ETSITS 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)

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: http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status.

Information on the current status of this and other ETSI documents is available at

https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

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

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 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	al verbs terminology	5
1	Scope	
_		
2	References	
2.1 2.2	Normative references	
2.2	Informative references	
3	Definition of terms, symbols and abbreviations	7
3.1	Terms	7
3.2	Symbols	
3.3	Abbreviations	7
4	Test Suite Structure (TSS)	8
4.1	Structure for Security tests	
~	•	
5	Test Purposes (TP)	
5.1	Introduction	
5.1.1 5.1.2	TP Identifier paming conventions	
5.1.2	TP Identifier naming conventions.	
5.1.3	Rules for the behaviour description	
5.1.4	Mnemonics for PICS reference	
3.1.3		
6	ITS-S Security	
6.1	Overview	
6.1.1	Certificates content	
6.1.1.1		
6.1.1.2		
6.1.1.3		
6.2 6.2.1	Sending behaviourGeneral sending behaviour	
6.2.1 6.2.1.1		
6.2.2	CAM profile	
6.2.2.1		
6.2.2.2	· · · · · · · · · · · · · · · · · · ·	
6.2.2.3		
6.2.2.4		15
6.2.2.5	5 Check that IUT sends certificate to unknown ITS-S	17
6.2.2.6	6 Check that IUT restarts the timer when the certificate has been sent	18
6.2.2.7		
6.2.2.8		
6.2.2.9	1	
6.2.2.1		
6.2.2.1	1 7	
6.2.2.1 6.2.2.1		
6.2.2.1 6.2.2.1	e	
6.2.2.1 6.2.2.1		
6.2.2.1 6.2.3	DENM profile	
6.2.3.1		
6.2.3.1		
6.2.3.3		
6.2.3.4		
6.2.3.5	· · · · · · · · · · · · · · · · · · ·	
6.2.3.6	· · · · · · · · · · · · · · · · · · ·	
6.2.3.7	7 Check payload	34

6.2.3.8	Check signing permissions	35
6.2.3.9	Check signature	
6.2.3.10	Check support for certificate content	36
6.2.3.11	Check certificate consistency conditions	37
6.2.4	Generic signed message profile	39
6.2.4.1	Check that secured message is signed	39
6.2.4.2	Check secured AID value	
6.2.4.3	Check header field	40
6.2.4.4	Check that signer info is a certificate or digest	40
6.2.4.5	Check generation time	
6.2.4.6	Check payload	41
6.2.4.7	Check signing permissions	42
6.2.4.8	Check signature	42
6.3	Receiving behaviour	43
6.3.1	Check the message protocol version	43
6.3.2	CAM profile	44
6.3.2.1	Check the valid message receiving	44
6.3.2.2	Check invalid HeaderInfo elements	47
6.3.2.3	Check invalid Signature elements	49
6.3.3	DENM profile	50
6.3.2.1	Check the valid message receiving	50
6.3.3.2	Check invalid HeaderInfo elements	53
6.3.3.3	Check invalid Signature elements	55
Annex A	A (informative): Bibliography	56
	, , , , , , , , , , , , , , , , , , ,	
LIIDIUI Y		

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.

DECTTM, **PLUGTESTS**TM, **UMTS**TM and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP**TM and **LTE**TM are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M**TM logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**[®] 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 <u>ETSI Drafting Rules</u> (Verbal forms for the expression of provisions).

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

1 Scope

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

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

2 References

2.1 Normative references

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

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

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

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

[1]	ETSI TS 103 097 (V1.4.1): "Intelligent Transport Systems (ITS); Security; Security header and
	certificate formats".

- [2] IEEE Std 1609.2TM-2016: "IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages", as amended by IEEE Std 1609.2aTM-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.3]	ISO/IEC 9646-1 (1994): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 1: General concepts".
[i.4]	ISO/IEC 9646-2 (1994): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 2: Abstract Test Suite specification".
[i.5]	ISO/IEC 9646-6 (1994): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 6: Protocol profile test specification".
[i.6]	ISO/IEC 9646-7 (1995): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 7: Implementation Conformance Statements".
[i.7]	ETSI ETS 300 406 (1995): "Methods for testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

3 Definition of terms, symbols and abbreviations

Terms 3.1

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.

Symbols 3.2

Void.

3.3 **Abbreviations**

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

Authorization Authority AA **AID Application Identifier** ITS Application Identifier for CAM AID CAM AID DENM Application Identifier for DENM Application Identifier for general GeoNetworking messages AID_GN Authorization Ticket ΑT ATS Abstract Test Suite **Exceptional Behaviour** BO Valid Behaviour BV CA Certificate Authority CAM Co-operative Awareness Messages CAN Controller Area Network **CERT** Certificate DE Data Element

Decentralized Environmental Notification DEN

DENM Decentralized Environmental Notification Message

EA **Enrolment Authority** Elliptic Curve Cryptography **ECC**

GeoNetworking GN

Intelligent Transport Systems ITS Intelligent Transport System - Station ITS-S

IUT Implementation under Test

MSG Message

PICS Protocol Implementation Conformance Statement

PSID Provider Service Identifier **RCA** Root Certificate Authority SSP Service Specific Permissions TP Test Purposes
TSS Test Suite Structure

4 Test Suite Structure (TSS)

4.1 Structure for Security tests

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

Table 1: TSS for Security

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

5 Test Purposes (TP)

5.1 Introduction

5.1.1 TP definition conventions

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

5.1.2 TP Identifier naming conventions

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

Table 2: TP naming convention

Identifier	TP_ <root>_<tgt>_<gr>_<rn>_<sn>_<x>[_<v>]</v></x></sn></rn></gr></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
		ВО	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

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

5.1.5 Mnemonics for PICS reference

To avoid an update of all TPs when the PICS document is changed, table 3 introduces mnemonics name and the correspondence with the real PICS item number. The 'PICS item' as defined in IEEE Std 1609.2 [2], ETSI TS 103 096-1 [3] and ETSI TS 102 871-1 [4] shall be used to determine the test applicability.

Table 3: Mnemonics for PICS reference

	Mnemonic	PICS item
1	PICS_GN_SECURITY	A.2/1 [4]
2	PICS_SEC_CERTIFICATE_SELECTION	A.8/1 [3]
3	PICS_SEC_CIRCULAR_REGION	S1.2.2.5.1.1 [2]
4	PICS_SEC_RECTANGULAR_REGION	S1.2.2.5.1.2 [2]
5	PICS_SEC_POLYGONAL_REGION	S1.2.2.5.1.3 [2]
6	PICS_SEC_IDENTIFIED_REGION	S1.2.2.5.1.4 [2]
7	PICS_SEC_ITS_AID_OTHER	A.7/1 [3]
8	PICS_SEC_SHA256	S1.2.2.1.1 [2]
9	PICS_SEC_SHA384	S1.2.2.1.2 [2]
10	PICS_SEC_BRAINPOOL_P256R1	S1.2.2.4.1.2 [2]
11	PICS_SEC_BRAINPOOL_P384R1	\$1.2.2.4.2 [2]
12	PICS_SEC_IMPLICIT_CERTIFICATE	\$1.2.2.8 [2]

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
OFDT ILIT A DOA		on the IUT
CERT_IUT_A_RCA	- self-signed	Yes
	- name "ETSI Test RCA A certificate"	
	- application permissions:	
	o CRL with SSP 0x01	
	o CTL with SSP 0x0138	
	- certificate issuing permissions:	
	o CAM with all possible SPP (0x01FFFC / 0xFF0003)	
	o DENM with all possible SSP (0x01FFFFFF / 0xFF000000)	
	o SPATEM with all possible SSP (0x01E0 / 0xFF1F)	
	o MAPEM with all possible SSP (0x01C0 / 0xFF3F)	
	o IVIM with all possible SSP (0x01000000FFF8 / 0xFF0000000007)	
	o SREM with all possible SSP (0x01FFFFE0 / 0xFF00001F)	
	o SSEM with all possible SSP (0x01 / 0xFF)	
	o GPC with all possible SSP (0x01 / 0xFF)	
	o GN-MGMT without SSP	
	CRT-REQ with SSP (0x01FE / 0xFF01)	
	- validation time for 3 years	
	- no region restriction	
	- assurance level 6	
	- verification key of type compressed with NIST P256R curve	
	- valid signature of type x-only with NIST P256R curve	
CERT_IUT_A_RCA_A8	Same as CERT_IUT_A_ATCERT_IUT_A_RCA, excepting the following:	Yes
	- certificate issuing permissions:	
	o same as in CERT_IUT_A_RCA	
	o unallocated ITS AIDs: 96, 97, 98, 99, 100, 101, 102 without SSP	
CERT_IUT_C_RCA	Same as CERT_IUT_A_ATCERT_IUT_A_RCA, excepting the following:	Yes
	- rectangular region restriction (10km square)	
	no unallocated ITS AID in certificate issuing permissions	

