# ETSI TS 103 096-2 V1.5.1 (2022-01)



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

Reference

RTS/ITS-005211

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 - APE 7112B Association à but non lucratif enregistrée à la Sous-Préfecture de Grasse (06) N° w061004871

#### Important notice

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

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format at <a href="http://www.etsi.org/deliver">www.etsi.org/deliver</a>.

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 <u>https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx</u>

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

#### Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

#### **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 convertent and the foregoing restriction extend to reproduction in all media

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2022. All rights reserved.

## Contents

Intelle	ectual Property Rights	5
Forew	vord	5
Moda	l verbs terminology	5
1	Scope	6
2	References	6
2.1	Normative references	6
2.2	Informative references	6
3	Definition of terms, symbols and abbreviations	7
3.1	Terms	
3.2	Symbols	
3.3	Abbreviations	
4	Test Suite Structure (TSS)	8
4.1	Structure for Security tests	
	-	
5	Test Purposes (TP)	
5.1 5.1.1	Introduction TP definition conventions	
5.1.1	TP Identifier naming conventions	
5.1.3	Rules for the behaviour description	
5.1.4	Sources of TP definitions	
5.1.5	Mnemonics for PICS reference	
6	ITS-S Security	10
6.1	Overview	
6.1.1	Certificates content	
6.1.1.1		
6.1.1.2		
6.1.1.3		
6.2	Sending behaviour	
6.2.1	General sending behaviour	
6.2.1.1 6.2.2	1 Check the message protocol version CAM profile	
6.2.2.1	1	
6.2.2.2	e	
6.2.2.3		
6.2.2.4		
6.2.2.5		
6.2.2.6		
6.2.2.7		
6.2.2.8 6.2.2.9	1	
6.2.2.1		
6.2.2.1		
6.2.2.1		
6.2.2.1	13 Check signature	26
6.2.2.1	11	
6.2.2.1		
6.2.3	DENM profile	
6.2.3.1 6.2.3.2		
6.2.3.3		
6.2.3.4		
6.2.3.5	e	
6.2.3.6	5 Check generation location	
6.2.3.7	7 Check payload	34

6.2.3.8	Check signing permissions	
6.2.3.9	Check signature	
6.2.3.10	Check support for certificate content	
6.2.3.11	Check certificate consistency conditions	
6.2.4	Generic signed message profile	
6.2.4.1	Check that secured message is signed	
6.2.4.2	Check secured AID value	
6.2.4.3	Check header field	
6.2.4.4	Check that signer info is a certificate or digest	
6.2.4.5	Check generation time	
6.2.4.6	Check payload	
6.2.4.7	Check signing permissions	
6.2.4.8	Check signature	
6.3	Receiving behaviour	
6.3.1	Check the message protocol version	
6.3.2	CAM profile	
6.3.2.1	Check the valid message receiving	
6.3.2.2	Check invalid HeaderInfo elements	
6.3.2.3	Check invalid Signature elements	
6.3.3	DENM profile	
6.3.2.1	Check the valid message receiving	
6.3.3.2	Check invalid HeaderInfo elements	
6.3.3.3	Check invalid Signature elements	
Annex A	(informative): Bibliography	56
History		57

## Intellectual Property Rights

#### **Essential patents**

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

**DECT<sup>TM</sup>**, **PLUGTESTS<sup>TM</sup>**, **UMTS<sup>TM</sup>** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP<sup>TM</sup>** and **LTE<sup>TM</sup>** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M<sup>TM</sup>** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**<sup>®</sup> and the GSM logo are trademarks registered and owned by the GSM Association.

## 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. Full details of the entire series can be found in part 1 [3].

## 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 <a href="https://docbox.etsi.org/Reference/">https://docbox.etsi.org/Reference/</a>.

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 (V1.4.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".
- IEEE Std 1609.2<sup>TM</sup>-2016: "IEEE Standard for Wireless Access in Vehicular Environments -Security Services for Applications and Management Messages", as amended by IEEE Std 1609.2a<sup>TM</sup>-2017: "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages - Amendment 1".
- [3] ETSI TS 103 096-1 (V1.5.1): "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] Void.

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

7

- [i.5]ISO/IEC 9646-6 (1994): "Information technology -- Open Systems Interconnection --<br/>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 Definition of terms, symbols and abbreviations

#### 3.1 Terms

For the purposes of the present document, the terms 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 Symbols

Void.

#### 3.3 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
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

ТР	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

8

Root Group		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>_<sgr>_<rn>_<sn>_<x>[_<v>]</v></x></sn></rn></sgr></tgt></root>		
	<root> = root</root>	SEC	
	<tgt> = target</tgt>	ITSS	ITS-S data transfer
		CA	Certificate Authority tests
		AA	ITS-S - AA authorization
		EA	ITS-S - EA enrolment
	<gr> = group</gr>	SND	Sending behaviour
		RCV	Receiving behaviour
	<sgr> =sub- group</sgr>	MSG	Generic messages
		CAM	CAM testing
		DENM	DENM testing
		CERT	Certificate testing
	<sn> = test purpose sequential number</sn>		01 to 99
	<x> = category</x>	BV	Valid Behaviour tests
		BO	Invalid Behaviour Tests
	<v> = variant (optional)</v>		A to Z

#### 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

PICS\_SEC\_IMPLICIT\_CERTIFICATE

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.

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

S1.2.2.8 [2]

#### **Table 3: Mnemonics for PICS reference**

## 6 ITS-S Security

6.1 Overview

### 6.1.1 Certificates content

#### 6.1.1.1 Root Certificate Authorities certificates

RCA certificate	Content	To be installed on the IUT
CERT_IUT_A_RCA	<ul> <li>self-signed</li> <li>name "ETSI Test RCA A certificate"</li> <li>application permissions:         <ul> <li>CRL with SSP 0x01</li> <li>CTL with SSP 0x0138</li> </ul> </li> <li>certificate issuing permissions:         <ul> <li>CAM with all possible SPP (0x01FFFC / 0xFF0003)</li> <li>DENM with all possible SSP (0x01FFFFF / 0xFF000000)</li> <li>SPATEM with all possible SSP (0x01E0 / 0xFF1F)</li> <li>MAPEM with all possible SSP (0x01C0 / 0xFF3F)</li> <li>IVIM with all possible SSP (0x01000000FFF8 / 0xFF000000007)</li> <li>SREM with all possible SSP (0x01 / 0xFF1F)</li> <li>GPC with all possible SSP (0x01 / 0xFF)</li> <li>GR-MGMT without SSP</li> <li>CRT-REQ with SSP (0x01 / 0xFF01)</li> </ul> </li> <li>validation time for 3 years</li> <li>no region restriction</li> <li>assurance level 6</li> <li>verification key of type compressed with NIST P256R curve</li> <li>valid signature of type x-only with NIST P256R curve</li> </ul>	Yes
CERT_IUT_A_RCA_A8	Same as CERT_IUT_A_ATCERT_IUT_A_RCA, excepting the following: - certificate issuing permissions: o same as in CERT_IUT_A_RCA o unallocated ITS AIDs: 96, 97, 98, 99, 100, 101, 102 without SSP	Yes
CERT_IUT_C_RCA	Same as CERT_IUT_A_ATCERT_IUT_A_RCA, excepting the following: - rectangular region restriction (10km square) - no unallocated ITS AID in certificate issuing permissions	Yes

AA certificate			
CERT_IUT_A_AA	<ul> <li>signer digest of the CERT_IUT_A_RCA</li> <li>application permissions: <ul> <li>CRT_REQ with SSP 0x0132</li> </ul> </li> <li>certificate issuing permissions: <ul> <li>CAM with all possible SPP (0x01FFFC / 0xFF0003)</li> <li>DENM with all possible SSP (0x01FFFFF / 0xFF000000)</li> <li>SPATEM with all possible SSP (0x01E0 / 0xFF1F)</li> <li>MAPEM with all possible SSP (0x01C0 / 0xFF3F)</li> <li>IVIM with all possible SSP (0x0100000FFF8 / 0xFF000000007)</li> <li>SREM with all possible SSP (0x01 / 0xFF5)</li> <li>IVIM with all possible SSP (0x01 / 0xFF)</li> <li>GPC with all possible SSP (0x01 / 0xFF)</li> <li>GPC with all possible SSP (0x01 / 0xFF)</li> <li>GN-MGMT without SSP</li> <li>validation time for 3 years</li> <li>no region restriction</li> <li>assurance level 4</li> <li>verification key of type compressed with NIST P256R curve</li> <li>encryption key of type compressed with NIST P256R curve</li> <li>valid signature of type x-only with NIST P256R curve</li> </ul> </li> </ul>	Yes	
CERT_IUT_A_N_AA	Same as CERT_IUT_A_ATCERT_IUT_A_AA, excepting the following: - verification key of type uncompressed	Yes	
CERT_IUT_A_B_AA	Same as CERT_IUT_A_ATCERT_IUT_A_AA, excepting the following: - verification key with Brainpool P256r1 curve	Yes	
CERT_IUT_A_B3_AA	Same as CERT_IUT_A_ATCERT_IUT_A_B_AA, excepting the following: - verification key with Brainpool P384r1 curve	Yes	
CERT_IUT_A_AA_A8	Same as CERT_IUT_A_ATCERT_IUT_A_AA, excepting the following: - signer digest of the CERT_IUT_A_RCA_A8 - certificate issuing permissions:	Yes	
CERT_IUT_CC_AA	Same as CERT_IUT_A_ATCERT_IUT_A_AA, excepting the following: - signer digest of the CERT_IUT_C_RCA - rectangular region restriction equal to the one in the CERT_IUT_C_RCA	Yes	
CERT_IUT_C3_AA	Same as CERT_IUT_A_ATCERT_IUT_CC_AA, excepting the following: - rectangular region restriction oversizing the one in the CERT_IUT_C_RCA	Yes	
CERT_IUT_CA_AA	Same as CERT_IUT_A_ATCERT_IUT_CC_AA, excepting the following: - no region restriction	Yes	
CERT_IUT_D_AA	Same as CERT_IUT_A_ATCERT_IUT_CC_AA, excepting the following: - polygonal region restriction as a square with the side of 10 km and center in the IUT position	Yes	
CERT_TS_A_AA	Same as CERT_IUT_A_ATCERT_IUT_A_AA. To be used on the Test System side.	Yes	
CERT_TS_B_AA	Same as CERT_IUT_A_ATCERT_IUT_A_B_AA. To be used on the Test System side.	Yes	
CERT_TS_A_B_AA	Same as CERT_IUT_A_ATCERT_IUT_A_B_AA. To be used on the Test System side.	Yes	

