ETSITS 103 096-2 V1.4.1 (2018-08)



Intelligent Transport Systems (ITS); Testing;

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

Reference RTS/ITS-00543

Keywords

ITS, security, testing, TSS&TP

ETSI

650 Route des Lucioles F-06921 Sophia Antipolis Cedex - FRANCE

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

Siret N° 348 623 562 00017 - NAF 742 C Association à but non lucratif enregistrée à la Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

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

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

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

Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

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

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

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

© ETSI 2018. All rights reserved.

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 logo is protected for the benefit of its Members. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

Intelle	ectual Property Rights	5
Forew	vord	5
Moda	ıl verbs terminology	5
1	Scope	6
2	References	6
2.1	Normative references	
2.1	Informative references	
3	Definitions and abbreviations	
3.1	Definitions	
3.2	Abbreviations	/
4	Test Suite Structure (TSS)	8
4.1	Structure for Security tests	8
5	Test Purposes (TP)	8
5.1	Introduction	
5.1.1	TP definition conventions	
5.1.2	TP Identifier naming conventions	
5.1.3	Rules for the behaviour description	
5.1.4	Sources of TP definitions	
5.1.5	Mnemonics for PICS reference	9
6	ITS-S Security	Q
6.1	Overview	
6.2	Sending behaviour	
6.2.1	Check the message protocol version	
6.2.2	CAM profile	
6.2.2.1		
6.2.2.2		
6.2.2.3		
6.2.2.4	6	
6.2.2.5		
6.2.2.6 6.2.2.7		
6.2.2. <i>1</i> 6.2.2.8		
6.2.2.9		
6.2.2.1		
6.2.2.1	č	
6.2.2.1	1 •	
6.2.2.1		
6.2.2.1	· · · · · · · · · · · · · · · · · · ·	
6.2.3	DENM profile	
6.2.3.1	č	
6.2.3.2 6.2.3.3		
6.2.3.4 6.2.3.4		
6.2.3.5		
6.2.3.6		
6.2.3.7		
6.2.3.8		
6.2.3.9		
6.2.3.1		
6.2.4	Generic signed message profile	
6.2.4.1		
6.2.4.2		
6.2.4.3	3 Check header field	34

6.2.4.4	Check that signer info is a certificate or digest		
6.2.4.5	Check generation time		
6.2.4.6	Check payload		
6.2.4.7	Check signing permissions	36	
6.2.4.8	Check signature	36	
6.2.5	Encrypted messages profile		
6.2.5.1	Check encrypted message generation	37	
6.2.5.2	Check recipient information		
6.2.5.3	Check encrypted data content	38	
6.2.5.4	Check encrypted and signed data	39	
6.2.6	Profiles for certificates		
6.2.6.1	Check that certificate version is 3	39	
6.2.6.2	Check basic certificate conformance to ETSI TS 103 097	40	
6.2.6.3	Check the issuer reference of the certificate	40	
6.2.6.4	Check rectangular region validity restriction	41	
6.2.6.5	Check polygonal region validity restriction	42	
6.2.6.6	Check identified region validity restriction	43	
6.2.6.7	Check time validity restriction in the chain	45	
6.2.6.8	Check ECC point type of the certificate signature	45	
6.2.6.9	Check ECC point type of the certificate public keys	46	
6.2.6.10	Verify certificate signatures		
6.2.6.11	Verify certificate permissions	47	
6.2.6.12	AT and AA certificate profiles	50	
Annex A	(informative): Bibliography	51	
History		52	

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

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

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

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

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

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

Modal verbs terminology

In the present document "shall", "shall not", "should", "should not", "may", "need not", "will", "will not", "can" and "cannot" are to be interpreted as described in clause 3.2 of the <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 (V1.3.1): "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 (V1.4.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)".
- [4] ETSI TS 102 871-1 (V1.4.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma".
- [5] United Nations Statistics Division: "Composition of Macro Geographical (Continental) Regions, Geographical Sub-Regions, and Selected Economic and Other Groupings".