6.1.1.2 Authorization Authorities certificates

AA certificate	Content	To be
		installed
CERT_IUT_A_AA	- signer digest of the CERT_IUT_A_RCA	on the IUT Yes
CERT_IUT_A_AA	- application permissions:	res
	CRT_REQ with SSP 0x0132	
	- certificate issuing permissions:	
	CAM with all possible SPP (0x01FFFC / 0xFF0003)	
	 DENM with all possible SSP (0x01FFFFFF / 0xFF000000) 	
	 SPATEM with all possible SSP (0x01E0 / 0xFF1F) 	
	 MAPEM with all possible SSP (0x01C0 / 0xFF3F) 	
	 IVIM with all possible SSP (0x01000000FFF8 / 0xFF0000000007) 	
	 SREM with all possible SSP (0x01FFFFE0 / 0xFF00001F) 	
	 SSEM with all possible SSP (0x01 / 0xFF) 	
	GPC with all possible SSP (0x01 / 0xFF)	
	GN-MGMT without SSP	
	- validation time for 3 years	
	- no region restriction	
	 assurance level 4 verification key of type compressed with NIST P256R curve 	
	- encryption key of type compressed with NIST P256R curve	
	- valid signature of type x-only with NIST P256R curve	
CERT_IUT_A_N_AA	Same as CERT_IUT_A_ATCERT_IUT_A_AA, excepting the following:	Yes
	- verification key of type uncompressed	100
CERT_IUT_A_B_AA	Same as CERT_IUT_A_ATCERT_IUT_A_AA, excepting the following:	Yes
	- verification key with Brainpool P256r1 curve	
CERT_IUT_A_B3_AA	Same as CERT_IUT_A_ATCERT_IUT_A_B_AA, excepting the following:	Yes
	- verification key with Brainpool P384r1 curve	
CERT_IUT_A_AA_A8	Same as CERT_IUT_A_ATCERT_IUT_A_AA, excepting the following:	Yes
	 signer digest of the CERT_IUT_A_RCA_A8 	
	- certificate issuing permissions:	
	o CAM with all possible SPP (0x01FFFC / 0xFF0003)	
	o unallocated ITS AIDs: 96, 97, 98, 99, 100, 101, 102 without SSP	
CERT HIT CO AA	o no other certificate issuing permissions	V
CERT_IUT_CC_AA	Same as CERT_IUT_A_ATCERT_IUT_A_AA, excepting the following:	Yes
	 signer digest of the CERT_IUT_C_RCA rectangular region restriction equal to the one in the CERT_IUT_C_RCA 	
CERT_IUT_C3_AA	Same as CERT_IUT_A_ATCERT_IUT_CC_AA, excepting the following:	Yes
CERT_IOT_CS_AA	- rectangular region restriction oversizing the one in the CERT_IUT_C_RCA	163
CERT_IUT_CA_AA	Same as CERT_IUT_A_ATCERT_IUT_CC_AA, excepting the following:	Yes
	- no region restriction	
CERT_IUT_D_AA	Same as CERT_IUT_A_ATCERT_IUT_CC_AA, excepting the following:	Yes
	- polygonal region restriction as a square with the side of 10 km and center in	
	the IUT position	
CERT_TS_A_AA	Same as CERT_IUT_A_ATCERT_IUT_A_AA.	Yes
	To be used on the Test System side.	
CERT_TS_B_AA	Same as CERT_IUT_A_ATCERT_IUT_A_B_AA.	Yes
	To be used on the Test System side.	
CERT_TS_A_B_AA	Same as CERT_IUT_A_ATCERT_IUT_A_B_AA.	Yes
	To be used on the Test System side.	

6.1.1.3 Authorization Tickets

Authorization ticket	Content	To be installed on the IUT
CERT_IUT_A_AT	 signer digest of the CERT_IUT_A_AA; application permissions: CAM with all SPP (0x01FFFC); 	Yes
	DENM with all SSP (0x01FFFFFF);GN-MGMT;	
	validation time for 1 year;no region restriction;assurance level 3;	
	 verification key of type compressed with NIST P256R curve; encryption key of type compressed with NIST P256R curve; valid signature of type x-only with NIST P256R curve; 	
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: - signer digest of the CERT_IUT_A_B_AA; - verification key with Brainpool P256r1 curve; - valid signature with Brainpool P256r1 curve;	Yes
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: - signer digest of the CERT_IUT_A_B3_AA; - valid signature with Brainpool P384r1 curve;	Yes
CERT_IUT_A_AT_A8	Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following: - signer digest of the CERT_IUT_A_AA_A8; - application permissions:	Yes
CERT_IUT_B_AT	Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following: - circular region restriction with the radius of 5 km and center at the IUT point;	Yes
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 IUT point;	Yes
CERT_IUT_D_AT	Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following: - signer digest of the CERT_IUT_D_AA; - polygonal region restriction identical to the one in the CERT_IUT_D_AA, including the IUT position;	Yes
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: - application permissions: - DENM with all SSP (0x01FFFFFF); - GN-MGMT;	Yes
CERT_IUT_A4_AT	Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following: - application permissions: - CAM with all SPP (0x01FFFC); - GN-MGMT;	Yes
CERT_IUT_C1_AT	Same as CERT_IUT_A_ATCERT_IUT_A_AT, excepting the following: - signer digest of the CERT_IUT_CC_AA; - rectangular region restriction outside of the IUT point;	Yes

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
Deference	ETSI TS 103 097 [1], clause 5.1
Reference	IEEE Std 1609.2 [2], clause 6.3.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
ensure that	
when	
the IUT is reques	sted to send a secured message
then	
the IUT sends a	EtsiTs103097Data
containing pro	tocolVersion
indicating va	alue '3'

6.2.2 CAM profile

6.2.2.1 Check that secured CAM is signed

TP Id	TP_SEC_ITSS_SND_CAM_01_BV			
Summary	Check that IUT sends the secured CAM using SignedData container			
Reference	ETSI TS 103 097 [1], clause 7.1.1			
PICS Selection	PICS_GN_SECURITY			
	Expected behaviour			
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			
Summary	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	AT certificate (CERT_IUT_A_AT)			
ensure that				
when				
the IUT is requested to	the IUT is requested to send a secured CAM			
then				
	the IUT sends a message of type EtsiTs103097Data			
containing content				
0 0	containing signedData			
containing tbsData				
containing headerInfo				
containing psid				
indicating 'AID_CAM'				

6.2.2.3 Check header fields

TP Id	TP_SEC_ITSS_SND_CAM_03_BV				
	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	send a secured CAM				
then					
the IUT sends a messa	age of type EtsiTs103097Data				
containing content					
containing signed					
containing tbs[Data				
containing h	eaderInfo				
	g generationTime				
and not containing expiryTime					
and not containing generationLocation,					
and not containing encryptionKey					
	ontaining p2pcdLearningRequest				
and not containing missingCrlldentifier					

6.2.2.4 Check signer information

P Id 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	AT certificate (CERT_IUT_A_AT)		
ensure that			
when			
the IUT is requested to	send a secured CAM		
then			
	the IUT sends a message of type EtsiTs103097Data		
containing content			
containing signed			
containing sign			
containing di			
or containing			
containing			
	indicating 'none'		
containing toBeSigned			
containing appPermissions			
	containing the item of type PsidSsp		
	containing psid		
indicating AID_CAM and not containing certIssuePermissions			
ani	u not containing certissuer ennissions		

Expected behaviour			
PICS Selection	PICS_GN_SECURITY AND X_PICS		
Reference	IEEE Std 1609.2 [2], clause 6.3.4		
Reference	ETSI TS 103 097 [1], clauses 5.2 and 7.1.1		
Summary	Check that IUT canonicalize certificates before hash calculation		
Summary	Check that IUT calculate the digest of certificate using proper hash algorithm		
TP Id	TP_SEC_ITSS_SND_CAM_05_BV		

with

the IUT is authorized with AT certificate (**X_CERTIFICATE**) and the IUT is configured to send more than one CAM per second and the IUT having sent a secured CAM containing signer

containing signer

containing certificate
indicating X_CERTIFICATE
containing verifyKeyIndicator
containing verificationKey
containing X_KEY

ensure that

when

the IUT is requested to send a subsequent secured CAM containing signer

containing signer

then

the IUT sends a message of type EtsiTs103097Data

containing content containing signedData containing signer containing digest

indicating last 8 bytes of the Hash value calculated using X_HASH algorithm

Permutation table				
XX	X_CERTIFICATE	X_KEY	X_HASH	X_PICS
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 (uncompressed)	SHA-384	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1

TP Id	TP_SEC_ITSS_SND_CAM_06_BV	
	Check that IUT sends the secured CAM containing the signing certificate when over the	
	time of one second no other secured CAM contained the certificate was sent	
Reference	ETSI TS 103 097 [1], clause 7.1.1	
PICS Selection	PICS_GN_SECURITY	
Expected behaviour		

with

the IUT is authorized with AT certificate (CERT_IUT_A_AT) and the IUT is configured to send more than one CAM per second

and the IUT having sent a secured CAM containing generationTime

indicating TIME_LAST

ensure that

when

the IUT is sending secured CAM as a message of type EtsiTs103097Data

containing signer containing certificate

then

this message is

containing headerInfo

containing generationTime

indicating TIME (TIME >= TIME_LAST + 1 sec)

TP ld	TP_SEC_ITSS_SND_CAM_07_BV
Summary	Check that IUT sends the secured CAM containing the signing certificate when the timeout
Summary	of one second has been expired after the previous CAM containing the certificate
Reference	ETSI TS 103 097 [1], clause 7.1.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT is authorized with	n AT certificate (CERT_IUT_A_AT)
and the IUT is configured	to send more than one CAM per second
and the IUT having sent	a secured CAM
containing signer	
containing certificate	·
and containing genera	tionTime
indicating TIME_LAS	ST
ensure that	
when	
the IUT is sending a se	ecured CAM as a message of type EtsiTs103097Data
containing generation	onTime
indicating TIME >	= TIME_LAST + 1 sec
then	
this message is	
containing certificate	e

6.2.2.5 Check that IUT sends certificate to unknown ITS-S

PId TP_SEC_ITSS_SND_CAM_08_BV			
Summary	Check that IUT sends the secured CAM containing the signing certificate when the IUT		
Summary	received a CAM from an unknown ITS-S		
Reference	ETSI TS 103 097 [1], clause 7.1.1		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT is authorized with	AT certificate (CERT_IUT_A_AT)		
and the IUT is configured	to send more than one CAM per second		
and the IUT having alread	ly sent secured CAM		
containing certificate			
at TIME_1			
	red a message of type EtsiTs103097Data		
	containing signedData		
containing signer			
containing digest			
indicating Hash			
referencing an unknown certificate (CERT_TS_F_AT)			
at TIME_2 (TIME_1 < TIME_2 < TIME_1+1 sec)			
ensure that			
when			
the IUT is requested to send secured CAM			
at TIME_3 (TIME_1 < TIME_2 < TIME_3 < TIME_1 + 1 sec)			
then			
the IUT sends a message of type EtsiTs103097Data			
containing signedData			
containing signer			
containing certif	псате		