#### 6.1.1.3 Authorization Tickets

Authorization ticket	Content	To be installed on the IUT
CERT_IUT_A_AT	<ul> <li>signer digest of the CERT_IUT_A_AA;</li> <li>application permissions:</li> </ul>	Yes
	<ul> <li>CAM with all SPP (0x01FFFC);</li> <li>DENM with all SSP (0x01FFFFFF);</li> </ul>	
	<ul> <li>GN-MGMT;</li> <li>validation time for 1 year;</li> </ul>	
	- no region restriction;	
	- assurance level 3;	
	<ul> <li>verification key of type compressed with NIST P256R curve;</li> <li>encryption key of type compressed with NIST P256R curve;</li> </ul>	
	<ul> <li>valid signature of type x-only with NIST P256R curve;</li> </ul>	
CERT_IUT_A_N_AT	Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following: - verification key of type uncompressed;	Yes
CERT_IUT_A_B_AT	Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following:	Yes
	<ul> <li>signer digest of the CERT_IUT_A_B_AA;</li> <li>verification key with Brainpool P256r1 curve;</li> </ul>	
	<ul> <li>valid signature with Brainpool P256r1 curve;</li> </ul>	
CERT_IUT_A_B_N_AT	Same as CERT_IUT_A_ATCERT_IUT_A_B_AT, excepting the following: - verification key of type uncompressed;	Yes
CERT_IUT_A_B3_AT	Same as CERT_IUT_A_ATCERT_IUT_A_B_AT, excepting the following: - verification key with Brainpool P384r1 curve;	Yes
CERT_IUT_A_B3_N_AT	Same as CERT_IUT_A_ATCERT_IUT_A_B3_AT, excepting the following: - verification key of type uncompressed;	Yes
CERT_IUT_A_B33_AT	Same as CERT_IUT_A_ATCERT_IUT_A_B3_AT, excepting the following:	Yes
	<ul> <li>signer digest of the CERT_IUT_A_B3_AA;</li> </ul>	
CERT_IUT_A_AT_A8	- valid signature with Brainpool P384r1 curve; Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following:	Yes
	- signer digest of the CERT_IUT_A_AA_A8;	163
	- application permissions:	
	<ul> <li>CAM with all SPP (0x01FFFC);</li> <li>unallocated ITS AIDs: 96, 97, 98, 99, 100, 101, 102 without SSP;</li> </ul>	
CERT_IUT_B_AT	Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following:	Yes
	<ul> <li>circular region restriction with the radius of 5 km and center at the IUT point;</li> </ul>	
CERT_IUT_C_AT	Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following: - rectangular region restriction with the side of 5 km and center at the	Yes
	IUT point;	
CERT_IUT_D_AT	Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following: - signer digest of the CERT_IUT_D_AA;	Yes
	<ul> <li>polygonal region restriction identical to the one in the CERT_IUT_D_AA, including the IUT position;</li> </ul>	
CERT_IUT_D_AT_8	Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following: - polygonal region restriction contains 8 points;	Yes
CERT_IUT_E_AT	Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following: - identified region restriction including the IUT point;	Yes
CERT_IUT_E_AT_8	Same as CERT_IUT_A_ATCERT_IUT_E_AT, excepting the following: - identified region restriction contains 8 region identifiers;	Yes
CERT_IUT_A1_AT	Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following: - the certificate is expired;	Yes
CERT_IUT_A2_AT	Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following: - the certificate is not valid yet;	Yes
CERT_IUT_A3_AT	Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following:	Yes
	<ul> <li>application permissions:</li> <li>DENM with all SSP (0x01FFFFFF);</li> <li>GN-MGMT;</li> </ul>	
CERT_IUT_A4_AT	Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following:	Yes
	- application permissions:	
	<ul> <li>CAM with all SPP (0x01FFFC);</li> <li>GN-MGMT;</li> </ul>	
CERT_IUT_C1_AT	Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following:	Yes
	<ul> <li>signer digest of the CERT_IUT_CC_AA;</li> </ul>	
	<ul> <li>rectangular region restriction outside of the IUT point;</li> </ul>	

Authorization ticket	Content	To be installed on the IUT	
CERT_IUT_C_AT_8	Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following: - rectangular region restriction contains 8 elements;	Yes	
CERT_TS_A_AT	Same as CERT_IUT_A_ATCERT_IUT_A_AT To be used on the Test System side.	Yes	
CERT_TS_A_B_AT	Same as CERT_IUT_A_ATCERT_TS_A_AT, excepting the following: - verification key with Brainpool P256r1 curve;	Yes	
CERT_TS_A_B3_AT	Same as CERT_IUT_A_ATCERT_TS_A_AT, excepting the following: - verification key with Brainpool P384r1 curve;	Yes	
CERT_TS_B_AT	Same as CERT_IUT_A_ATCERT_TS_A_AT, excepting the following: - circular region restriction with a radius of 5 km from the IUT point; To be used on the Test System side.	Yes	
CERT_TS_B1_AT	Same as CERT_IUT_A_ATCERT_IUT_A_B_AT, excepting the following: - circular region restriction with a radius of 5 km from the base point; To be used on the Test System side.	Yes	
CERT_TS_C_AT	Same as CERT_IUT_A_ATCERT_TS_A_AT, excepting the following: - rectangular region restriction with the side of 5 km and center at the IUT point; To be used on the Test System side.	Yes	
CERT_TS_D_AT	Same as CERT_IUT_A_ATCERT_TS_A_AT, excepting the following: - polygonal region restriction including the IUT position;	Yes	
CERT_TS_E_AT	Same as CERT_IUT_A_ATCERT_TS_A_AT, excepting the following: - identified region restriction including the IUT point;	Yes	
CERT_TS_F_AT	Same as CERT_IUT_A_ATCERT_TS_A_AT To be used on the Test System side.	No	
CERT_TS_F3_AT	Same as CERT_TS_F_AT, excepting the following: - verification key with Brainpool P384r1 curve; To be used on the Test System side.	No	

## 6.2 Sending behaviour

## 6.2.1 General sending behaviour

### 6.2.1.1 Check the message protocol version

TP ld	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 'auth ensure that when the IUT is requested to then the IUT sends a EtsiTs containing protocol indicating value '3	o send a secured message s103097Data /ersion	

### 6.2.2 CAM profile

### 6.2.2.1 Check that secured CAM is signed

TP ld	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
ensure that when the IUT is requested to then	age of type EtsiTs103097Data

#### 6.2.2.2 Check secured CAM AID value

TP ld	TP_SEC_ITSS_SND_CAM_02_BV	
Summony	Check that IUT sends the secured CAM containing the HeaderInfo field psid set to	
Summary	'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	th AT certificate (CERT_IUT_A_AT)	
ensure that		
when		
the IUT is requested	to send a secured CAM	
then		
	sage of type EtsiTs103097Data	
containing content		
containing signe		
containing tbs		
containing headerInfo		
	containing psid	
Indicat	ting 'AID_CAM'	

TP ld	TP_SEC_ITSS_SND_CAM_03_BV	
	Check that IUT sends the secured CAM with the HeaderInfo containing generationTime	
Summary	and does not contain expiryTime, generationLocation, encryptionKey,	
	p2pcdLearningRequest, missingCrlldentifier	
Reference	ETSI TS 103 097 [1], clauses 5.2 and 7.1.1	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT is authorized with	n AT certificate (CERT_IUT_A_AT)	
ensure that		
when		
the IUT is requested to	o send a secured CAM	
then		
the IUT sends a messa	age of type EtsiTs103097Data	
containing content		
containing signed		
containing tbs		
containing h		
containing	g generationTime	
	ontaining expiryTime	
	ontaining generationLocation,	
and not containing encryptionKey		
	ontaining p2pcdLearningRequest	
and not co	ontaining missingCrlIdentifier	

#### 6.2.2.3 Check header fields

### 6.2.2.4 Check signer information

TP ld	TP_SEC_ITSS_SND_CAM_04_BV	
	Check that IUT sends the secured CAM containing signer containing either certificate or	
Summary	digest	
	Check that signing certificate has permissions to sign CAM messages	
Reference	ETSI TS 103 097 [1], clauses 5.2 and 7.1.1	
Reference	IEEE Std 1609.2 [2], clause 6.3.4	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT is authorized with	h AT certificate (CERT_IUT_A_AT)	
ensure that		
when		
the IUT is requested to	o send a secured CAM	
then		
the IUT sends a message of type EtsiTs103097Data		
containing content		
containing signed	Data	
containing sigr	ner	
containing d	ligest	
or containing	g certificate	
containin	g id	
indicating 'none'		
	ining toBeSigned	
containing appPermissions		
	containing the item of type PsidSsp	
	containing psid	
	indicating AID_CAM	
ar	nd not containing certIssuePermissions	

TP I	d	TP_SEC_ITSS_SND_C	AM 05 BV	
Sum	mary	Check that IUT calculate	e the digest o	f certificate using proper hash algorithm
				tes before hash calculation
Refe	erence	ETSI TS 103 097 [1], cl		d 7.1.1
		IEEE Std 1609.2 [2], cla		
PICS	S Selection	PICS_GN_SECURITY		
		Expec	ted behaviou	Ir
with				
	e IUT is authorized with AT			
	nd the IUT is configured to		A per second	
ar	nd the IUT having sent a se	ecured CAM		
	containing signer containing certificate			
	indicating X_CERTIF			
	containing verifyKe			
	containing verifi			
	containing X_			
ensu	ure that			
w	hen			
	the IUT is requested to se	nd a subsequent secured	d CAM	
	containing signer			
416	containing digest			
th	ien the IUT sends a message	of type EtciTe102007Da	to	
	containing content	or type Etsins 103097 Da	la	
	containing signedDat	a		
	containing signer			
	containing diges	st		
			le calculated	using <b>X_HASH</b> algorithm
	-		utation table	
ХХ	X_CERTIFICATE	X_KEY	X_HASH	X_PICS
Α	CERT_IUT_A_AT	ecdsaNistP256	SHA-256	
AN	CERT_IUT_A_N_AT	ecdsaNistP256 (uncompressed)	SHA-256	
В	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				
С	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
		(uncompressed)	PICS_SEC_BRAINPOOL_P384R1	

