA (CERT_IUT_A_AA) containing toBeSigned not containing region and issued 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 Std 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 Std 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 does not contain any region restriction
Reference	ETSI TS 103 097 [1], clause 7.1.2 IEEE Std 1609.2 [2], clauses 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 issued by the certificate AA (CERT_IUT_CC_AA) containing toBeSigned containing circularRegion indicating REGION and issued 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 do not contain any region restriction
Reference	ETSI TS 103 097 [1], clause 7.1.2 IEEE Std 1609.2 [2], clauses 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 issued by the certificate AA (CERT_IUT_CA_AA) containing toBeSigned not containing region and issued 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	

6.2.3.7 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	

6.2.3.8 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 appPermissions allowing to sign DEN messages
Reference	ETSI TS 103 097 [1], clause 7.1.2 IEEE Std 1609.2 [2], clause 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	

6.2.3.9 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 algorithm by cryptographically verifying the signature
Reference	ETSI TS 103 097 [1], clauses 5.2, 7.1.2 IEEE Std 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

6.2.3.10 Check certificate consistency conditions

TP Id	TP_SEC_ITSS_SND_DENM_14_BV
Summary	Check that IUT does not send secured DENMs if IUT does not possess an AT certificate allowing sending messages in this location
Reference	IEEE Std 1609.2 [2], clause 6.2.3.2.2
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 does not send DENM

TP Id	TP_SEC_ITSS_SND_DENM_15_BV
Summary	Check that IUT does not 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 Std 1609.2 [2], clause 6.2.3.2.2
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 does not send DENM	

TP Id	TP_SEC_ITSS_SND_DENM_16_BV
Summary	Check that IUT does not send secured DENMs if all AT certificates installed on the IUT are expired
Reference	IEEE Std 1609.2 [2], clause 6.2.3.2.2
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 does not send DENM	

TP Id	TP_SEC_ITSS_SND_DENM_17_BV
Summary	Check that IUT does not send secured DENMs if all AT certificates installed on the IUT have the starting time in the future
Reference	IEEE Std 1609.2 [2], clause 6.2.3.2.2
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 does not send DENM	

TP Id	TP_SEC_ITSS_SND_DENM_18_BV
Summary	Check that IUT does not send secured DENMs if IUT does not possess an AT certificate allowing sending DENM by its appPermissions
Reference	IEEE Std 1609.2 [2], clause 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 does not send DENM	

6.2.4 Generic signed message profile

6.2.4.1 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], 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	

6.2.4.2 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	

6.2.4.3 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	

6.2.4.4 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 Std 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	

6.2.4.5 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, 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 - 10 min <= GEN_TIME <= CUR_TIME + 10 min) 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	

6.2.4.6 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	

6.2.4.7 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 appPermissions allowing to sign these messages
Reference	ETSI TS 103 097 [1], clause 7.1.3 IEEE Std 1609.2 [2], clause 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	

6.2.4.8 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 algorithm by cryptographically verifying the signature
Reference	ETSI TS 103 097 [1], clauses 5.2, 7.1.3 IEEE Std 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

6.2.5 Encrypted messages profile

6.2.5.1 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], clause 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	

6.2.5.2 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 Std 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 Std 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 recipient 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

6.2.5.3 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 Std 1609.2 [2], clause 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	

6.2.5.4 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 Std 1609.2 [2], clause 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	

6.2.6 Profiles for certificates

6.2.6.1 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], clause 6 IEEE Std 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	

6.2.6.2 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 [1], clause 6
Reference	ETSI TS 103 097 [1], clause 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	

6.2.6.3 Check the issuer reference of the certificate

TP Id	TP_SEC_ITSS_SND_CERT_04_BV_***X***
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 Std 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***	

Permutation table

X	***X_DIGEST***	***X_ALGORITHM***	***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

6.2.6.4 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 Std 1609.2 [2], clauses 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 Std 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***	

6.2.6.5 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 Std 1609.2 [2], clauses 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 than 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 Std 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***	

6.2.6.6 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 [5]
Reference	IEEE Std 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 Std 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 Std 1609.2 [2], clauses 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
```

6.2.6.7 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 validityPeriod of the issuing certificate
Reference	IEEE Std 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	

6.2.6.8 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 Std 1609.2 [2], clauses 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

6.2.6.9 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 Std 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 Std 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

6.2.6.10 Verify certificate signatures

TP Id	TP_SEC_ITSS_SND_CERT_16_BV
Summary	Check the certificate signature
Reference	ETSI TS 103 097 [1], clause 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

6.2.6.11 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 Std 1609.2 [2], clauses 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 Std 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 Std 1609.2 [2], clauses 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 Std 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 Std 1609.2 [2], clauses 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 issuing entry
Reference	IEEE Std 1609.2 [2], clauses 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 ]
```

6.2.6.12 AT and AA certificate profiles

TP Id	TP_SEC_ITSS_SND_CERT_AT_01_BV
Summary	Check that the IUT signs 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 does not 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
V1.4.1	August 2018	Publication