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

TP Id TP SEC ITSS SND CAM 09 B				
TP Id TP_SEC_ITSS_SND_CAM_09_B\				
	te sending timer when the signing certificate was sent			
Reference ETSI TS 103 097 [1], clause 7.1.1				
PICS Selection PICS_GN_SECURITY				
Expected be	naviour			
with				
the IUT is authorized with AT certificate (CERT_IUT_A_AT)				
and the IUT is configured to send more than one CAM per se	cond			
and the IUT having already sent secured CAM				
containing signer				
containing certificate				
at TIME_1				
and the IUT having received a secured CAM				
containing signer				
containing digest				
indicating HashID8 value				
referencing an unknown certificate (CERT_TS_F_/	AT)			
at TIME_2 (TIME_1 + 0,3 sec)				
and the IUT having sent secured CAM				
containing signer				
containing certificate				
at TIME_3 (TIME_3 > TIME_2)				
ensure that				
when				
the IUT is sending the next secured CAM				
containing signedData containing signer				
containing signer containing certificate				
at TIME_4				
then				
	the difference between TIME_4 and TIME_3 is about 1 sec			

6.2.2.7 Check sending certificate request for unknown certificate

Check that the IUT sends certificate request when it receives secured CAM containing digest of unknown certificate as a message signer ETSI TS 103 097 [1], clause 7.1.1 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 with AT certificate (CERT_IUT_A_AT) and the IUT has receiving a EtsiTs103097Data containing signer containing digest indicating HashedId8 value DIGEST_F referencing an unknown certificate (CERT_TS_F_AT)	_				
digest of unknown certificate as a message signer ETSI TS 103 097 [1], clause 7.1.1 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 with AT certificate (CERT_IUT_A_AT) and the IUT has receiving a EtsiTs103097Data containing signer containing digest indicating HashedId8 value DIGEST_F referencing an unknown certificate (CERT_TS_F_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing headerInfo containing inlineP2pcdRequest	TP ld	**			
Reference ETSI TS 103 097 [1], clause 7.1.1 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 with AT certificate (CERT_IUT_A_AT) and the IUT has receiving a EtsiTs103097Data containing signer containing digest indicating HashedId8 value DIGEST_F referencing an unknown certificate (CERT_TS_F_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing headerInfo containing inlineP2pcdRequest	Summary	Check that the IUT sends certificate request when it receives secured CAM containing			
PICS Selection PICS_GN_SECURITY, PICS_SEC_P2P_AT_DISTRIBUTION Expected behaviour with the IUT is authorized with AT certificate (CERT_IUT_A_AT) and the IUT has receiving a EtsiTs103097Data containing signer containing digest indicating HashedId8 value DIGEST_F referencing an unknown certificate (CERT_TS_F_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing headerInfo containing inlineP2pcdRequest	Summary	digest of unknown certificate as a message signer			
PICS Selection PICS_GN_SECURITY, PICS_SEC_P2P_AT_DISTRIBUTION Expected behaviour with the IUT is authorized with AT certificate (CERT_IUT_A_AT) and the IUT has receiving a EtsiTs103097Data containing signer containing digest indicating HashedId8 value DIGEST_F referencing an unknown certificate (CERT_TS_F_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing headerInfo containing inlineP2pcdRequest	Deference	ETSI TS 103 097 [1], clause 7.1.1			
Expected behaviour with the IUT is authorized with AT certificate (CERT_IUT_A_AT) and the IUT has receiving a EtsiTs103097Data containing signer containing digest indicating HashedId8 value DIGEST_F referencing an unknown certificate (CERT_TS_F_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing headerInfo containing inlineP2pcdRequest	Reference	IEEE Std 1609.2 [2], clauses 6.3.9 and 8.2.4.1.2			
with the IUT is authorized with AT certificate (CERT_IUT_A_AT) and the IUT has receiving a EtsiTs103097Data containing signer containing digest indicating HashedId8 value DIGEST_F referencing an unknown certificate (CERT_TS_F_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing headerInfo containing inlineP2pcdRequest	PICS Selection	PICS_GN_SECURITY, PICS_SEC_P2P_AT_DISTRIBUTION			
the IUT is authorized with AT certificate (CERT_IUT_A_AT) and the IUT has receiving a EtsiTs103097Data containing signer containing digest indicating HashedId8 value DIGEST_F referencing an unknown certificate (CERT_TS_F_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing headerInfo containing inlineP2pcdRequest		Expected behaviour			
and the IUT has receiving a EtsiTs103097Data containing signer containing digest indicating HashedId8 value DIGEST_F referencing an unknown certificate (CERT_TS_F_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing headerInfo containing inlineP2pcdRequest	with				
containing signer containing digest indicating HashedId8 value DIGEST_F referencing an unknown certificate (CERT_TS_F_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing headerInfo containing inlineP2pcdRequest	the IUT is authorized wi	th AT certificate (CERT_IUT_A_AT)			
containing digest indicating HashedId8 value DIGEST_F referencing an unknown certificate (CERT_TS_F_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing headerInfo containing inlineP2pcdRequest	and the IUT has receiving	ng a EtsiTs103097Data			
indicating HashedId8 value DIGEST_F referencing an unknown certificate (CERT_TS_F_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing headerInfo containing inlineP2pcdRequest	containing signer				
referencing an unknown certificate (CERT_TS_F_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing headerInfo containing inlineP2pcdRequest	containing digest				
referencing an unknown certificate (CERT_TS_F_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing headerInfo containing inlineP2pcdRequest	indicating Hashe				
when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing headerInfo containing inlineP2pcdRequest	referencing ar	n unknown certificate (CERT_TS_F_AT)			
the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data containing headerInfo containing inlineP2pcdRequest	ensure that	·			
then the IUT sends a message of type EtsiTs103097Data containing headerInfo containing inlineP2pcdRequest	when				
the IUT sends a message of type EtsiTs103097Data containing headerInfo containing inlineP2pcdRequest	the IUT is requested	the IUT is requested to send a secured CAM			
containing headerInfo containing inlineP2pcdRequest	then				
containing inlineP2pcdRequest	the IUT sends a message of type EtsiTs103097Data				
containing inlineP2pcdRequest	0 71				
	_	· ·			
indicating last 3 octets of DIGEST_F					

PICS_SEC_SHA384

XX	XX X_FIELD_1 X_CERT X_PICS					
		ation table				
indic	ating last 3 octets of DIGEST_F					
	ing HashedId3 value					
	inlineP2pcdRequest					
containing h						
containing tbs[
containing signed						
	ssage of type EtsiTs103097Data					
then	to send secured CAM					
when	to sond socured CAM					
ensure that						
	cing an unknown certificate (X_C	EKICERI_IS_F_AI)				
9	HashedId8 value DIGEST_F					
containing X						
containing issu						
containing certific	ate					
containing signer	mig a moodage of type Etoria root	Data				
	ring a message of type EtsiTs103	•				
	vith AT certificate (CERT_IUT_A_	4 T)				
with	Expecte	d behaviour				
	AND X_PICS	d habariaru				
PICS Selection	AND PICS_SEC_P2P_AA_DI	SIKIBUTION				
D100 0 1 11	PICS_GN_SECURITY	TRIBUTION				
EEE Std 1609.2 [2], clauses 6.3.9 and 8.2.4.1.2						
Reference	ETSI TS 103 097 [1], clause 7					
certificate signed by unknown AA certificate						
n		ficate request when it receives	secured CAM containing			
TP ld	TP_SEC_ITSS_SND_CAM_1	I_BV_ <i>XX</i>				

CERT_TS_F_AT CERT_TS_F3_AT

sha256AndDigest sha384AndDigest

6.2.2.8 Check that IUT sends AT certificate when requested

TP Id TP_SEC_ITSS_SND_CAM_12_BV			
	Check that IUT sends the secured CAM containing the signing certificate when it received a		
Summary	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		
Reference	IEEE Std 1609.2 [2], clauses 6.3.9 and 8.2.4.2.3		
PICS Selection	PICS_GN_SECURITY		
FICS Selection	AND PICS_SEC_P2P_AT_DISTRIBUTION		
	Expected behaviour		
with			
the IUT is authorized wi	th AT certificate (CERT_IUT_A_AT)		
and the IUT is configure	d to send more than one CAM per second		
and the IUT having alre	ady sent secured CAM		
containing signer			
containing certifica	te		
at TIME_1			
and the IUT having received a secured CAM			
containing headerInfo			
containing inlineP2			
containing Hash			
	ue HASHED_ID_3		
O .	ast 3 octets of currently used AT certificate		
	: TIME_2 < TIME_1+1 sec)		
ensure that			
when	1 044		
the IUT is requested to send a CAM			
at TIME_3 (TIME_1 < TIME_2 < TIME_3 < TIME_1+1 sec)			
then			
the IUT sends a SecuredMessage of type EtsiTs103097Data			
containing signer and containing certificate			
9	ertificate the HashedId3 value HASHED_ID_3		
letereticed by	the Hadhedido value HADHED_ID_3		

6.2.2.9 Check that IUT sends AA certificate when requested

TP Id 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			
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_AT_DISTRIBUTION			
	Expected behaviour			
with				
	AT certificate (CERT_IUT_A_AT)			
	cate (CERT_IUT_A_AA)			
and the IUT is configured	to send more than one CAM per second			
and the IUT having alread	dy sent a secured CAM			
containing signer				
containing certificate				
at TIME_1				
and the IUT having received a secured CAM				
containing headerInfo				
	containing inlineP2pcdRequest			
	containing HashedId3 value			
	indicating last 3 octets of the digest of CERT_IUT_A_AA			
_ \ _	ΓIME_2 < TIME_1+1 sec)			
	ensure that			
when				
the IUT is requested to send a secured CAM				
at TIME_3 (TIME_1 < TIME_2 < TIME_3 < TIME_1+1 sec)				
then				
the IUT sends a SecuredMessage of type EtsiTs103097Data				
containing headerInfo				
containing requested				
indicating request	ed AA certificate CERT_IUT_A_AA			