TP ld	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	d with AT certificate (CERT_IUT_A_AT)
and the IUT is config	gured to send more than one CAM per second
and the IUT having	sent a secured CAM
containing genera	itionTime
indicating TIME	LAST
ensure that	
when	
the IUT is sending	g secured CAM as a message of type EtsiTs103097Data
containing sign	
containing c	ertificate
then	
this message is	
containing head	
00	
indicating	TIME (TIME >= TIME_LAST + 1 sec)

TP ld	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	I with AT certificate (CERT_IUT_A_AT)
and the IUT is config	ured to send more than one CAM per second
and the IUT having s	ent a secured CAM
containing signer	
containing certifi	icate
and containing ge	nerationTime
indicating TIME_	_LAST
ensure that	
when	
the IUT is sending	a secured CAM as a message of type EtsiTs103097Data
containing gene	erationTime
indicating TIN	/E >= TIME_LAST + 1 sec
then	
this message is	
containing certil	ficate

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

TP ld	TP_SEC_ITSS_SND_CAM_08_BV
Summary	Check that IUT sends the secured CAM containing the signing certificate when the IUT
ounnary	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	
	d with AT certificate (CERT_IUT_A_AT)
	gured to send more than one CAM per second
	already sent secured CAM
containing certification	ate
at TIME_1	
	received a message of type EtsiTs103097Data
containing signed	
containing sign	
containing di	
	HashedId8 value
	cing an unknown certificate (CERT_TS_F_AT)
ensure that	_1 < TIME_2 < TIME_1+1 sec)
when	
	ted to send secured CAM
	$\beta$ (TIME_1 < TIME_2 < TIME_3 < TIME_1 + 1 sec)
then	(TIME_I > TIME_2 > TIME_0 > TIME_I + 1 300)
	nessage of type EtsiTs103097Data
containing sign	
containing sign	
	l certificate

TP Id	TP_SEC_ITSS_SND_CAM_09_BV	
Summary		
Reference	ETSI TS 103 097 [1], clause 7.1.1	
PICS Selection	PICS GN SECURITY	
	Expected behaviour	
with		
the IUT is authori	zed with AT certificate (CERT_IUT_A_AT)	
	nfigured to send more than one CAM per second	
	g already sent secured CAM	
containing sign	er	
containing c	ertificate	
at TIME_1		
and the IUT havir	g received a secured CAM	
containing sign	er	
containing d	igest	
indicating	HashID8 value	
	cing an unknown certificate (CERT_TS_F_AT)	
	1E_1 + 0,3 sec)	
	ig sent secured CAM	
containing sign		
containing c		
	1E_3 > TIME_2)	
ensure that		
when		
	ling the next secured CAM	
containing si		
containing		
	ing certificate	
at TIME_4		
then		
the difference t	between TIME_4 and TIME_3 is about 1 sec	

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

6.2.2.7	Check sending certificate request for unknown certificate
---------	---

TP ld	TP SEC ITSS SND CAM 10 BV
C	Check that the IUT sends certificate request when it receives secured CAM containing
Summary	digest of unknown certificate as a message signer
Reference	ETSI TS 103 097 [1], clause 7.1.1
Relefence	IEEE Std 1609.2 [2], clauses 6.3.9 and 8.2.4.1.2
PICS Selection	PICS_GN_SECURITY, PICS_SEC_P2P_AT_DISTRIBUTION
	Expected behaviour
with	
the IUT is authorized wi	th AT certificate (CERT_IUT_A_AT)
and the IUT has receive	ng a EtsiTs103097Data
containing signer	
containing digest	
indicating Hashe	edid8 value DIGEST_F
referencing a	n unknown certificate (CERT_TS_F_AT)
ensure that	
when	
the IUT is requested	to send a secured CAM
then	
the IUT sends a mes	sage of type EtsiTs103097Data
containing headerl	nfo
containing inline	
	ishedld3 value
indicating la	ast 3 octets of DIGEST_F

TP ld	P_SEC_ITSS_SND_CAM_1	1_BV_ <b>XX</b>			
C	Check that the IUT sends certificate request when it receives secured CAM containing				
	certificate signed by unknown AA certificate				
E	TSI TS 103 097 [1], clause 7				
	EEE Std 1609.2 [2], clauses 6				
	ICS GN SECURITY				
PICS Selection A	ND PICS_SEC_P2P_AA_DI	STRIBUTION			
A	ND <b>X_PICS</b>				
	Expected	d behaviour			
with					
the IUT is authorized with A	AT certificate (CERT_IUT_A_/	AT)			
and the IUT has receiving a	a message of type EtsiTs1030	097Data			
containing signer					
containing certificate					
containing issuer					
containing X_FIE					
indicating Hasl	indicating HashedId8 value DIGEST_F				
referencing	an unknown certificate (X_CI	E <b>RT</b> CERT_TS_F_AT)			
ensure that					
when					
the IUT is requested to s	end secured CAM				
then					
	e of type EtsiTs103097Data				
containing signedData	1				
containing tbsData					
containing heade					
containing inlineP2pcdRequest					
	lashedid3 value				
containing H					
	last 3 octets of DIGEST_F				
indicating	last 3 octets of DIGEST_F Permut	ation table			
indicating XX	l last 3 octets of DIGEST_F Permut X_FIELD_1	X_CERT	X_PICS		
indicating XX	l last 3 octets of DIGEST_F Permut X_FIELD_1		X_PICS		

TP ld	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 and 8.2.4.2.3	
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_P2P_AT_DISTRIBUTION	
	Expected behaviour	
with		
	ed with AT certificate (CERT_IUT_A_AT)	
and the IUT is conf	igured to send more than one CAM per second	
	already sent secured CAM	
containing signer	r	
containing cer	tificate	
at TIME_1		
and the IUT having received a secured CAM		
containing heade	erInfo	
containing inli	neP2pcdRequest	
containing H		
	g value HASHED_ID_3	
indicating last 3 octets of currently used AT certificate		
_ `	E_1 < TIME_2 < TIME_1+1 sec)	
ensure that		
when		
the IUT is requested to send a CAM		
= \	ME_1 < TIME_2 < TIME_3 < TIME_1+1 sec)	
then		
	SecuredMessage of type EtsiTs103097Data	
containing sig		
	ing certificate ed by the HashedId3 value <b>HASHED_ID_3</b>	

20

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

TP ld	TP_SEC_ITSS_SND_CAM_13_BV	
	Check that IUT sends the secured CAM containing the AA certificate in the	
Summary	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 and 8.2.4.2.3	
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_P2P_AT_DISTRIBUTION	
	Expected behaviour	
with		
the IUT is authorized	d with AT certificate (CERT_IUT_A_AT)	
	certificate (CERT_IUT_A_AA)	
	gured to send more than one CAM per second	
and the IUT having a	already sent a secured CAM	
containing signer		
containing certi	ficate	
at TIME_1 and the IUT having received a secured CAM		
	eP2pcdRequest	
containing HashedId3 value		
indicating last 3 octets of the digest of CERT_IUT_A_AA		
	_1 < TIME_2 < TIME_1+1 sec)	
ensure that		
when		
the IUT is requested to send a secured CAM		
- `	1E_1 < TIME_2 < TIME_3 < TIME_1+1 sec)	
then		
	SecuredMessage of type EtsiTs103097Data	
containing header		
	lestedCertificate	
indicating red	quested AA certificate CERT_IUT_A_AA	

21

### 6.2.2.9 Check that IUT sends AA certificate when requested

TP ld	TP_SEC_ITSS_SND_CAM_14_BV
	Check that IUT sends the secured CAM containing the AA certificate in the
C	requestedCertificate headerInfo field when it received a CAM containing a request for
Summary	unrecognized certificate that matches with the known AA certificate ID which is not currently
	used by the IUT
D	ETSI TS 103 097 [1], clause 7.1.1
Reference	IEEE Std 1609.2 [2], clauses 6.3.9 and 8.2.4.2.3
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_P2P_AA_DISTRIBUTION
	Expected behaviour
with	
	d with AT certificate (CERT_IUT_A_AT)
	gured to send more than one CAM per second
	gured to know the AA certificate (CERT_IUT_A_N_AA)
and the IUT has alread	eady sent secured CAM
containing sigr	19ľ
containing c	ertificate
at TIME_1	
	received a secured CAM
containing heade	
	neP2pcdRequest
	łashedld3 value
	last 3 octets of the digest of CERT_IUT_A_N_AA
	s not an issuer of currently used AT certificate
at TIME_2 (TIME	_1 < TIME_2 < TIME_1+1 sec)
ensure that	
when	
	ted to send a secured CAM
at TIME_3 (TI	ME_1 < TIME_2 < TIME_3 < TIME_1+1 sec)
then	
	SecuredMessage of type EtsiTs103097Data
containing hea	
•	equestedCertificate
indicating	requested AA certificate (CERT_IUT_A_N_AA)

TP ld	TP_SEC_ITSS_SND_CAM_15_BV	
	Check that the IUT does not send a secured CAM containing the AA certificate in the	
Summary	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	
Relefence	IEEE Std 1609.2 [2], clauses 6.3.9 and 8.2.4.2.3	
PICS Selection	PICS_GN_SECURITY, PICS_SEC_P2P_AA_DISTRIBUTION	
	Expected behaviour	
with		
the IUT is authorized	d with AT certificate (CERT_IUT_A_AT)	
	certificate (CERT_IUT_A_AA)	
and the IUT is config	gured to send more than one CAM per second	
	already sent secured CAM	
containing signer		
containing cert	ificate	
at TIME_1		
and the IUT having	received a secured CAM	
containing headerInfo		
containing inlineP2pcdRequest		
containing H	lashedId3 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 re-	quested 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		
	SecuredMessage of type EtsiTs103097Data	
containing head		
does not cor	ntain requestedCertificate	