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

2.2 Informative references

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

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

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

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

[i.2]	ETSI TS 102 965 (V1.3.1): "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration".
[i.3]	ISO/IEC 9646-1 (1994): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 1: General concepts".
[i.4]	ISO/IEC 9646-2 (1994): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 2: Abstract Test Suite specification".
[i.5]	ISO/IEC 9646-6 (1994): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 6: Protocol profile test specification".
[i.6]	ISO/IEC 9646-7 (1995): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 7: Implementation Conformance Statements".
[i.7]	ETSI ETS 300 406 (1995): "Methods for testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

3 Definitions and abbreviations

3.1 Definitions

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

3.2 Abbreviations

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

AA Authorization Authority
AID Application Identifier

AID_CAM ITS Application Identifier for CAM AID_DENM Application Identifier for DENM

AID_GN Application Identifier for general GeoNetworking messages

AT Authorization Ticket
ATS Abstract Test Suite
BO Exceptional Behaviour
BV Valid Behaviour
CA Certificate Authority

CAM Co-operative Awareness Messages

CAN Controller Area Network

CERT Certificate

COER Cannonical Octet Encoding Rules

DE Data Element

DEN Decentralized Environmental Notification

DENM Decentralized Environmental Notification Message

EA Enrolment Authority

ECC Elliptic Curve Cryptography

GN GeoNetworking

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

IUT Implementation under Test

MSG Message

PICS Protocol Implementation Conformance Statement

PSID Provider Service Identifier RCA Root Certificate Authority SSP Service Specific Permissions

TP Test Purposes

Test Suite Structure

4 Test Suite Structure (TSS)

4.1 Structure for Security tests

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

Table 1: TSS for Security

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

5 Test Purposes (TP)

5.1 Introduction

5.1.1 TP definition conventions

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

5.1.2 TP Identifier naming conventions

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

Table 2: TP naming convention

Identifier	TP_ <root>_<tgt>_<gr>_<sgr>_<rn>_<sn>_<x></x></sn></rn></sgr></gr></tgt></root>		
	<root> = root</root>	SEC	
	<tgt> = target</tgt>	ITSS	ITS-S data transfer
		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

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 1609.2TM[2].

5.1.5 Mnemonics for PICS reference

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

Table 3: Mnemonics for PICS reference

	Mnemonic	PICS item
1	PICS_GN_SECURITY	A.2/1 [4]
2	PICS_SEC_CERTIFICATE_SELECTION	A.8/1 [3]
3	PICS_SEC_CIRCULAR_REGION	S1.2.2.5.1.1 [2]
4	PICS_SEC_RECTANGULAR_REGION	S1.2.2.5.1.2 [2]
5	PICS_SEC_POLYGONAL_REGION	S1.2.2.5.1.3 [2]
6	PICS_SEC_IDENTIFIED_REGION	S1.2.2.5.1.4 [2]
7	PICS_SEC_ITS_AID_OTHER	A.7/1 [3]
8	PICS_SEC_SHA256	S1.2.2.1.1 [2]
9	PICS_SEC_SHA384	S1.2.2.1.2 [2]
10	PICS_SEC_BRAINPOOL_P256R1	S1.2.2.4.1.2 [2]
11	PICS_SEC_BRAINPOOL_P384R1	S1.2.2.4.2 [2]

6 ITS-S Security

6.1 Overview

Void.