_				
TP_SEC_ITSS_SND_CAM_14_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			
Summary	unrecognized certificate that matches with the known AA certificate ID which is not currently			
	used by the IUT			
Reference	ETSI TS 103 097 [1], clause 7.1.1			
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				
	th AT certificate (CERT_IUT_A_AT)			
	ed to send more than one CAM per second			
	ed to know the AA certificate (CERT_IUT_A_N_AA)			
and the IUT has already	y sent secured CAM			
containing signer				
	containing certificate			
at TIME_1				
and the IUT having received a secured CAM				
containing headerInfo				
	containing inlineP2pcdRequest			
containing Hash				
indicating last 3 octets of the digest of CERT_IUT_A_N_AA				
	which is not an issuer of currently used AT certificate			
- \ -	< TIME_2 < TIME_1+1 sec)			
ensure that				
when				
the IUT is requested to send a secured CAM				
_ , _	1 < TIME_2 < TIME_3 < TIME_1+1 sec)			
then	uradManaga of tuna EtaiTa102007Data			
the IUT sends a SecuredMessage of type EtsiTs103097Data				
containing headerInfo containing requestedCertificate				
• .				
indicating req	uested AA certificate (CERT_IUT_A_N_AA)			

TDIA	TD CEC ITCC CND CAM 45 DV		
TP Id	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		
. 10.0.0.0.00	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			
	AT certificate (CERT_IUT_A_AT)		
	icate (CERT_IUT_A_AA)		
and the IUT is configured	to send more than one CAM per second		
and the IUT having alread	dy sent secured CAM		
containing signer			
containing certificate			
at TIME_1			
and the IUT having receive	ved a secured CAM		
containing headerInfo			
containing inlineP2pcdRequest			
containing HashedId3 value			
indicating last 3	3 octets of the digest of CERT_IUT_A_AA		
at TIME_2 (TIME_1 < 7	TIME_2 < TIME_1 + 0,8 sec)		
and the IUT having receive	ved a secured CAM		
containing headerInfo			
containing requested	dCertificate		
	indicating requested AA certificate (CERT_IUT_A_AA)		
at TIME_3 (TIME_2 < TIME	ME_3 < TIME_2 + 0,1 sec)		
ensure that			
when			
the IUT is requested to send a secured CAM			
at TIME_4 (TIME_3 < TIME_4 < TIME_1 + 0,9 sec)			
then			
the IUT sends a Secur	edMessage of type EtsiTs103097Data		
containing headerInf			
does not contain i	requestedCertificate		

TP Id	TP_SEC_ITSS_SND_CAM_16_BV		
Summary	Check that the IUT does not send a secured CAM containing the AA certificate in the		
Summary	requestedCertificate headerInfo field when it contains certificate in the signer field		
	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, PICS_SEC_P2P_AA_DISTRIBUTION		
	Expected behaviour		
with			
the IUT is authorized with	AT certificate (CERT_IUT_A_AT)		
	cate (CERT_IUT_A_AA)		
and the IUT is configured	to send more than one CAM per second		
and the IUT having alread	dy sent a secured CAM		
containing signer			
containing certificate			
at TIME_1			
and the IUT having receive	and the IUT having received a SecuredMessage		
containing headerInfo			
containing inlineP2p			
containing Hashed			
indicating last 3 octets of the digest of CERT_IUT_A_AA			
at TIME_2 (TIME2 = TIMI	at TIME_2 (TIME2 = TIME_1 + 0,9 sec)		
ensure that			
when			
<u> </u>	the IUT is requested to send a secured CAM		
at TIME_3 (TIME_2 < TIME_3 < TIME_1 + 1 sec)			
then			
the IUT sends a SecuredMessage of type EtsiTs103097Data			
containing signer			
containing certification			
and containing head			
not containing red	questedCertificate		

TP Id TP_SEC_ITSS_SND_CAM_17_BV			
Summary	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		
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			
	AT certificate (CERT_IUT_A_AT)		
	cate (CERT_IUT_A_AA)		
	to send more than one CAM per second		
and the IUT having alread	dy sent secured CAM		
containing signer			
containing certificate			
at TIME_1			
and the IUT having received a SecuredMessage of type EtsiTs103097Data			
containing headerInfo			
containing inlineP2p			
containing Hashed			
	octets of the digest of CERT_IUT_A_AA		
_ ` _ ·	9 sec < TIME2 < TIME_1 + 1 sec)		
ensure that			
when			
	st subsequent secured CAM		
containing signer			
containing digest			
then			
this message			
containing headerInf			
containing reques			
indicating reque	ested AA certificate CERT_IUT_A_AA		

6.2.2.10 Check generation time

TP Id 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	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 wi	th AT certificate (CERT_IUT_A_AT)		
ensure that			
when			
the IUT is requested	to send CAM		
containing certifica	te		
then			
	redMessage of type EtsiTs103097Data		
containing headerl			
containing gene			
_	indicating GEN_TIME (CUR_TIME - 5 min <= GEN_TIME <= CUR_TIME + 5 min)		
	and containing signer		
	containing certificate		
containing toBeSigned			
containing validityPeriod			
containing start			
indicating value X_START_VALIDITY (X_START_VALIDITY <= GEN_TIME)			
	and containing duration		
indica	ting value > GEN_TIME - X_START_VALIDITY		

6.2.2.11 Check payload

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				
PICS Selection	PICS_GN_SECURITY			
	Expected behaviour			
with				
the IUT is authorized with	AT certificate (CERT_IUT_A_AT)			
ensure that				
when				
the IUT is requested to	send a secured CAM			
then				
	age of type EtsiTs103097Data			
contains content				
contains signedDa				
containing tbsData				
containing payload				
containing data				
containing content				
containing unsecuredData				
COI	ntaining not-empty data			

6.2.2.12 Check signing permissions

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		
	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	ted to send a secured CAM		
then			
the IUT sends a message of type EtsiTs103097Data			
containing signer			
containing certificate			
containing	g appPermissions		
contair	ling an item of type PsidSsp		
cont	aining psid = AID CAM		

6.2.2.13 Check signature

TP Id	TP_SEC_ITSS_SND_CAM_21_BV_XX	
	Check that IUT sends the secured CAM containing signature	
Summary	Check that the signature is calculated over the right fields and using right hash algorithm by	
	cryptographically verifying the signature	
Reference	ETSI TS 103 097 [1], clauses 5.2, 7.1.1	
Reference	IEEE Std 1609.2 [2], clauses 5.3.1, 6.3.4, 6.3.29, 6.3.30 and 6.3.31	
PICS Selection	PICS_GN_SECURITY AND X_PICS	
	Expected behaviour	
with		
the IUT is authorized with	AT certificate (X_CERTIFICATE)	
containing verifyKeyInd		
containing verification		
containing X_KE		
indicating KEY		
ensure that		
when		
the IUT is requested to	send a secured CAM	
then	/	
	age of type EtsiTs103097Data	
containing signedDa	ata .	
containing signer	-1	
containing digest		
referencing the certificate X_CERTIFICATE		
or containing certificate		
indicating X_CERTIFICATE		
and containing signature containing <i>X_SIGNATURE</i>		
verifiable using KEY		
verillable usi	Permutation table	
	r cilliutation table	

	Volition of the first terms of t			
	Permutation 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_P256 R1
С	CERT_IUT_A_B3_AT	ecdsaBrainpoolP384r1	ecdsaBrainpoolP384r1Signature	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384 R1

PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1

TP Id	k	TP_SEC_ITSS_SND_CAM_22_BV_ XX		
Summary		Check that IUT sends the secured CAM containing signature containing the ECC point of		
		type set to either compressed_lsb_y_0, compressed_lsb_y_1 or x_coordinate_only		
Refe	rence	ETSI TS 103 097 [1], clauses 5.2, 7.1.1		
IXCIC	101100	IEEE Std 1609.2 [2], clauses 6.3.30 and 6.3	3.31	
PICS	Selection	PICS_GN_SECURITY AND X_PICS		
		Expected behaviour		
with				
		AT certificate (X_CERTIFICATE)		
	re that			
	nen			
	the IUT is requested to	send a secured CAM		
the	- · ·	(
		age of type EtsiTs103097Data		
	containing signedDa			
	containing signatu			
	containing X_SIGNATURE			
	containing rS			
	containing x-only or containing compressed-y-0			
	or containing compressed-y-1			
Permutation table				
XX	X CERTIFICATE	X SIGNATURE	X PICS	
Α	CERT_IUT_A_AT	ecdsaNistP256Signature		
В	CERT_IUT_A_B_AT	ecdsaBrainpoolP256r1Signature	PICS_SEC_BRAINPOOL_P256R1	
		·	*	