TP ld	TP_SEC_ITSS_SND_CAM_16_BV			
C	Check that the IUT does not send a secured CAM containing the AA certificate in the			
Summary	requestedCertificate headerInfo field when it contains certificate in the signer field			
Reference	ETSI TS 103 097 [1], clause 7.1.1			
Reference	IEEE Std 1609.2 [2], clauses 6.3.9 and 8.2.4.2.3			
PICS Selection	PICS_GN_SECURITY, PICS_SEC_P2P_AA_DISTRIBUTION			
	Expected behaviour			
with				
the IUT is authorized	d with AT certificate (CERT_IUT_A_AT)			
issued by the AA	certificate (CERT_IUT_A_AA)			
	gured to send more than one CAM per second			
	already sent a secured CAM			
containing signer				
	containing certificate			
	at TIME_1			
and the IUT having received a SecuredMessage				
containing headerInfo				
0	eP2pcdRequest			
	ashedId3 value			
indicating last 3 octets of the digest of CERT_IUT_A_AA				
at TIME_2 (TIME2 =	IIME_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 ULT conde a Secured Massage of type EtciTe 102007 Deta				
the IUT sends a SecuredMessage of type EtsiTs103097Data				
	containing signer containing certificate			
9	and containing headerInfo not containing requestedCertificate			

TP ld	TP_SEC_ITSS_SND_CAM_17_BV		
	Check that the IUT sends a secured CAM containing the AA certificate in the		
Summary	requestedCertificate headerInfo field with the next CAM containing digest as a signer info		
	ETSI TS 103 097 [1], clause 7.1.1		
Reference	IEEE Std 1609.2 [2], clauses 6.3.9 and 8.2.4.2.3		
PICS Selection	PICS_GN_SECURITY, PICS_SEC_P2P_AA_DISTRIBUTION		
	Expected behaviour		
with			
	h AT partificate (CEDT IIIT A AT)		
	h AT certificate (CERT_IUT_A_AT) ficate (CERT_IUT_A_AA)		
	d to send more than one CAM per second		
and the IUT having alrea			
5	ady sent sectired CAW		
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	$3.3360 < 11012 < 11012_1 + 1360$		
when			
	ret subsequent secured CAM		
the IUT is sending a first subsequent secured CAM containing signer			
containing signer			
then			
this message			
containing headerlr	nfo		
containing reque			
0 1	lested AA certificate CERT_IUT_A_AA		

TP ld	TP_SEC_ITSS_SND_CAM_18_BV		
	Check that IUT sends the secured CAM containing generation time and this time is inside		
Summary	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		
Reference	EEE Std 1609.2 [2], clauses 5.2.3.2.2, 5.2.4.2.2 and 5.2.4.2.3		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT is authorized with	n AT certificate (CERT_IUT_A_AT)		
ensure that			
when			
the IUT is requested to	) send CAM		
containing certificate	containing certificate		
then			
	redMessage of type EtsiTs103097Data		
containing headerIn	fo		
containing genera	ationTime		
indicating GEN	I_TIME (CUR_TIME - 5 min <= GEN_TIME <= CUR_TIME + 5 min)		
	and containing signer		
containing certific	containing certificate		
containing toBeSigned			
	containing validityPeriod		
	containing start		
indicati	indicating value X_START_VALIDITY (X_START_VALIDITY <= GEN_TIME)		
	ining duration		
indicating value > GEN_TIME - X_START_VALIDITY			

### 6.2.2.10 Check generation time

### 6.2.2.11 Check payload

TP ld	TP_SEC_ITSS_SND_CAM_19_BV		
Summary	Check that IUT sends the secured CAM containing the 'data' field in signed data payload,		
Summary	containing the EtsiTs103097Data of type unsecured, contained the CAM payload		
Reference	ETSI TS 103 097 [1], clauses 5.2 and 7.1.1		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT is authorized	d with AT certificate (CERT_IUT_A_AT)		
ensure that			
when			
the IUT is request	ed to send a secured CAM		
then			
the IUT sends a m	nessage of type EtsiTs103097Data		
contains conter	nt		
contains sign	iedData		
containing	tbsData		
containi	ing payload		
containing data			
cor	containing content		
(	containing unsecuredData		
	containing not-empty data		

26

TP ld	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		
Relefence	IEEE Std 1609.2 [2], clause 5.2.3.2.2		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT is authorize	d with AT certificate (CERT_IUT_A_AT)		
ensure that			
when			
the IUT is reques	the IUT is requested to send a secured CAM		
then			
the IUT sends a	message of type EtsiTs103097Data		
containing sigr	ner		
containing o	zertificate		
containin	g appPermissions		
	ning an item of type PsidSsp		
cont	aining psid = AID_CAM		

### 6.2.2.12 Check signing permissions

## 6.2.2.13 Check signature

TP lo	1	TP_SEC_ITSS_SND_C/	AM 21 BV <b>XX</b>		
	Check that IUT sends the secured CAM containing signature				
Summary Check that the signature is calculated over the right fields and using right hash algorith					
cryptographically verifying the signature					
		ETSI TS 103 097 [1], cla			
Rete			uses 5.3.1, 6.3.4, 6.3.29, 6.3.30 ar	nd 6.3.31	
PICS	Selection	PICS_GN_SECURITY A	ND X_PICS		
		Ex	pected behaviour		
with					
the	e IUT is authorized with	AT certificate (X_CERT	IFICATE)		
	containing verifyKeyInc				
	containing verificatio				
	containing X_KEY	/			
	indicating KEY				
	re that				
	the IUT is requested to	send a secured CAM			
the			Data		
	containing signedDa	ge of type EtsiTs103097	Data		
	containing signer	la			
	containing dige	et			
		he certificate X_CERTIFI	CATE		
	or containing ce		UNIT E		
		CERTIFICATE			
	and containing sig				
containing X_SIGNATURE					
verifiable using KEY					
Permutation table					
XX X_CERTIFICATE X_KEY X_SIGNATURE X_PICS					
Α	CERT_IUT_A_AT	ecdsaNistP256	ecdsaNistP256Signature		
			PICS_SEC_BRAINPOOL_P256 R1		
с	CERT_IUT_A_B3_AT	ecdsaBrainpoolP384r1	ecdsaBrainpoolP384r1Signature	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384 R1	

TP lo	1	TP_SEC_ITSS_SND_CAM_22_BV_XX			
	mmary Check that IUT sends the secured CAM containing signature containing the ECC poir				
type set to either compressed_lsb_y_0, compressed_lsb_y_1 or x_coordinate_only					
Dofo		ETSI TS 103 097 [1], clauses 5.2, 7.1.1	· · · · ·		
IEEE Std 1609.2 [2], clauses 6.3.30 and 6.3.31					
PICS	Selection	PICS_GN_SECURITY AND X_PICS			
		Expected behaviour			
with					
the	e IUT is authorized with	AT certificate (X_CERTIFICATE)			
ensu	re that				
wh	ien				
	the IUT is requested to	send a secured CAM			
the					
		ge of type EtsiTs103097Data			
	containing signedDa				
	containing signatu				
	containing X_SI				
	containing rSi				
	containing:				
		ng compressed-y-0			
		ng compressed-y-1 Permutation table			
XX     X_CERTIFICATE     X_SIGNATURE     X_PICS					
	CERT_IUT_A_AT	ecdsaNistP256Signature			
		ecdsaBrainpoolP256r1Signature	PICS_SEC_BRAINPOOL_P256R1		
		ecdsaBrainpoolP384r1Signature	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1		

### 6.2.2.14 Check support for certificate content

TP ld	TP_SEC_ITSS_SND_CAM_23_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 authorize	d with AT certificate (CERT_IUT_A_AT_A8)		
containing toBeS	igned		
containing app			
	containing 8 entries		
	the last item		
containing psid			
indicating the 'AID_CAM'			
ensure that			
when			
	ted to send a secured CAM		
then			
	nessage of type EtsiTs103097Data		
containing con			
containing s			
containing tbsData			
	ing headerInfo		
	containing psid		
In	dicating 'AID_CAM'		

TP ld	TP_SEC_ITSS_SND_CAM_24_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			
	n AT certificate (CERT_IUT_A_AT_A8)		
containing appPermiss			
conformed to the ce			
	e (CERT_IUT_A_AA_A8)		
containing toBeSign			
containing certIss			
	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 h			
containing			
indicating 'AID_CAM'			

### 6.2.2.15 Check certificate consistency conditions

TP ld	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 authoriz	ed with AT certificate (CERT_IUT_C1_AT)	
containing region		
containing regio	n	
0 0		
indicating rec	n tangular region ning current IUT position	
indicating rec not contain	tangular region	
indicating rec not contain and the IUT has no	tangular region ing current IUT position	
indicating rec not contain and the IUT has no	tangular region ing current IUT position	
indicating rec not contain and the IUT has no ensure that when	tangular region ing current IUT position o other installed AT certificates	
indicating rec not contain and the IUT has no ensure that when	tangular region ing current IUT position	

TP ld	TP_SEC_ITSS_SND_CAM_24_BV	
	Check that IUT does not send the secured CAM if IUT is configured to use an AT	
Summary	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 a	uthorized with the AT certificate (CERT_IUT_CA3_AT)	
not containing re	gion	
and issued by the	AA certificate (CERT_IUT_C3_AA)	
containing reg	ion	
indicating re	indicating rectangular region	
not conta	ining current IUT position	
ensure that		
when		
the IUT is requested to send a secured CAM		
then		
the IUT does not send CAM		

TP ld	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
containing validityPerio	ration < CURRENT_TIME installed AT certificates o send a secured CAM

TP ld	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 containing validityPe indicating start > 0 and the IUT has no other ensure that when the IUT is requested to then the IUT does not send	CURRENT_TIME installed AT certificates o send a secured CAM

TP ld	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 authorize	ed with AT certificate (CERT_IUT_A3_AT)
containing appP	ermissions
not containing	PsidSSP
containing	bsid
indicating	AID_CAM
and the IUT has no	other installed AT certificates
ensure that	
when	
the IUT is reques	sted 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 ld	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
ensure that when	

#### 6.2.3.2 Check secured DENM AID value

TP ld	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 ensure that	AT certificate (CERT_IUT_A_AT)		
when			
the IUT is requested to	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'			