6.2 Sending behaviour

6.2.1 Check the message protocol version

TP Id	TP_SEC_ITSS_SND_MSG_01_BV		
Summary	Check that the IUT sends a secured message containing protocol version set to 3		
Reference	ETSI TS 103 097 [1], clause 5.1		
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 reque	the IUT is requested to send a secured message		
then			
the IUT sends a EtsiTs103097Data			
containing protocolVersion			
indicating value '3'			

6.2.2 CAM profile

6.2.2.1 Check that secured CAM is signed

TP ld	TP_SEC_ITSS_SND_CAM_01_BV		
Summary	Check that IUT sends the secured CAM using SignedData container		
Reference	ETSI TS 103 097 [1], clause 7.1.1		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT is authorized with	n 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			
containing signedData			

6.2.2.2 Check secured CAM AID value

TP Id	TP_SEC_ITSS_SND_CAM_02_BV		
Summary	Check that IUT sends the secured CAM containing the HeaderInfo field psid set to		
Odiffilial y	'AID_CAM'		
Reference	ETSI TS 103 097 [1], clause 7.1.1		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT is authorized with	AT certificate (CERT_IUT_A_AT)		
ensure that			
when			
the IUT is requested to	send a secured CAM		
then			
	the IUT sends a message of type EtsiTs103097Data		
containing content			
containing signedData			
containing tbsData			
containing headerInfo			
containing psid			
indicating 'AID_CAM'			

6.2.2.3 Check header fields

TP Id	TP_SEC_ITSS_SND_CAM_03_BV		
	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, 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	then		
the IUT sends a mess	age of type EtsiTs103097Data		
containing content			
containing signedData			
containing tbs[Data		
containing headerInfo			
	containing generationTime		
and not co	and not containing expiryTime		
	and not containing generationLocation,		
	ontaining encryptionKey		
	ontaining p2pcdLearningRequest		
and not co	ontaining missingCrlldentifier		

6.2.2.4 Check signer information

TP ld	TP_SEC_ITSS_SND_CAM_04_BV	
	Check that IUT sends the secured CAM containing signer containing either certificate or	
Summary	digest	
	Check that signing certificate has permissions to sign CAM messages	
Reference	ETSI TS 103 097 [1], clauses 5.2, 7.1.1	
Kelelelice	IEEE Std 1609.2 [2], clause 6.3.4	
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	(
	age of type EtsiTs103097Data	
containing content		
containing signed containing sign		
containing sign		
or containing digest		
containing to Be Signed		
containing appPermissions		
containing the item of type PsidSsp		
	ntaining psid	
	indicating AID_CAM	

Expected behaviour		
PICS Selection	PICS_GN_SECURITY AND X_PICS	
Reference	IEEE Std 1609.2 [2], clause 6.3.4	
,	ETSI TS 103 097 [1], clauses 5.2, 7.1.1	
	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 digest

then

the IUT sends a message of type EtsiTs103097Data

containing content containing signedData containing signer containing digest

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

Permutation table X_HASH X_

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	I S Η Δ = 3 Χ /I	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1
CN	CERT_IUT_A_B3_N_AT	ecdsaBrainpoolP384r1 (uncompressed)	ISHA-384	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1

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

with

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

and the IUT having sent a secured CAM

containing generationTime

indicating TIME_LAST

ensure that

when

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

containing signer containing certificate

then

this message is containing headerInfo

containing generationTime

indicating TIME (TIME >= TIME_LAST + 1 sec)

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

6.2.2.5 Check that IUT sends certificate to unknown ITS-S

TP ld	TP_SEC_ITSS_SND_CAM_08_BV		
Summary	Check that IUT sends the secured CAM containing the signing certificate when the IUT		
	received a CAM from an unknown ITS-S		
Reference ETSI TS 103 097 [1], clause 7.1.1			
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT is authorized with	AT certificate (CERT_IUT_A_AT)		
and the IUT is configured	to send more than one CAM per second		
and the IUT having alread	dy 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_B_AT)			
at TIME_2 (TIME_1 < TIME_2 < TIME_1+1 sec)			
ensure that			
when			
the IUT is requested to send secured CAM			
at TIME_3 (TIME_1 < TIME_2 < TIME_3 < TIME_1 + 1 sec)			
then			
	the IUT sends a message of type EtsiTs103097Data		
containing signedDa	ta		
containing signer			
containing certif	ficate		