6.2.2.14 Check support for certificate content

C | CERT_IUT_A_B3_AT | ecdsaBrainpoolP384r1Signature

TP Id	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 authorized with	AT certificate (CERT_IUT_A_AT_A8)	
containing toBeSigned		
containing appPermissions		
containing 8 entries		
indicating the last item		
containing psid		
indicating the 'AID_CAM'		
ensure that		
when		
the IUT is requested to send a secured CAM		
then	/	
the IUT sends a message of type EtsiTs103097Data		
containing content		
containing signedData		
containing tbsData		
containing he		
containing psid		
indicatir	ng '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		
Summary	certificate		
Reference	IEEE Std 1609.2 [2], clause 6.4.8		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
	AT certificate (CERT_IUT_A_AT_A8)		
containing appPermiss			
conformed to the cer			
issued by AA certificate (CERT_IUT_A_AA_A8)			
	containing toBeSigned		
containing certIssuePermissions			
containing 8 entries			
indicating the last item			
containing psid			
indicating the 'AID_CAM'			
ensure that when			
*****	and a accurad CAM		
the IUT is requested to send a secured CAM			
	then the ILIT conds a massage of two EtciTs102007Data		
the IUT sends a message of type EtsiTs103097Data containing content			
containing content			
containing signed bata			
containing he			
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 authorized with AT certificate (CERT_IUT_C1_AT)		
containing region		
indicating rectangular region		
not containing current IUT position		
and the IUT has no other installed AT certificates		
ensure that		
when		
the IUT is requested to send a secured CAM		
then		
the IUT does not send	CAM	

TP Id	TP_SEC_ITSS_SND_CAM_24_BV	
	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 authorize	zed with the AT certificate (CERT_IUT_CA3_AT)	
not containing region		
and issued by the AA certificate (CERT_IUT_C3_AA)		
containing region		
indicating rectangular region		
not containing current IUT position		
ensure that		
when		
the IUT is requested to send a secured CAM		
then		
the IUT does not send	CAM	

TP ld	TP_SEC_ITSS_SND_CAM_25_BV		
Cummary.	Check that IUT does not send secured CAMs if all AT certificates installed on the IUT was		
Summary	expired		
Reference	IEEE Std 1609.2 [2], clause 5.2.3.2.2		
PICS Selection	PICS_GN_SECURITY		
Expected behaviour			
with			
the IUT is authorized	the IUT is authorized with AT certificate (CERT_IUT_A1_AT)		
containing validity	containing validityPeriod		
indicating start	indicating start + duration < CURRENT_TIME		
and the IUT has no other installed AT certificates			
ensure that			
when			
the IUT is requested to send a secured CAM			
then			
the IUT does not send CAM			

TP Id	TP_SEC_ITSS_SND_CAM_26_BV
Summary	Check that IUT does not send secured CAMs if all AT certificates installed on the IUT have
	the starting time in the future
Reference	IEEE Std 1609.2 [2], clause 5.2.3.2.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with the IUT is authorized with 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 send a secured CAM

TP Id	TP_SEC_ITSS_SND_CAM_27_BV	
Summany	Check that IUT does not send secured CAMs if IUT does not possess an AT certificate	
Summary	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	d with AT certificate (CERT_IUT_A3_AT)	
containing appPe	ermissions	
not containing PsidSSP		
containing psid		
indicating AID_CAM		
and the IUT has no	other installed AT certificates	
ensure that		
when		
the IUT is reques	ted 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

Reference ETSLTS 10 PICS Selection PICS_GN_S with	IUT sends the secured DENM using SignedData container 3 097 [1], clause 7.1.2 SECURITY Expected behaviour
PICS Selection PICS_GN_S with	SECURITY
with	
******	Expected behaviour

with the IUT is authorized with AT certificate (CERT_IUT_A_AT) ensure that when the IUT is requested to send a secured DENM then the IUT sends a EtsiTs103097Data containing content	

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 wi	th AT certificate (CERT_IUT_A_AT)		
ensure that			
when			
the IUT is requested to send a secured DENM			
then			
the IUT sends a EtsiTs103097Data			
containing content			
containing signedData			
containing tbsData			
containing headerInfo			
containin	containing psid		
indicating 'AID_DENM'			

6.2.3.3 Check header fields

	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,	
	p2pcdLearningRequest, missingCrlIdentifier, inlineP2pcdRequest, requestedCertificate	
Reference	ETSI TS 103 097 [1], clauses 5.2 and 7.1.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
vith		
the IUT is authorized with	AT certificate (CERT_IUT_A_AT)	
ensure that		
when		
the IUT is requested to send a secured DENM		
then		
the IUT sends a EtsiTs103097Data		
containing content		
containing signed		
containing tbsData		
containing headerInfo		
containing generationTime		
and containing generationLocation,		
and not containing expiryTime and not containing encryptionKey		
and not containing p2pcdLearningRequest and not containing missingCrlIdentifier		
and not containing missing cindentiner and not containing inlineP2pcdRequest		
and not containing requestedCertificate		

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	
Potoronoo	ETSI TS 103 097 [1], clause 7.1.2	
Reference	IEEE Std 1609.2 [2], clause 6.3.4	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT is authorized with	AT certificate (CERT_IUT_A_AT)	
ensure that		
when		
the IUT is requested to send a secured DENM		
then		
the IUT sends a EtsiTs103097Data		
containing content		
containing signedData		
containing signer		
containing certificate		
containing toBeSigned		
containing appPermissions		
	containing the item of type PsidSsp	
	ntaining psid	
indicating AID_DENM		

6.2.3.5 Check generation time

TP ld	TP_SEC_ITSS_SND_DENM_05_BV	
Summary	Check that IUT sends the secured DENM containing generation time and this time is inside	
	the validity period of the signing certificate	
	Check that message generation time value is realistic	
Reference	ETSI TS 103 097 [1], clause 7.1.2	
Reference	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 generationTime		
indicating GEN_TIME (CUR_TIME - 10min <= GEN_TIME <= CUR_TIME + 10 min)		
and containing signer		
containing certificate		
containing toBeSigned		
containing validityPeriod		
containing start		
indicating value X_START_VALIDITY (X_START_VALIDITY <= GEN_TIME)		
	ining duration	
indicating value > GEN_TIME - X_START_VALIDITY		

6.2.3.6 Check generation location

TP Id	TP_SEC_ITSS_SND_DENM_06_BV		
Summary	Check that IUT sends the secured DENM containing generation location when signing		
	certificate chain does not have any region restriction		
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			
the IUT has been author	ized with the AT certificate (CERT_IUT_A_AT)		
containing toBeSigned	d ·		
not containing regio	not containing region		
and issued by the cert	and issued by the certificate AA (CERT_IUT_A_AA)		
containing toBeSigr	containing toBeSigned not containing region		
not containing re			
and issued by the c	ertificate RCA (CERT_IUT_A_RCA)		
containing toBeSigned			
not containing region			
ensure that			
when			
the IUT is requested to send a secured DENM			
then			
the IUT sends a mess	age of type EtsiTs103097Data		
containing headerIn	nfo		
containing genera	ationLocation		

TP ld	TP_SEC_ITSS_SND_DENM_07_BV_ XX	
Summary	Check that IUT sends the secured DENM containing generation location which is inside	
Sullillary	the region defined by the validity restriction of the certificate pointed by the message signer	
Reference	ETSI TS 103 097 [1], clause 7.1.2	
	IEEE Std 1609.2 [2], clause 5.2.3.2.2	
PICS Selection PICS_GN_SECURITY AND PICS_SEC_CERTIFICATE_SELECTION AND X_PICS		
Expected behaviour		

with

the IUT has been authorized with the AT certificate (X_AT_CERTIFICATE)

containing toBeSigned containing region containing **X_FIELD** indicating REGION

ensure that

when

the IUT is requested to send a secured DENM

then

the IUT sends a message of type EtsiTs103097Data

containing headerInfo

containing generationLocation

indicating value inside the REGION

	Permutation Table			
_XX X_FIELD X_AT_CERTIFICATE X_PICS		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 Id	TP_SEC_ITSS_SND_DENM_09_BV		
Summary	Check that IUT sends the secured DENM containing generation location which is inside the identified region defined by the validity restriction of the AA certificate used to sign the certificate pointed by the message signer does not contain any region restriction		
Reference	ETSI TS 103 097 [1], clause 7.1.2 IEEE Std 1609.2 [2], clauses 5.2.3.2.2 and 6.4.8		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_CERTIFICATE_SELECTION		
Expected behaviour			

with

the IUT has been authorized with the AT certificate (CERT_IUT_CA1_AT)

containing toBeSigned not containing region

and issued by the certificate AA (CERT_IUT_CC_AA)

containing toBeSigned containing circularRegion

indicating REGION

and issued by the certificate RCA (CERT_IUT_C_RCA) containing toBeSigned

containing circularRegion

indicating REGION

ensure that

when

the IUT is requested to send a secured DENM

then

the IUT sends a message of type EtsiTs103097Data

containing headerInfo

containing generationLocation

indicating value inside the REGION

TP 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		
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 autho	rized with the AT certificate (CERT_IUT_CA2_AT)		
containing toBeSigne			
not containing regi			
	rtificate AA (CERT_IUT_CA_AA)		
containing toBeSigned			
	not containing region		
	and issued by the certificate RCA (CERT_IUT_C_RCA)		
•	containing toBeSigned		
containing circularRegion indicating REGION			
lensure that	REGION		
when			
	to send a secured DENM		
then	to dolla a dodalog BEITIVI		
the IUT sends a message of type EtsiTs103097Data			
containing headerl			
containing gene			
	indicating value inside the REGION		

6.2.3.7 Check payload

TP Id	TP_SEC_ITSS_SND_DENM_11_BV		
Summary	Check that IUT sends the secured DENM containing the 'data' field in signed data payload,		
	containing the EtsiTs103097Data of type unsecured, contained the DENM payload		
Reference	ETSI TS 103 097 [1], clauses 5.2 and 7.1.2		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT has been author	orized with the AT certificate (CERT_IUT_A_AT)		
ensure that			
when			
the IUT is requested to send a secured DENM			
then			
	the IUT sends a message of type EtsiTs103097Data		
contains content			
contains signedData			
containing tbsData			
containing payload			
containing data			
	ing content		
	aining unsecuredData		
containing not-empty data			