TP Id	TP_SEC_ITSS_SND_DENM_03_BV	
	Check that IUT sends the secured DENM with the HeaderInfo containing generationTime	
Summary	and generationLocation and does not contain expiryTime, encryptionKey,	
cumu,	p2pcdLearningRequest, missingCrlIdentifier, inlineP2pcdRequest, requestedCertificate	
Reference	ETSI TS 103 097 [1], clauses 5.2 and 7.1.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
	d with AT certificate (CERT_IUT_A_AT)	
ensure that		
when		
the IUT is reques	ted to send a secured DENM	
then		
the IUT sends a EtsiTs103097Data		
containing content		
containing s		
containing		
	ing headerInfo	
containing generationTime		
and containing generationLocation,		
and not containing expiryTime		
and not containing encryptionKey		
	not containing p2pcdLearningRequest	
	not containing missingCrIIdentifier not containing inlineP2pcdRequest	
	not containing requestedCertificate	
anu		

#### 6.2.3.3 Check header fields

### 6.2.3.4 Check signer information

TP ld	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	d with AT certificate (CERT_IUT_A_AT)		
ensure that			
when			
the IUT is request	ed to send a secured DENM		
then			
the IUT sends a E	the IUT sends a EtsiTs103097Data		
containing cont	ent		
containing si			
containing			
	containing certificate		
containing toBeSigned			
containing appPermissions			
containing the item of type PsidSsp			
	containing psid		
	indicating AID_DENM		
L			

TP ld	TP_SEC_ITSS_SND_DENM_05_BV	
	Check that IUT sends the secured DENM containing generation time and this time is inside	
Summary	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 and 5.2.4.2.3	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT is authorized with	n 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 genera		
indicating GEN_TIME (CUR_TIME - 10min <= GEN_TIME <= CUR_TIME + 10 min)		
and containing signer		
containing certificate		
containing toBeSigned		
containing validityPeriod		
containing start		
	ng value X_START_VALIDITY (X_START_VALIDITY <= GEN_TIME)	
	ining duration	
indicating value > GEN_TIME - X_START_VALIDITY		

### 6.2.3.5 Check generation time

### 6.2.3.6 Check generation location

TP ld	TP_SEC_ITSS_SND_DENM_06_BV		
0	Check that IUT sends the secured DENM containing generation location when signing		
Summary	certificate chain does not have any region restriction		
Deference	ETSI TS 103 097 [1], clause 7.1.2		
Reference	IEEE Std 1609.2 [2], clause 5.2.3.2.2		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_CERTIFICATE_SELECTION		
	Expected behaviour		
with			
	thorized with the AT certificate (CERT_IUT_A_AT)		
containing toBeSi			
not containing r			
and issued by the certificate AA (CERT_IUT_A_AA) containing toBeSigned			
			not containin
	he certificate RCA (CERT_IUT_A_RCA)		
containing toBeSigned			
not containing region			
ensure that			
when			
	ed to send a secured DENM		
	then		
the IUT sends a message of type EtsiTs103097Data			
containing headerInfo containing generationLocation			
containing ge			

TP Id		TP_SEC_ITSS_SND_DENM_07_E	3V <b>XX</b>	
<b>.</b>		Check that IUT sends the secured DENM containing generation location which is inside		
Summary		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 S	Selection	PICS_GN_SECURITY AND PICS_	SEC_CERTIFICATE_SELECTION AND X_PICS	
		Expected beh	aviour	
with				
the	IUT has been authori:	zed with the AT certificate (X_AT_C	ERTIFICATE)	
C	ontaining toBeSigned			
	containing region			
	containing X_FIE			
	indicating REG	ION		
ensure				
whe				
	•	send a secured DENM		
then		an of two EtciTo102007Date		
u	containing headerIn	age of type EtsiTs103097Data		
	containing neaderning			
		e inside the REGION		
	indicating value	Permutation	Table	
_XX	X_FIELD	X_AT_CERTIFICATE	X_PICS	
В	circularRegion	CERT_IUT_B_AT	PICS_SEC_CIRCULAR_REGION	
С	rectangularRegion	CERT_IUT_C_AT	PICS_SEC_RECTANGULAR_REGION	
D	polygonalRegion	CERT_IUT_D_AT	PICS_SEC_POLYGONAL_REGION	
Е	identifiedRegion	CERT_IUT_E_AT	PICS_SEC_IDENTIFIED_REGION	

TP ld	TP_SEC_ITSS_SND_DENM_09_BV		
	Check that IUT sends the secured DENM containing generation location which is inside		
Summary	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		
Kelelelice	IEEE Std 1609.2 [2], clauses 5.2.3.2.2 and 6.4.8		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_CERTIFICATE_SELECTION		
	Expected behaviour		
with			
the IUT has been authori	zed 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 RI	EGION		
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		
	e inside the REGION		

TP ld	TP_SEC_ITSS_SND_DENM_10_BV		
	Check that IUT sends the secured DENM containing generation location which is inside		
Summary	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		
Kelerence	IEEE Std 1609.2 [2], clauses 5.2.3.2.2 and 6.4.8		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_CERTIFICATE_SELECTION		
	Expected behaviour		
with			
the IUT has been authori	ized with the AT certificate (CERT_IUT_CA2_AT)		
containing toBeSigned			
not containing regio			
	and issued by the certificate AA (CERT_IUT_CA_AA)		
containing toBeSigned			
not containing region			
and issued by the ce	ertificate RCA (CERT_IUT_C_RCA)		
	containing toBeSigned		
containing circularRegion			
indicating REGION			
ensure that			
when			
•	the IUT is requested to send a secured DENM		
	the IUT sends a message of type EtsiTs103097Data		
•	containing headerInfo		
containing generationLocation			
indicating value inside the REGION			

### 6.2.3.7 Check payload

TP ld	TP SEC ITSS SND DENM 11 BV		
-	Check that IUT sends the secured DENM containing the 'data' field in signed data payload,		
Summary	containing the EtsiTs103097Data of type unsecured, contained the DENM payload		
Reference ETSI TS 103 097 [1], clauses 5.2 and 7.1.2			
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT has been a	uthorized with the AT certificate (CERT_IUT_A_AT)		
ensure that			
when			
the IUT is requested to send a secured DENM			
then			
	essage of type EtsiTs103097Data		
contains content			
contains signedData			
containing tbsData			
	containing payload		
containing data			
	containing content		
C	containing unsecuredData		
	containing not-empty data		

[			
TP ld	TP_SEC_ITSS_SND_DENM_12_BV		
Summers.	Check that the IUT sends the secured DENM signed with the certificate containing		
Summary	appPermissions allowing to sign DEN messages		
Reference	ETSI TS 103 097 [1], clause 7.1.2		
Reference	IEEE Std 1609.2 [2], clause 5.2.3.2.2		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT has been author	zed with the AT certificate (CERT_IUT_A_AT)		
ensure that	ensure that		
when			
the IUT is requested to	o send a secured DENM		
then			
the IUT sends a message of type EtsiTs103097Data			
containing signer	0 71		
containing certific	containing certificate		
containing appPermissions			
containing a	containing an item of type PsidSsp		
containing	containing psid		
indicating AID_DENM			

### 6.2.3.8 Check signing permissions

#### 6.2.3.9 Check signature

TP le	d	TP_SEC_ITSS_SND_D	ENM 13 BV		
			e secured DENM containing signate	ure	
Summary		Check that the signature is calculated over the right fields and using right hash algorithm			
		by cryptographically verifying the signature			
Defe		ETSI TS 103 097 [1], cla			
Reference		IEEE Std 1609.2 [2], cla	uses 5.3.1, 6.3.4, 6.3.29, 6.3.30 and	d 6.3.31	
PICS	6 Selection	PICS_GN_SECURITY A	AND <b>X_PICS</b>		
		Expe	cted behaviour		
with					
th		AT certificate (X_CERTIF	ICATE)		
	containing verifyKeyIndi				
	containing verification	Кеу			
	containing X_KEY				
one	indicating KEY				
	hen				
VVI	the IUT is requested to a	send a secured DENM			
th	en				
	the IUT sends a messad	e of type EtsiTs103097D	ata		
	containing signedData				
	containing signer				
	containing certifi	cate			
		CERTIFICATE			
		verifyKeyIndicator			
		g verificationKey			
	containing <b>X_KEY</b>				
		cating KEY			
	and containing signature				
	containing <b>X_SIGNATURE</b> verifiable using KEY				
			nutation table		
ΧХ	X_CERTIFICATE	X_KEY	X_SIGNATURE	X_PICS	
А	CERT_IUT_A_AT	ecdsaNistP256	ecdsaNistP256Signature		
В	CERT_IUT_A_B_AT	ecdsaBrainpoolP256r1	ecdsaBrainpoolP256r1Signature	PICS_SEC_BRAINPOOL_P 256R1	
С	CERT_IUT_A_B3_AT	ecdsaBrainpoolP384r1	ecdsaBrainpoolP384r1Signature	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P 384R1	

TP ld	TP_SEC_ITSS_SND_DENM_14_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		
	ed with AT certificate (CERT_IUT_C_AT_8)	
containing toBeS		
containing reg		
0	ectangularRegion	
containing 8 entries containing an entry (ENTRY)		
ensure that		
when the ILIT is reques	sted to send a secured DENM	
then	seu lo seria a securea DENNI	
	message of type EtsiTs103097Data	
containing headerInfo		
•	generationLocation	
	position inside the <b>ENTRY</b>	

### 6.2.3.10 Check support for certificate content

TP ld	TP_SEC_ITSS_SND_DENM_15_BV	
Summory	Check that the IUT supports at least 8 points in the polygonal certificate validity region in	
Summary	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 toBeSig		
containing region		
containing polygonalRegion containing 8 entries		
· · · · ·	n is inside the polygon <b>P</b>	
ensure that		
when		
	ed to send a secured DENM	
then	accesses of type EtciTc102007Data	
the IUT sends a message of type EtsiTs103097Data		
0	containing headerInfo containing generationLocation	
indicating position inside the <b>P</b>		
indicating		
TP ld	TP_SEC_ITSS_SND_DENM_16_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	n AT certificate (CERT_IUT_E_AT_8)	
containing toBeSigned		
containing region		
containing identifi	edRegion	
containing 8 er	ntries	
containing o	ne of the items ( <i>I</i> )	
containing	current IUT position	
ensure that		
when		
the IUT is requested to send a secured DENM		
then		
the IUT sends a mess	age of type EtsiTs103097Data	
containing headerIn	fo	
containing genera	ationLocation	
indicating posit	ion inside the I	

### 6.2.3.11 Check certificate consistency conditions

TP ld	TP_SEC_ITSS_SND_DENM_17_BV
C	Check that IUT does not send secured DENMs if IUT does not possess an AT certificate
Summary	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 a	authorized with the AT certificate CERT_IUT_C1_AT)
containing regior	n
	tangular region
	ing current IUT position
ensure that	
when	
the IUT is reque	
	sted to send a secured DENM
then	sted to send a secured DENM

TP ld	TP_SEC_ITSS_SND_DENM_18_BV
	Check that IUT does not send the secured DENM if IUT is configured to use an AT
Summary	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 a	authorized with the AT certificate (CERT_IUT_CA3_AT)
not containing re	egion
and issued by th	e AA certificate (CERT_IUT_C3_AA)
containing reg	jion
indicating r	ectangular region
not conta	aining current IUT position
ensure that	
when	
the IUT is reque	sted to send a secured DENM
then	

TP ld	TP SEC ITSS SND DENM 19 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
containing validityPer indicating start + du and the IUT has no othe ensure that when	uration < CURRENT_TIME r installed AT certificates o send a secured DENM

TP ld	TP_SEC_ITSS_SND_DENM_20_BV
6	Check that IUT does not send secured DENMs if all AT certificates installed on the IUT
Summary	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 a	uthorized with the AT certificate (CERT_IUT_A2_AT)
containing validit	tyPeriod
indicating star	t > CURRENT_TIME
and IUT has no oth	er certificates installed
ensure that	
when	
the IUT is requested to send a secured DENM	
then	
the IUT does not	t send DENM

TP ld	TP_SEC_ITSS_SND_DENM_21_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
containing appPermiss not containing PsidS containing psid indicating AID_ and IUT has no other cer ensure that when	SSP DENM tificates installed o send a secured DENM

## 6.2.4 Generic signed message profile

#### 6.2.4.1 Check that secured message is signed

TP ld	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		
ensure that when the IUT is requested to then	n AT certificate (CERT_IUT_A_AT) o send a secured Beacon age of type EtsiTs103097Data Data		

#### 6.2.4.2 Check secured AID value

TP ld	TP_SEC_ITSS_SND_GENMSG_02_BV
S	Check that the sent Secured Message contains HeaderField its_aid that is set to other
Summary	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 requeste	d to send a secured Beacon
then	
the IUT sends a me	essage of type EtsiTs103097Data
containing conte	
containing sig	
containing t	
	g headerInfo
	ning psid
indi	cating AID_GNMGMT

#### 6.2.4.3 Check header field

TP ld	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 and 7.1.3
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER
	Expected behaviour
with	
the IUT is authorized wit	th AT certificate (CERT_IUT_A_AT)
ensure that	
when	
the IUT is requested t	o send a secured Beacon
then	
	sage of type EtsiTs103097Data
containing content	
containing signed	
containing tbs	
containing h	
	g generationTime
	containing expiryTime
	containing generationLocation
	containing p2pcdLearningRequest
and not c	containing missingCrlldentifier

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

TP ld	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 and 7.1.3
Reference	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 requeste	d to send a secured Beacon
then	
the IUT sends a me	essage of type EtsiTs103097Data
containing conte	
containing sig	nedData
containing s	
containin	
	ning certificate
	ning toBeSigned
	aining appPermissions
CC	ontaining the item of type PsidSsp
	containing psid
	indicating AID_GNMGMT

TP ld	TP_SEC_ITSS_SND_GENMSG_05_BV
	Check that IUT sends the secured GeoNetworking message containing generation time
Summary	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 authorize	d with AT certificate (CERT_IUT_A_AT)
ensure that	
when	
the IUT is reques	ted to send a secured Beacon
containing cert	ificate
then	
the IUT sends a	message of type EtsiTs103097Data
containing hea	derInfo
containing g	enerationTime
indicating	GEN_TIME (CUR_TIME - 10 min <= GEN_TIME <= CUR_TIME + 10 min)
and containing	signer
containing c	
	g toBeSigned
contair	ing validityPeriod
cont	aining start
	dicating value X_START_VALIDITY (X_START_VALIDITY <= GEN_TIME)
and	containing duration
in	dicating value > GEN_TIME - X_START_VALIDITY

### 6.2.4.5 Check generation time

## 6.2.4.6 Check payload

TP ld	TP_SEC_ITSS_SND_GENMSG_06_BV
	Check that IUT sends the secured message using the 'data' field in signed data payload,
Summary	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 w	ith AT certificate (CERT_IUT_A_AT)
ensure that	
when	
the IUT is requested	to send a secured Beacon
then	
the IUT sends a mes	sage of type EtsiTs103097Data
contains content	
contains signed	Data
containing the	sData
containing	payload
containi	
	ining content
	ntaining unsecuredData
	containing not-empty data

TP ld	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 au	uthorized with the AT certificate (CERT_IUT_A_AT)	
ensure that		
when		
the IUT is reques	ted to send Beacon	
then		
the IUT sends a r	nessage of type EtsiTs103097Data	
containing sigr	ier	
containing c	ertificate	
	g appPermissions	
	containing an item of type PsidSsp	
	aining psid	
ind	dicating value AID_GNMGMT	

42

### 6.2.4.7 Check signing permissions

### 6.2.4.8 Check signature

TP l	d	TP_SEC_ITSS_SND_G		
			ne secured GeoNetworking message	e containing signature
Summary		Check that the signature	e is calculated over the right fields a	
		by cryptographically ver		
Dofe	rence	ETSI TS 103 097 [1], cla	auses 5.2 and 7.1.3	
Refe			uses 5.3.1, 6.3.4, 6.3.29, 6.3.30 and	
PICS	Selection	PICS_GN_SECURITY /	AND PICS_SEC_ITS_AID_OTHER	AND <b>X_PICS</b>
		Expec	cted behaviour	
with				
th		T certificate (X_CERTIFIC	CATE)	
	containing verifyKeyIndic			
	containing verification	Key		
	containing X_KEY			
	indicating KEY			
	ire that			
W	nen			
	the IUT is requested to se	end a secured Beacon		
th	en			
		e of type EtsiTs103097Dat	ta	
	containing signedData			
	containing signer			
	containing digest	certificate X_CERTIFICA	TE	
	or containing cert		IE .	
	indicating X_C			
	and containing signa			
	containing X_SIG			
	verifiable using			
			nutation table	
XX	X_CERTIFICATE	X_KEY	X_SIGNATURE	X_PICS
Α	CERT_IUT_A_AT	ecdsaNistP256	ecdsaNistP256Signature	
В	CERT_IUT_A_B_AT	ecdsaBrainpoolP256r1	ecdsaBrainpoolP256r1Signature	PICS_SEC_BRAINPOOL_P 256R1
С	CERT_IUT_A_B3_AT	ecdsaBrainpoolP384r1	ecdsaBrainpoolP384r1Signature	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P 384R1

# 6.3 Receiving behaviour

# 6.3.1 Check the message protocol version

TP ld	TP_SEC_ITSS_RCV_MSG_01_BV
Summary	Check that IUT accepts a secured message containing protocol version set to a value 3
Reference	ETSI TS 103 097 [1], clause 5.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT is being auth	orized with the certificate CERT_IUT_A_AT
and the IUT current t	ime is inside the time validity period of CERT TS A AT and CERT IUT A AT
ensure that	
when	
the IUT is receiving	g a message of type EtsiTs103097Data
signed using CE	RT_TS_A_AT
and containing r	protocol_version
indicating 3	
01	

TP ld	TP_SEC_ITSS_RCV_MSG_01_BO
Summary	Check that IUT discards a secured message containing protocol version set to a value less
	than 3
Reference	ETSI TS 103 097 [1], clause 5.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT is being auth	orized with the certificate CERT_IUT_A_AT
and the IUT current ti	me is inside the time validity period of CERT_TS_A_AT and CERT_IUT_A_AT
ensure that	
when	
	g a message of type EtsiTs103097Data
signed using CE	
and containing p	protocol_version
indicating 2	
then	
the IUT discards th	e SecuredMessage

TP ld	TP_SEC_ITSS_RCV_MSG_02_BO
Summary	Check that IUT discards a secured message containing protocol version set to a value
	greater than 3
Reference	ETSI TS 103 097 [1], clause 5.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
0	thorized with the certificate CERT_IUT_A_AT t time is inside the time validity period of CERT_TS_A_AT and CERT_IUT_A_AT
signed using (	ing a message of type EtsiTs103097Data CERT_TS_A_AT g protocol_version
then	
the IUT discards	the SecuredMessage

# 6.3.2 CAM profile

TP ld	TP_SEC_ITSS_RCV_CAM_01_BV
Summary	Check that IUT accepts a valid secured CAM message signed with certificate
Reference	ETSI TS 103 097 [1], clause 7.1.1
PICS Selection	PICS GN SECURITY
	Expected behaviour
with	
the IUT being in the 'aut	horized' state
5	e (CUR_TIME) is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receiving a	a message of type EtsiTs103097Data (MSG)
containing protoc	
indicating 3	
and containing co	ontent.signedData
containing ha	shid
	hash algorithm of the verification key of CERT_TS_A_AT
and containin	
containing	
	ning data
COI	ntaining protocolVersion
	indicating 3
an	d containing content.unsecuredData
and conta	containing CAM payload ining headerInfo
	ning psid
	licating CAM AID value
	ontaining generationTime
	licating time within 2sec around the CUR_TIME
	OT containing other headers
and containin	g signer
containing	certificate
	ning 1 item of type EtsiTs103097Certificate
	licating CERT_TS_A_AT
and containin	
	ecdsaNistP256Signature
	ning rSig.x-only
	l over the MSG.content.signedData.tbsData
then	verification key of CERT_TS_A_AT
the IUT accepts the	SecuredMessage

### 6.3.2.1 Check the valid message receiving

TP ld	TP_SEC_ITSS_RCV_CAM_02_BV
Summary	Check that IUT accepts a valid secured CAM message signed with digest
Reference	ETSI TS 103 097 [1], clause 7.1.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'au	thorized' state
and the IUT current tim	e (CUR_TIME) is inside the time validity period of CERT_TS_A_AT
and the IUT has alread	y received the message signed with CERT_TS_A_AT
ensure that	
when	
the IUT is receiving	a message of type EtsiTs103097Data
indicating the m	essage described in TP_SEC_ITSS_RCV_CAM_01_BV
	content.signedData.signer
containing di	gest
indicating	HashedId8 value
	encing the CERT_TS_A_AT
then	-
the IUT accepts the	SecuredMessage