6.2.3.8 Check signing permissions

TP Id	TP_SEC_ITSS_SND_DENM_12_BV		
	Check that the IUT sends the secured DENM signed with the certificate containing		
	appPermissions allowing to sign DEN messages		
Reference	ETSI TS 103 097 [1], clause 7.1.2		
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	ized with the AT certificate (CERT_IUT_A_AT)		
ensure that			
when	when		
the IUT is requested to	the IUT is requested to send a secured DENM		
then	then		
the IUT sends a message of type EtsiTs103097Data			
containing signer	containing signer		
containing certificate			
containing appPermissions			
containing an item of type PsidSsp			
containin	g psid		
indicating AID_DENM			

6.2.3.9 Check signature

TDII	TR OFO ITOO OUR RENIM 40 RV	
TP ld	TP_SEC_ITSS_SND_DENM_13_BV	
	Check that IUT sends the secured DENM containing signature	
Summary	Check that the signature is calculated over the right fields and using right hash algorithm	
	by cryptographically verifying the signature	
Reference	ETSI TS 103 097 [1], clauses 5.2, 7.1.2	
Reference	IEEE Std 1609.2 [2], clauses 5.3.1, 6.3.4, 6.3.29, 6.3.30 and 6.3.31	
PICS Selection	PICS_GN_SECURITY AND X_PICS	
	Expected behaviour	
with	·	
the IUT is authorized with A	AT certificate (X_CERTIFICATE)	
containing verifyKeyIndic	cator	
containing verification	Key	
containing X_KEY	•	
indicating KEY		
ensure that		
when		
the IUT is requested to s	end a secured DENM	
then		
the IUT sends a messag	e of type EtsiTs103097Data	
containing signedData	1	
containing signer		
containing certific	cate	
indicating X_C	ERTIFICATE	
containing v	verifyKeyIndicator	
	g verificationKey	
containing X_KEY		
indicating KEY		
and containing sign	and containing signature	
containing X_SIG	GNATURE	
verifiable using KEY		
	Permutation table	

	Permutation 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

6.2.3.10 Check support for certificate content

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			
the IUT is authorized with	AT certificate (CERT_IUT_C_AT_8)		
containing toBeSigned	containing toBeSigned		
containing region	containing region		
containing rectang	containing rectangularRegion		
	containing 8 entries		
•	containing an entry (ENTRY)		
containing current IUT position			
ensure that			
when			
the IUT is requested to send a secured DENM			
then			
the IUT sends a message of type EtsiTs103097Data			
containing headerInf			
	containing generationLocation		
indicating positi	ion inside the ENTRY		

TP ld	TP SEC ITSS SND DENM 15 BV		
TF IU			
Summary	Check that the IUT supports at least 8 points in the polygonal certificate validity region in		
-	the AT certificate		
Reference	IEEE Std 1609.2 [2], clause 6.4.17		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_POLYGONAL_REGION		
	Expected behaviour		
with			
the IUT is authorized with	n AT certificate (CERT_IUT_D_AT_8)		
containing toBeSigned			
containing region			
containing polygo	nalRegion		
	containing 8 entries		
indicating polygon P			
and the IUT's position is inside the polygon P			
ensure that			
when			
the IUT is requested to send a secured DENM			
then			
the IUT sends a message of type EtsiTs103097Data			
containing headerInfo			
containing generationLocation			
indicating position inside the P			

TP Id	TD SEC ITSS SND DENM 46 DV	
I F IU	TP_SEC_ITSS_SND_DENM_16_BV	
Summary	Check that the IUT supports at least 8 points in the polygonal certificate validity region in	
Cammary	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	containing identifiedRegion	
containing 8 entries		
	containing one of the items (<i>I</i>)	
_	current IUT position	
ensure that	•	
when		
the IUT is requested to send a secured DENM		
then		
the IUT sends a message of type EtsiTs103097Data		
containing headerInfo		
containing genera	ationLocation	
indicating positi		

6.2.3.11 Check certificate consistency conditions

TP ld	TP_SEC_ITSS_SND_DENM_17_BV
Summary	Check that IUT does not send secured DENMs if IUT does not possess an AT certificate
<u></u>	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 as	uthorized with the AT certificate CERT_IUT_C1_AT)
containing region	
indicating recta	angular region
not containir	ng current IUT position
ensure that	
when	
the IUT is reques	sted to send a secured DENM
then	
uion	

TP Id	TP_SEC_ITSS_SND_DENM_18_BV
Summary	Check that IUT does not send the secured DENM if IUT is configured to use an AT certificate without region validity restriction and generation location is outside of the region of the issuing AA certificate
Reference	IEEE Std 1609.2 [2], clause 6.2.3.2.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
not containing reg and issued by the containing regio indicating red not contain	AA certificate (CERT_IUT_C3_AA)
ensure that when	
the IUT is requested to send a secured DENM then	
the IUT does not s	send DENM

TP Id	TP_SEC_ITSS_SND_DENM_19_BV
Cummory	Check that IUT does not send secured DENMs if all AT certificates installed on the IUT are
Summary	expired
Reference	IEEE Std 1609.2 [2], clause 6.2.3.2.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
	I with AT certificate (CERT_IUT_A1_AT)
containing validity	
	+ duration < CURRENT_TIME
and the IUT has no other installed AT certificates	
ensure that	
when	
the IUT is requested to send a secured DENM	
then	
the IUT does not s	send DENM

TP ld	TP_SEC_ITSS_SND_DENM_20_BV
Summary	Check that IUT does not send secured DENMs if all AT certificates installed on the IUT
	have the starting time in the future
Reference	IEEE Std 1609.2 [2], clause 6.2.3.2.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
containing validit indicating star	uthorized with the AT certificate (CERT_IUT_A2_AT) yPeriod t > CURRENT_TIME er certificates installed
the IUT is requested to send a secured DENM	
then	
the IUT does not	send DENM

TP Id	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 appPe not containing containing p indicating	PsidSSP
when the IUT is reques then the IUT does not	ted to 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	a AT certificate (CERT_IUT_A_AT) send a secured Beacon age of type EtsiTs103097Data Data

6.2.4.2 Check secured AID value

TP Id	TD SEC ITSS SND CENIMSC 02 DV		
I F IU	TP_SEC_ITSS_SND_GENMSG_02_BV		
Summary	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	when		
the IUT is requested to	send a secured Beacon		
then			
the IUT sends a message of type EtsiTs103097Data			
containing content			
containing signedData			
containing tbsData			
containing headerInfo			
containing psid			
indicating AID_GNMGMT			

6.2.4.3 Check header field

TP Id	TP_SEC_ITSS_SND_GENMSG_03_BV	
Summary	Check that IUT sends the secured GeoNetworking message with the headerInfo	
	containing generationTime	
Reference	ETSI TS 103 097 [1], clauses 5.2 and 7.1.3	
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER	
	Expected behaviour	
with		
the IUT is authorized v	with AT certificate (CERT_IUT_A_AT)	
ensure that		
when		
the IUT is requested	d to send a secured Beacon	
then		
the IUT sends a me	essage of type EtsiTs103097Data	
containing conte	nt	
containing sigr	nedData	
containing the		
	g headerInfo	
	ning generationTime	
and not containing expiryTime		
	and not containing generationLocation	
and not containing p2pcdLearningRequest		
and no	t containing missingCrlldentifier	

6.2.4.4 Check that signer info is a certificate or digest

TP Id	TP_SEC_ITSS_SND_GENMSG_04_BV		
Summary	Check that IUT sends the secured GeoNetworking message containing certificate or digest		
	as a signer		
Reference	ETSI TS 103 097 [1], clauses 5.2 and 7.1.3		
Kelelelice	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			
	send a secured Beacon		
	then		
	age of type EtsiTs103097Data		
	containing content		
containing signedData			
containing signer			
containing digest			
or containing certificate			
containing toBeSigned			
containing appPermissions			
	aining the item of type PsidSsp		
	ntaining psid		
	indicating AID_GNMGMT		

6.2.4.5 Check generation time

TP Id	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 authorized with	AT certificate (CERT_IUT_A_AT)
ensure that	
when	
· ·	send a secured Beacon
containing certificate	
then	(
	age of type EtsiTs103097Data
containing headerInf containing genera	
0 0	_TIME (CUR_TIME - 10 min <= GEN_TIME <= CUR_TIME + 10 min)
and containing signe	
containing certificate	
containing toBeSigned	
containing validityPeriod	
containing start	
indicatir	ng value X_START_VALIDITY (X_START_VALIDITY <= GEN_TIME)
and contain	ining duration
indicatir	ng value > GEN_TIME - X_START_VALIDITY

6.2.4.6 Check payload

TP Id	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 wit	th AT certificate (CERT_IUT_A_AT)		
ensure that			
when			
the IUT is requested t	o send a secured Beacon		
then			
the IUT sends a mess	the IUT sends a message of type EtsiTs103097Data		
contains content			
	contains signedData		
	containing tbsData		
containing payload			
containing data			
containing content			
cont	containing unsecuredData		
containing not-empty data			

6.2.4.7 Check signing permissions

TP Id TP_SEC_ITSS_SND_GENMSG_07_BV Check that the IUT sends the secured messages signed with the certificate containing appPermissions allowing to sign these messages ETSI TS 103 097 [1], clause 7.1.3 IEEE Std 1609.2 [2], clause 5.2.3.2.2		
Reference appPermissions allowing to sign these messages ETSI TS 103 097 [1], clause 7.1.3 IEEE Std 1609.2 [2], clause 5.2.3.2.2		
Reference ETSI TS 103 097 [1], clause 7.1.3 IEEE Std 1609.2 [2], clause 5.2.3.2.2		
IEEE Std 1609.2 [2], clause 5.2.3.2.2		
IEEE Std 1609.2 [2], clause 5.2.3.2.2		
PICS Selection PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER		
Expected behaviour		
with		
the IUT has been authorized with the AT certificate (CERT_IUT_A_AT)		
ensure that		
when		
the IUT is requested to send Beacon		
then		
the IUT sends a message of type EtsiTs103097Data		
containing signer		
containing certificate		
containing appPermissions		
containing an item of type PsidSsp		
containing psid		
indicating value AID_GNMGMT		