TP ld	TP_SEC_ITSS_RCV_CAM_03_BV
Summary	Check that IUT accepts a valid secured CAM message signed with compressed signature
Reference	ETSI TS 103 097 [1], clause 7.1.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'au	thorized' state
and the IUT current tim	e (CUR_TIME) is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
	a message of type EtsiTs103097Data (MSG)
indicating the m	essage described in TP_SEC_ITSS_RCV_CAM_01_BV
and containing c	content.signedData.signature
containing e	cdsaNistP256Signature
containin	g rSig.compressed-y-0
or contai	ning rSig.compressed-y-1
calculated ov	ver the MSG.content.signedData.tbsData
using ver	ification key of CERT_TS_A_AT
then	
the UIT eccepte the	Conversion

45

the IUT accepts the SecuredMessage

TP ld		VV
	TP_SEC_ITSS_RCV_CAM_04_BV	
		red CAM message signed with certificate containing
-	region restriction	
	ETSI TS 103 097 [1], clause 7.1.1	
PICS Selection	PICS_GN_SECURITY AND X_PIC	
	Expected beh	naviour
with		
the IUT being in the 'auth		
	(CUR_TIME) is inside the time valid	
ensure that	ion is inside the region restriction of	X_AI_CERTIFICATE
when		
	message of type EtsiTs103097Dat	a (MSG)
	ssage described in TP_SEC_ITSS_	
and containing co		
containing sig		
containing		
	ing 1 item of type EtsiTs103097Cer	tificate
	cating X_AT_CERTIFICATE	
	containing toBeSigned.region	
	containing X_FIELD	
and containing		
	ecdsaNistP256Signature	
	ing rSig.x-only over the MSG.content.signedData.t	heDete
	erification key of X_AT_CERTIFICA	
then		
the IUT accepts the S	SecuredMessage	
	Permutation	Table
_XX X_FIELD	X_AT_CERTIFICATE	X_PICS
01 circularRegion	CERT_TS_B_AT	PICS_SEC_CIRCULAR_REGION
02 rectangularRegion	CERT_TS_C_AT	PICS_SEC_RECTANGULAR_REGION
03 polygonalRegion	CERT_TS_D_AT	PICS_SEC_POLYGONAL_REGION

TP ld	TP_SEC_ITSS_RCV_CAM_05_BV
Summary	Check that IUT accepts a valid secured CAM message signed using the brainpoolP256r1
Caninary	algorithm
Reference ETSI TS 103 097 [1], clause 7.1.1	
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_BRAINPOOL_P256R1
	Expected behaviour
With	
the IUT being in the 'aut	horized' state
and the IUT current time	e (CUR_TIME) is inside the time validity period of CERT_TS_A_B_AT
ensure that	
when	
the IUT is receiving a	a message of type EtsiTs103097Data
indicating the me	ssage described in TP_SEC_ITSS_RCV_CAM_01_BV
and containing content.signedData	
containing sig	
	g certificate
	ning 1 item of type EtsiTs103097Certificate
ind	licating CERT_TS_A_B_AT
	containing toBeSigned.verifyKeyIndicator.verificationKey
	containing ecdsaBrainpoolP256r1
and containin	
	gecdsaBrainpoolP256r1Signature
containing rSig.x-only	
	l over the MSG.content.signedData.tbsData
	verification key of CERT_TS_A_B_AT
then	Converse Manager
the IUT accepts the	Securearivessage

TP ld	TP_SEC_ITSS_RCV_CAM_06_BV
Summary	Check that IUT accepts a valid secured CAM message signed using the brainpoolP384r1
Summary	algorithm
Reference ETSI TS 103 097 [1], clause 7.1.1	
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_BRAINPOOL_P384R1
	Expected behaviour
With	
the IUT being in the 'au	uthorized' state
and the IUT current tim	ne (CUR_TIME) is inside the time validity period of CERT_TS_A_B3_AT
ensure that	
when	
	a message of type EtsiTs103097Data
	nessage described in TP_SEC_ITSS_RCV_CAM_01_BV
	content.signedData
containing s	
	ng certificate
	aining 1 item of type EtsiTs103097Certificate
Ir	ndicating CERT_TS_A_B3_AT
	containing to BeSigned. verifyKeyIndicator.verificationKey
and contain	containing ecdsaBrainpoolP384r1
	ing signature ng ecdsaBrainpoolP384r1Signature
	aining rSig.x-only
	ed over the MSG.content.signedData.tbsData
	g verification key of CERT_TS_A_B3_AT
then	
the IUT accepts the	SecuredMessage

TP ld	TP_SEC_ITSS_RCV_CAM_01_BO
Summary	Check that IUT discards a secured CAM if the HeaderInfo contains the header field an invalid Psid value
Reference	ETSI TS 103 097 [1], clause 7.1.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivi	ng a message of type EtsiTs103097Data
	nessage described in TP_SEC_ITSS_RCV_CAM_02_BV
and containing	SignedData
containing T	oBeSignedData
containing	g HeaderInfo
contair	ing Psid
not	indicating CAM AID value
then	
the IUT discards	the SecuredMessage

#### 6.3.2.2 Check invalid HeaderInfo elements

TP ld	TP_SEC_ITSS_RCV_CAM_02_BO	
0	Check that IUT discards a secured CAM if the HeaderInfo contains the header field	
Summary	generationLocation	
Reference	ETSI TS 103 097 [1], clause 7.1.1	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
With		
the IUT being in the	e 'authorized' state	
and the IUT curren	t time is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
the IUT is receiv	ing a message of type EtsiTs103097Data	
containing Sig	nedData	
containing	ToBeSignedData	
containin	g HeaderInfo	
contaii	ning psid	
indi	cating CAM AID value	
and containing generationLocation		
then		
the IUT discards	the SecuredMessage	

TP ld	TP_SEC_ITSS_RCV_CAM_03_BO
Summari	Check that IUT discards a secured CAM if the HeaderInfo contains the header field
Summary	expiryTime
Reference	ETSI TS 103 097 [1], clause 7.1.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
With	
the IUT being in the and the IUT current ensure that when	'authorized' state time is inside the time validity period of CERT_TS_A_AT
the IUT is receiving	ng a message of type EtsiTs103097Data
containing Sigr	
	oBeSignedData
-	g HeaderInfo
	ing psid
indicating CAM AID value	
and containing expiryTime	
then	
the IUT discards	the SecuredMessage

TP ld	TP_SEC_ITSS_RCV_CAM_04_BO	
Summary	Check that IUT discards a secured CAM if the HeaderInfo contains the header field	
Summary	p2pcdLearningRequest	
Reference	ETSI TS 103 097 [1], clause 7.1.1	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
With		
the IUT being in the 'au	thorized' state	
and the IUT current time	e is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
the IUT is receiving a	a message of type EtsiTs103097Data	
containing Signed	Data	
containing ToBe	∋SignedData	
containing He	eaderInfo	
containing psid		
indicating CAM AID value		
and containing p2pcdLearningRequest		
then		
the IUT discards the	SecuredMessage	

TP ld	TP_SEC_ITSS_RCV_CAM_05_BO	
	Check that IUT discards a secured CAM if the HeaderInfo contains the header field	
Summary	missingCrIIdentifier	
Reference ETSI TS 103 097 [1], clause 7.1.1		
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
With		
the IUT being in the	e 'authorized' state	
and the IUT curren	t time is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
the IUT is receiv	ing a message of type EtsiTs103097Data	
containing Sig	unedData	
containing	ToBeSignedData	
containing HeaderInfo		
containing psid		
indicating CAM AID value		
and containing missingCrlldentifier		
41		
then		

TP ld	TP_SEC_ITSS_RCV_CAM_06_BO		
Summary	Check that IUT discards a secured CAM if the HeaderInfo contains the header field		
Summary	encryptionKey		
Reference	ETSI TS 103 097 [1], clause 7.1.1		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
With			
the IUT being in the 'aut	horized' state		
9	is inside the time validity period of CERT_TS_A_AT		
ensure that			
when			
the IUT is receiving a	the IUT is receiving a message of type EtsiTs103097Data		
containing SignedD			
containing ToBe			
containing Hea			
containing p			
indicating CAM AID value			
and containing encryptionKey			
then	ing energy ion reg		
	SecuredMacage		
the IUT discards the S	secureumessage		

## 6.3.2.3 Check invalid Signature elements

TP ld	TP_SEC_ITSS_RCV_CAM_07_BO
Summary	Check that IUT discards a secured CAM if the 'SignedData' contains an invalid signature algorithm
Reference	ETSI TS 103 097 [1], clause 6
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
the IUT being in the and the IUT curren ensure that when	t time is inside the time validity period of CERT_TS_A_AT
containing Sig containing S	
then	
the IUT discards	the SecuredMessage

TP ld	TP_SEC_ITSS_RCV_CAM_08_BO
Summary	Check that IUT discards a secured CAM if the 'SignerIdentifier' contains an invalid choice
Reference	ETSI TS 103 097 [1], clause 6
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the and the IUT current ensure that when	a 'authorized' state time is inside the time validity period of CERT_TS_A_AT
the IUT is receivi containing Sig	Signerldentifier
then	
the IUT discards	the SecuredMessage

TP ld	TP_SEC_ITSS_RCV_CAM_09_BO
Summary	Check that IUT discards a secured CAM if the Signature cannot be verified
Reference	ETSI TS 103 097 [1], clause 6
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
ensure that when the IUT is receive containing Sig indicating a then	t time is inside the time validity period of CERT_TS_A_AT