6.2.4.8 Check signature

TP ld	TP_SEC_ITSS_SND_GENMSG_08_BV	
11 14	Check that IUT sends the secured GeoNetworking message containing signature	
Summary	Check that the signature is calculated over the right fields and using right hash algorithm	
Julillal y	by cryptographically verifying the signature	
	ETSI TS 103 097 [1], clauses 5.2 and 7.1.3	
Reference	IEEE Std 1609.2 [2], clauses 5.3.1, 6.3.4, 6.3.29, 6.3.30 and 6.3.31	
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER AND X_PICS	
1100 0010011011	Expected behaviour	
with	Expedica seriavioai	
	ith AT certificate (X_CERTIFICATE)	
containing verifyKeyl		
containing verificat		
containing X_KI		
indicating KEY		
ensure that		
when		
the IUT is requested to send a secured Beacon		
then		
the IUT sends a message of type EtsiTs103097Data		
containing signedData		
containing signer		
containing digest		
referencing the certificate X_CERTIFICATE		
or containing certificate		
indicating X_CERTIFICATE		
and containing signature		
containing X_SIGNATURE		
verifiable u	sing KEY	

Permutation 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 authorize	d with the certificate CERT_IUT_A_AT		
and the IUT current time i	and the IUT current time is inside the time validity period of CERT_TS_A_AT and CERT_IUT_A_AT		
ensure that	· ·		
when	when		
the IUT is receiving a message of type EtsiTs103097Data			
signed using CERT_TS_A_AT			
and containing protocol_version			
indicating 3			
then			
the IUT forwards the SecuredMessage to the Facility layers			

TP Id	TP_SEC_ITSS_RCV_MSG_01_BO		
S. mmor.	Check that IUT discards a secured message containing protocol version set to a value less		
Summary	than 3		
Reference	ETSI TS 103 097 [1], clause 5.1		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT is being aut	horized with the certificate CERT_IUT_A_AT		
•	and the IUT current time is inside the time validity period of CERT TS A AT and CERT IUT A AT		
ensure that			
when			
the IUT is receivi	the IUT is receiving a message of type EtsiTs103097Data		
signed using CERT_TS_A_AT			
and containing protocol_version			
indicating 2			
then			
the IUT discards the SecuredMessage			

TP Id	TP_SEC_ITSS_RCV_MSG_02_BO		
S	Check that IUT discards a secured message containing protocol version set to a value		
Summary	greater than 3		
Reference	ETSI TS 103 097 [1], clause 5.1		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT is being aut	horized with the certificate CERT_IUT_A_AT		
and the IUT current	and the IUT current time is inside the time validity period of CERT_TS_A_AT and CERT_IUT_A_AT		
ensure that			
when	when		
the IUT is receiving a message of type EtsiTs103097Data			
signed using CERT_TS_A_AT			
and containing protocol_version			
indicating 4			
then			
the IUT discards the SecuredMessage			

6.3.2 CAM profile

6.3.2.1 Check the valid message receiving

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		
rics selection	Expected behaviour		
with	Expected benaviour		
	therized etate		
the IUT being in the 'au			
ensure that	e (CUR_TIME) is inside the time validity period of CERT_TS_A_AT		
when			
	a message of type EtsiTs103097Data (MSG)		
containing proto			
indicating 3	COLVELSION		
	content.signedData		
containing h			
	g hash algorithm of the verification key of CERT_TS_A_AT		
and containi			
	g payload		
	containing data		
containing protocolVersion			
indicating 3			
and containing content.unsecuredData			
	containing CAM payload		
and conta	aining headerInfo		
containing psid			
indicating CAM AID value			
and containing generationTime			
indicating time within 2sec around the CUR_TIME			
and NOT containing other headers			
and containing signer			
	containing certificate		
containing 1 item of type EtsiTs103097Certificate			
indicating CERT_TS_A_AT			
and containing signature containing ecdsaNistP256Signature			
	ining rSig.x-only		
	d over the MSG.content.signedData.tbsData		
	verification key of CERT_TS_A_AT		
then			
	the IUT accepts the SecuredMessage		

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 'auth	norized' state		
	(CUR_TIME) is inside the time validity period of CERT_TS_A_AT		
and the IUT has already	received the message signed with CERT_TS_A_AT		
ensure that			
when			
the IUT is receiving a message of type EtsiTs103097Data			
indicating the message described in TP_SEC_ITSS_RCV_CAM_01_BV			
and containing content.signedData.signer			
containing digest			
indicating HashedId8 value			
referencing the CERT_TS_A_AT			
then	then		
the IUT accepts the SecuredMessage			

```
TP Id
                          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
   the IUT being in the 'authorized' state
   and the IUT current time (CUR_TIME) is inside the time validity period of CERT_TS_A_AT
ensure that
   when
      the IUT is receiving a message of type EtsiTs103097Data (MSG)
         indicating the message described in TP_SEC_ITSS_RCV_CAM_01_BV
         and containing content.signedData.signature
             containing ecdsaNistP256Signature
                containing rSig.compressed-y-0
                or containing rSig.compressed-y-1
             calculated over the MSG.content.signedData.tbsData
                using verification key of CERT_TS_A_AT
      the IUT accepts the SecuredMessage
```

TP ld	TP_SEC_ITSS_RCV_CAM_04_BV_ <i>XX</i>			
Summary	Check that IUT accepts a valid secured CAM message signed with certificate containing			
	region restriction			
Reference ETSI TS 103 097 [1], clause 7.1.1				
PICS Selection	PICS_GN_SECURITY AND X_PICS			
	Expected behaviour			
with				
the IUT being in the 'au	thorized' state			
and the IUT current time	e (CUR_TIME) is inside the time validity period of X_AT_CERTIFICATE			
and the IUT current pos	sition is inside the region restriction of X_AT_CERTIFICATE			
ensure that				
when				
	a message of type EtsiTs103097Data (MSG)			
indicating the me	essage described in TP_SEC_ITSS_RCV_CAM_01_BV			
and containing content.signedData				
containing signer				
containing certificate				
containing 1 item of type EtsiTs103097Certificate				
indicating X_AT_CERTIFICATE				
containing toBeSigned.region				
containing X_FIELD				
and containing signature				
containing ecdsaNistP256Signature				
containing rSig.x-only				
calculate	d over the MSG.content.signedData.tbsData			
using	verification key of X_AT_CERTIFICATE			
then				
the IUT accepts the	SecuredMessage			

the IUT accepts the 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
04	identifiedRegion	CERT TS E AT	PICS SEC IDENTIFIED REGION

TP ld	TP_SEC_ITSS_RCV_CAM_05_BV		
Summary	Check that IUT accepts a valid secured CAM message signed using the brainpoolP256r1		
Cullillal y	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			
	a message of type EtsiTs103097Data		
	ssage described in TP_SEC_ITSS_RCV_CAM_01_BV		
•	and containing content.signedData		
	containing signer		
containing certificate			
	containing 1 item of type EtsiTs103097Certificate		
indicating CERT_TS_A_B_AT			
containing toBeSigned.verifyKeyIndicator.verificationKey			
containing ecdsaBrainpoolP256r1			
and containing signature			
containing ecdsaBrainpoolP256r1Signature			
containing rSig.x-only			
	l over the MSG.content.signedData.tbsData		
	verification key of CERT_TS_A_B_AT		
then	Coourad Mooonage		
the IUT accepts the	Securearilessage		

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 'aut	horized' state		
and the IUT current time	e (CUR_TIME) is inside the time validity period of CERT_TS_A_B3_AT		
ensure that			
when			
	a message of type EtsiTs103097Data		
	ssage described in TP_SEC_ITSS_RCV_CAM_01_BV		
•	and containing content.signedData		
containing signer			
	g certificate		
	containing 1 item of type EtsiTs103097Certificate		
ind	indicating CERT_TS_A_B3_AT		
containing toBeSigned. verifyKeyIndicator.verificationKey			
containing ecdsaBrainpoolP384r1			
and containing signature			
containing ecdsaBrainpoolP384r1Signature			
containing rSig.x-only calculated over the MSG.content.signedData.tbsData			
	verification key of CERT_TS_A_B3_AT		
then	verilloation key of OLICI_10_A_D0_A1		
the IUT accepts the	SecuredMessage		
inc to t accepts the t	Occurrentiosage		

6.3.2.2 Check invalid HeaderInfo elements

	-	
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	
- Carrinary	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 '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 r	nessage of type EtsiTs103097Data	
indicating the messa	age described in TP_SEC_ITSS_RCV_CAM_02_BV	
and containing SignedData		
containing ToBeSignedData		
containing HeaderInfo		
containing Psid		
not indicating CAM AID value		
then		
the IUT discards the SecuredMessage		

TP Id TP_SEC_ITSS_RCV_CAM_02_BO		
Summary	Check that IUT discards a secured CAM if the HeaderInfo contains the header field	
	generationLocation	
Reference	ETSI TS 103 097 [1], clause 7.1.1	
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 ToBeSignedData		
containing HeaderInfo		
containing psid		
indicating CAM AID value		
and containing generationLocation		
then		
the IUT discards the SecuredMessage		

TP ld	TP_SEC_ITSS_RCV_CAM_03_BO	
Summary	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 '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 r	message of type EtsiTs103097Data	
containing SignedDa	ata	
containing ToBeSignedData		
containing HeaderInfo		
containing psid		
indicating CAM AID value		
and containing	ng expiryTime	
then		
the IUT discards the S	ecuredMessage	

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 'author	orized' state		
and the IUT current time i	s inside the time validity period of CERT_TS_A_AT		
ensure that			
when	when		
	nessage of type EtsiTs103097Data		
containing SignedDa			
	containing ToBeSignedData		
containing HeaderInfo			
containing psid			
indicating CAM AID value			
and containing p2pcdLearningRequest			
then			
the IUT discards the SecuredMessage			