# 6.3.3 DENM profile

### 6.3.2.1 Check the valid message receiving

TP ld	TP_SEC_ITSS_RCV_DENM_01_BV	
	Check that IUT accepts a valid secured DENM message signed with certificate	
	ETSI TS 103 097 [1], clause 7.1.1	
PICS Selection PICS_GN_SECURITY		
	Expected behaviour	
with		
the IUT being in the 'auti	horized' state	
	(CUR_TIME) is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
	a message of type EtsiTs103097Data (MSG)	
containing protoc	olVersion	
indicating 3		
	ontent.signedData	
containing ha		
	hash algorithm of the verification key of CERT_TS_A_AT	
and containing	g tbsData	
containing		
	ning data	
Cor	ntaining protocolVersion indicating 3	
and	d containing content.unsecuredData	
and	containing DENM payload	
and contai	ining headerInfo	
	ning psid	
	icating DENM AID value	
	ntaining generationTime	
ind	icating time within 2sec around the CUR_TIME	
	ntaining generationLocation	
and NOT containing other headers		
and containing signer		
containing certificate		
containing 1 item of type EtsiTs103097Certificate		
	icating CERT_TS_A_AT	
and containing		
	ecdsaNistP256Signature	
	ning rSig.x-only l over the MSG.content.signedData.tbsData	
	verification key of CERT_TS_A_AT	
then		
the IUT accepts the S	SecuredMessage	

TP ld		TP_SEC_ITSS_RCV_DENM_02_B	V_ <b>XX</b>
Summary	2011	Check that IUT accepts a valid secu	ured DENM message signed with certificate containing
Summ	iai y	region restriction	
	eference ETSI TS 103 097 [1], clause 7.1.1		
PICS S	Selection	PICS_GN_SECURITY AND <b>X_PIC</b>	
		Expected beh	naviour
and ensure whe	d the IUT current position that en the IUT is receiving a indicating the mea and containing containing containing containing containing containing containing containing containing containing containing containing containing containing containing containing containing containing	(CUR_TIME) is inside the time valid tion is inside the region restriction of message of type EtsiTs103097Dat ssage described in TP_SEC_ITSS_ ontent.signedData Data headerInfo hing generationLocation icating location inside the X_AT_CA g signer certificate hing 1 item of type EtsiTs103097Cen icating X_AT_CERTIFICATE containing toBeSigned.region containing X_FIELD g signature ecdsaNistP256Signature hing rSig.x-only over the MSG.content.signedData.to verification key of X_AT_CERTIFICATE	a (MSG) RCV_DENM_01_BV ERTIFICATE region restriction rtificate
		Permutation	Table
_XX	X_FIELD	X_AT_CERTIFICATE	X_PICS
01	circularRegion	CERT_TS_B_AT	PICS_SEC_CIRCULAR_REGION
02	rectangularRegion	CERT_TS_C_AT	PICS_SEC_RECTANGULAR_REGION
03	polygonalRegion	CERT_TS_D_AT	PICS_SEC_POLYGONAL_REGION
04	identifiedRegion	CERT_TS_E_AT	PICS_SEC_IDENTIFIED_REGION

TP ld	TP_SEC_ITSS_RCV_DENM_03_BV	
Summary	Check that IUT accepts a valid secured DENM message signed using the brainpoolP256r1	
Summary	algorithm	
Reference ETSI TS 103 097 [1], clause 7.1.1		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_BRAINPOOL_P256R1	
	Expected behaviour	
With		
the IUT being in the 'auth	horized' state	
and the IUT current time	(CUR_TIME) is inside the time validity period of CERT_TS_A_B_AT	
ensure that		
when		
	a message of type EtsiTs103097Data (MSG)	
	ssage described in TP_SEC_ITSS_RCV_DENM_01_BV	
and containing content signedData		
containing sig		
	certificate	
	hing 1 item of type EtsiTs103097Certificate	
indicating CERT_TS_A_B_AT containing toBeSigned.verifyKeyIndicator.verificationKey		
containing to Besigned. Verny Reyndicator. Vernication Rey		
and containing signature		
containing ecdsaBrainpoolP256r1Signature		
containing rSig.x-only		
calculated over the MSG.content.signedData.tbsData		
using verification key of CERT_TS_A_B_AT		
then		
the IUT accepts the S	SecuredMessage	

TP ld	TP_SEC_ITSS_RCV_DENM_04_BV
Summary	Check that IUT accepts a valid secured DENM message signed using the brainpoolP384r1
Reference	algorithm ETSI TS 103 097 [1], clause 7.1.1
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_BRAINPOOL_P384R1
NA (: 4)-	Expected behaviour
With	
the IUT being in the	
	t time (CUR_TIME) is inside the time validity period of CERT_TS_A_B3_AT
ensure that	
when	
	ving a message of type EtsiTs103097Data (MSG)
	ne message described in TP_SEC_ITSS_RCV_DENM_01_BV
	ing content.signedData
	ng signer
	aining certificate
C	containing 1 item of type EtsiTs103097Certificate
	indicating CERT_TS_A_B3_AT
	containing toBeSigned. verifyKeyIndicator.verificationKey containing ecdsaBrainpoolP384r1
and can	taining signature
	aining signature aining ecdsaBrainpoolP384r1Signature
	containing rSig.x-only
	ulated over the MSG.content.signedData.tbsData
	ising verification key of CERT_TS_A_B3_AT
then	Bing vernication key of OLITI TO A DO AT
	s the SecuredMessage

TP ld	TP_SEC_ITSS_RCV_DENM_01_BO		
Summary	y Check that IUT discards a secured DENM if the HeaderInfo contains the header invalid Psid value		
Reference	ETSI TS 103 097 [1], clause 7.1.2		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
With			
the IUT being in the and the IUT current ensure that when	time is inside the time validity period of CERT_TS_A_AT		
containing Sig containing T containing containing	ng a message of type EtsiTs103097Data nedData oBeSignedData g HeaderInfo ning Psid indicating DENM AID value		
then			
the IUT discards			

### 6.3.3.2 Check invalid HeaderInfo elements

TP ld	TP_SEC_ITSS_RCV_DENM_02_BO		
Summary	Check that IUT discards a secured DENM if the HeaderInfo does not contain the header		
Summary	field generationLocation		
Reference	ETSI TS 103 097 [1], clause 7.1.2		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
With			
the IUT being in the 'auth	iorized' state		
and the IUT current time	is inside the time validity period of CERT_TS_A_AT		
ensure that			
when			
the IUT is receiving a r	message of type EtsiTs103097Data		
containing SignedData			
containing ToBeSignedData			
containing Hea	containing HeaderInfo		
containing Psid			
indicating DENM AID value			
and <b>not</b> containing generationLocation			
then			
the IUT discards the SecuredMessage			

TP ld	TP_SEC_ITSS_RCV_DENM_03_BO		
Summary	Check that IUT discards a secured DENM if the HeaderInfo contains the header field		
	expiryTime		
Reference	ETSI TS 103 097 [1], clause 7.1.2		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
With			
the IUT being in the	'authorized' state		
and the IUT current	time is inside the time validity period of CERT_TS_A_AT		
ensure that			
when			
the IUT is receivin	g a message of type EtsiTs103097Data		
containing SignedData			
containing ToBeSignedData			
	HeaderInfo		
containing Psid			
indicating DENM AID value			
and containing expiryTime			
then			
the IUT discards t	he SecuredMessage		

TP ld	TP_SEC_ITSS_RCV_DENM_04_BO	
Summary	Check that IUT discards a secured DENM if the HeaderInfo contains the header field	
	p2pcdLearningRequest	
Reference ETSI TS 103 097 [1], clause 7.1.2		
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
With		
the IUT being in the	e 'authorized' state	
	t time is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
the IUT is received	ing a message of type EtsiTs103097Data	
containing Sig	nedData	
containing	FoBeSignedData	
containin	g HeaderInfo	
contair	und Psid	
	cating DENM AID value	
	ntaining p2pcdLearningRequest	
then		

TP ld	TO SEC ITSS DOV DENIM OF DO	
	TP_SEC_ITSS_RCV_DENM_05_BO	
Summary	Check that IUT discards a secured DENM if the HeaderInfo contains the header field	
	missingCrIIdentifier	
Reference	ETSI TS 103 097 [1], clause 7.1.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
With		
the IUT being in the 'a	authorized' state	
and the IUT current til	me is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
the IUT is receiving	a message of type EtsiTs103097Data	
containing Signe	dData	
containing ToBeSignedData		
containing HeaderInfo		
containing Psid		
indicating DENM AID value		
and containing missingCrlldentifier		
then		
the IUT discards the SecuredMessage		

TP Id TP_SEC_ITSS_RCV_DENM_06_BO	
Summary	Check that IUT discards a secured DENM if the HeaderInfo contains the header field
	encryptionKey
Reference	ETSI TS 103 097 [1], clause 7.1.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
With	
the IUT being in the	e 'authorized' state
and the IUT curren	t time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is received	ing a message of type EtsiTs103097Data
containing Sig	nedData
containing	ToBeSignedData
containin	g HeaderInfo
	ning Psid
contair	0
contair indio	cating DENM AID value
contair indio	0

TP ld	TP_SEC_ITSS_RCV_DENM_07_BO		
Cummon (	Check that IUT discards a secured DENM if the 'SignedData' contains an invalid signature		
Summary	algorithm		
Reference	e ETSI TS 103 097 [1], clause 6		
PICS Selection	CS Selection PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT being in th	e 'authorized' state		
and the IUT currer	It time is inside the time validity period of CERT_TS_A_AT		
ensure that			
when			
the IUT is received	/ing a message of type EtsiTs103097Data		
containing Sig	gnedData		
containing Signature			
indicating wrong signature algorithm			
then			
the IUT discards	s the SecuredMessage		

TP ld		
	TP_SEC_ITSS_RCV_DENM_08_BO	
Summary	Check that IUT discards a secured DENM if the 'SignerIdentifier' contains an invalid choice	
Reference	ETSI TS 103 097 [1], clause 6	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'auth	orized' state	
and the IUT current time	is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
the IUT is receiving a n	nessage of type EtsiTs103097Data	
containing SignedDa	ata	
containing SignerIdentifier		
indicating 'self'		
then		
the IUT discards the SecuredMessage		

TP ld	TP_SEC_ITSS_RCV_DENM_09_BO	
Summary	Check that IUT discards a secured DENM if the Signature cannot be verified	
Reference	ETSI TS 103 097 [1], clause 6	
PICS Selection	S Selection PICS_GN_SECURITY	
	Expected behaviour	
with the IUT being in the and the IUT current ensure that when	e 'authorized' state time is inside the time validity period of CERT_TS_A_AT	
the IUT is receiving a message of type EtsiTs103097Data containing Signature indicating an altered value then the IUT discords the Secured Message		
the IUT discards the SecuredMessage		

• 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".

56

# 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	
V1.5.1	January 2022	Publication	