TP ld	TP_SEC_ITSS_RCV_CAM_05_BO		
Summary	Check that IUT discards a secured CAM if the HeaderInfo contains the header field		
	missingCrlldentifier		
Reference	ETSI TS 103 097 [1], clause 7.1.1		
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	when		
the IUT is receiving a r	message of type EtsiTs103097Data		
containing SignedDa	ata		
containing ToBeS	containing ToBeSignedData		
containing Hea	containing HeaderInfo		
containing psid			
indicating CAM AID value			
and containing missingCrlldentifier			
then			
the IUT discards the SecuredMessage			

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	Reference ETSI TS 103 097 [1], clause 7.1.1		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
With			
the IUT being in the 'auth	orized' state		
and the IUT current time i	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 ToBeS			
containing Hea	derInfo		
containing ps	sid		
indicating	CAM AID value		
and containir	ng encryptionKey		
then			
the IUT discards the Se	ecuredMessage		

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		
ensure that when the IUT is receiving a r containing SignedDa containing Signati	is inside the time validity period of CERT_TS_A_AT nessage of type EtsiTs103097Data ata ure g signature algorithm		

TP Id	TP_SEC_ITSS_RCV_CAM_08_BO		
Check that IUT discards a secured CAM if the 'SignerIdentifier' contains an invalid choice			
Reference	leference ETSI TS 103 097 [1], clause 6		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT being in the 'author and the IUT current time i ensure that when	orized' state s inside the time validity period of CERT_TS_A_AT		
the IUT is receiving a message of type EtsiTs103097Data containing SignedData containing SignerIdentifier indicating 'self'			
then the IUT discards the Se	ecuredMessage		

TP Id	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		
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 r	the IUT is receiving a message of type EtsiTs103097Data		
containing Signature			
indicating an altered value			
then			
the IUT discards the SecuredMessage			

6.3.3 DENM profile

6.3.2.1 Check the valid message receiving

TP Id	TP_SEC_ITSS_RCV_DENM_01_BV		
Summary	Check that IUT accepts a valid secured DENM 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			
	e (CUR_TIME) is inside the time validity period of CERT_TS_A_AT		
ensure that			
when	(
	a message of type EtsiTs103097Data (MSG)		
containing protoc	corversion		
indicating 3	ontent.signedData		
containing ha			
	hash algorithm of the verification key of CERT_TS_A_AT		
and containir			
containing			
	ning data		
со	containing protocolVersion		
	indicating 3		
an	d containing content.unsecuredData		
and soute	containing DENM payload		
	aining headerInfo		
containing psid			
indicating DENM AID value and containing generationTime			
and containing generation lime indicating time within 2sec around the CUR_TIME			
and containing generationLocation			
and NOT containing other headers			
and containing signer			
containing certificate			
containing 1 item of type EtsiTs103097Certificate			
indicating CERT_TS_A_AT			
and containing signature			
containing ecdsaNistP256Signature containing rSig.x-only			
containing rsig.x-only calculated over the MSG.content.signedData.tbsData			
using verification key of CERT_TS_A_AT			
then	·		
the IUT accepts the SecuredMessage			

TP ld	TP_SEC_ITSS_RCV_DENM_02_BV_ XX	
Summary Check that IUT accepts a valid secured DENM message signed with certificate containing region restriction		
Reference	Reference ETSI TS 103 097 [1], clause 7.1.1	
PICS Selection PICS_GN_SECURITY AND X_PICS		
Expected behaviour		

with

the IUT being in the 'authorized' state

and the IUT current time (CUR_TIME) is inside the time validity period of **X_AT_CERTIFICATE** and the IUT current position is inside the region restriction of **X_AT_CERTIFICATE**

ensure that

when

the IUT is receiving a message of type EtsiTs103097Data (MSG)

indicating the message described in TP_SEC_ITSS_RCV_DENM_01_BV

and containing content.signedData

containing tbsData

containing headerInfo

containing generationLocation

indicating location inside the X_AT_CERTIFICATE region restriction

and containing signer

containing certificate

containing 1 item of type EtsiTs103097Certificate

indicating X_AT_CERTIFICATE
containing toBeSigned.region
containing X_FIELD

and containing signature

containing ecdsaNistP256Signature

containing rSig.x-only

calculated over the MSG.content.signedData.tbsData

using verification key of X_AT_CERTIFICATE

then

the IUT accepts the 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
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	eference 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			
	a message of type EtsiTs103097Data (MSG)		
	ssage described in TP_SEC_ITSS_RCV_DENM_01_BV		
_	ontent.signedData		
containing sig			
	g certificate		
	ning 1 item of type EtsiTs103097Certificate		
indicating CERT_TS_A_B_AT			
containing toBeSigned.verifyKeyIndicator.verificationKey			
containing ecdsaBrainpoolP256r1			
and containing signature			
	g ecdsaBrainpoolP256r1Signature		
containing rSig.x-only			
calculated over the MSG.content.signedData.tbsData using verification key of CERT_TS_A_B_AT			
then	Verification key of OLIVI_10_A_D_A1		
the IUT accepts the	SecuredMessage		

TP ld	TP_SEC_ITSS_RCV_DENM_04_BV		
Summary	Check that IUT accepts a valid secured DENM message signed using the brainpoolP384r1		
	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 'aut			
and the IUT current time	e (CUR_TIME) is inside the time validity period of CERT_TS_A_B3_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			
	g certificate		
containing 1 item of type EtsiTs103097Certificate			
indicating CERT_TS_A_B3_AT			
containing toBeSigned. verifyKeyIndicator.verificationKey			
containing ecdsaBrainpoolP384r1			
and containing signature			
containing ecdsaBrainpoolP384r1Signature containing rSig.x-only			
calculated over the MSG.content.signedData.tbsData			
using verification key of CERT_TS_A_B3_AT			
then	To modify of 02.11_10_11_50_111		
the IUT accepts the	SecuredMessage		

6.3.3.2 Check invalid HeaderInfo elements

TP ld	TP_SEC_ITSS_RCV_DENM_01_BO		
Summary	Check that IUT discards a secured DENM if the HeaderInfo contains the header field an		
	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 'autl	norized' state		
and the IUT current time	is inside the time validity period of CERT_TS_A_AT		
ensure that			
when	when		
	message of type EtsiTs103097Data		
containing SignedD	pata Pata		
containing ToBes	containing ToBeSignedData		
containing HeaderInfo			
containing Psid			
not indicating DENM AID value			
then			
the IUT discards the SecuredMessage			

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		
	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	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	the IUT is receiving a message of type EtsiTs103097Data		
containing SignedDa	ata		
containing ToBeSignedData			
containing HeaderInfo			
containing Psid			
indicating DENM AID value			
and not containing generationLocation			
then			
the IUT discards the Se	ecuredMessage		

TP ld	TP_SEC_ITSS_RCV_DENM_03_BO	
Summary	Check that IUT discards a secured DENM if the HeaderInfo contains the header field	
Summary	expiryTime	
Reference	ETSI TS 103 097 [1], clause 7.1.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
With		
the IUT being in the 'autho	orized' state	
and the IUT current time i	s inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
· ·	the IUT is receiving a message of type EtsiTs103097Data	
	containing SignedData	
containing ToBeSignedData		
containing HeaderInfo		
containing Psid		
indicating DENM AID value		
and containing expiryTime		
then		
the IUT discards the 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 '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	the IUT is receiving a message of type EtsiTs103097Data		
containing SignedDa	ata		
containing ToBeSignedData			
containing HeaderInfo			
containing Pa	sid		
indicating DENM AID value			
and containing p2pcdLearningRequest			
then			
the IUT discards the Se	ecuredMessage		

TP ld	TP_SEC_ITSS_RCV_DENM_05_BO		
Summary	Check that IUT discards a secured DENM if the HeaderInfo contains the header field		
	missingCrlldentifier		
Reference	ETSI TS 103 097 [1], clause 7.1.2		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
With			
the IUT being in the 'author	orized' state		
and the IUT current time i	is inside the time validity period of CERT_TS_A_AT		
ensure that			
when	when		
	nessage of type EtsiTs103097Data		
containing SignedDa			
containing ToBeS	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	ETSÍ TS 103 097 [1], clause 7.1.2		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
With			
the IUT being in the 'au	ıthorized' state		
and the IUT current tim	e is inside the time validity period of CERT_TS_A_AT		
ensure that			
when	when		
the IUT is receiving	the IUT is receiving a message of type EtsiTs103097Data		
containing Signed	Data		
containing ToB	containing ToBeSignedData		
containing H	containing HeaderInfo		
containing Psid			
indicating DENM AID value			
and containing encryptionKey			
then			
the IUT discards the SecuredMessage			

6.3.3.3 Check invalid Signature elements

TP Id	TP SEC ITSS RCV DENM 07 BO	
Summary	Check that ILIT discards a secured DENM if the 'SignedData' contains an invalid signatur	
Reference	ETSI TS 103 097 [1], clause 6	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
ensure that when the IUT is receiving a r containing SignedDa containing Signat	is inside the time validity period of CERT_TS_A_AT message of type EtsiTs103097Data ata ure g signature algorithm	

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 'a	authorized' state		
and the IUT current ti	and the IUT current time is inside the time validity period of CERT_TS_A_AT		
ensure that			
when			
the IUT is receiving	g a message of type EtsiTs103097Data		
containing Signe	containing SignedData		
containing SignerIdentifier			
indicating 'self'			
then			
the IUT discards th	ne SecuredMessage		

TP Id	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	PICS_GN_SECURITY		
	Expected behaviour		
ensure that when	nessage of type EtsiTs103097Data ed value		

Annex A (informative): Bibliography

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

History

Document history		
V1.1.1	July 2013	Publication
V1.2.1	September 2015	Publication
V1.3.1	March 2017	Publication
V1.4.1	August 2018	Publication
V1.5.1	January 2022	Publication