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

_			
TP Id	TP_SEC_ITSS_SND_CAM_09_BV		
Summary	Check that IUT restarts the certificate sending timer when the signing certificate was sent		
Reference	ETSI TS 103 097 [1], clause 7.1.1		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with	•		
the IUT is authorized wi	th AT certificate (CERT_IUT_A_AT)		
and the IUT is configure	ed to send more than one CAM per second		
and the IUT having alrea			
containing signer			
containing certifica	te		
at TIME_1			
and the IUT having rece	and the IUT having received a secured CAM		
containing signer			
containing digest	containing digest		
indicating Hashl			
•	n unknown certificate		
at TIME_2 (TIME_1 +			
	and the IUT having sent secured CAM		
containing signer			
containing certificate			
at TIME_3 (TIME_3 > TIME_2)			
ensure that			
when	and account OAM		
the IUT is sending the next secured CAM			
containing signedData			
containing signer			
	containing certificate		
at TIME_4 then			
	on TIME 4 and TIME 2 is shout 1 ass		
the difference between TIME_4 and TIME_3 is about 1 sec			

6.2.2.7 Check sending certificate request for unknown certificate

TP ld	TP_SEC_ITSS_SND_CAM_10_BV		
Summary	Check that the IUT sends certificate request when it receives secured CAM containing		
Summary	digest of unknown certificate as a message signer		
Deference	ETSI TS 103 097 [1], clause 7.1.1		
Reference	IEEE Std 1609.2 [2], clauses 6.3.9, 8.2.4.1.2		
PICS Selection	PICS_GN_SECURITY, PICS_SEC_P2P_AT_DISTRIBUTION		
	Expected behaviour		
with	•		
the IUT is authorized wit	h AT certificate (CERT_IUT_A_AT)		
and the IUT has receiving	g a EtsiTs103097Data		
containing signer			
containing digest			
indicating Hashe	dld8 value DIGEST_A		
referencing an	referencing an unknown certificate (CERT_TS_B_AT)		
ensure that	· · · · · · · · · · · · · · · · · · ·		
when			
the IUT is requested t	the IUT is requested to send a secured CAM		
then			
the IUT sends a message of type EtsiTs103097Data			
containing headerInfo			
containing inlineP2pcdRequest			
containing HashedId3 value			
indicating last 3 octets of DIGEST_A			

7.7.	\(\alpha_1\) 100	
XX	X FIELD 1 X PICS	
indicating last 3 octets of DIGEST Permutation table		
containing HashedId3 value		
containing inlineP2pcdRequest		
	headerInfo	
containing tb		
containing sign		
the IUT sends a n	essage of type EtsiTs103097Data	
then		
	ed to send secured CAM	
when		
ensure that	noing an unknown certificate	
	g HashedId8 value DIGEST ncing an unknown certificate	
	X_FIELD_1	
containing is		
containing certi		
containing signer		
	iving a message of type EtsiTs103097Data	
	with AT certificate (CERT_IUT_A_AT)	
with	Exposion soliuvioni	
	Expected behaviour	
rica selection	AND PICS_SEC_P2P_AA_DISTRIBUTION AND X PICS	
PICS Selection	PICS_GN_SECURITY	
	IEEE Std 1609.2 [2], clauses 6.3.9, 8.2.4.1.2	
Reference	ETSI TS 103 097 [1], clause 7.1.1	
Julilliai y	certificate signed by unknown AA certificate	
Summary	Check that the IUT sends certificate request when it receives secured CAM	containing
TP ld	TP_SEC_ITSS_SND_CAM_11_BV_ <i>XX</i>	

PICS_SEC_SHA384

sha256AndDigest sha384AndDigest

6.2.2.8 Check that IUT sends AT certificate when requested

TP ld	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		
	IEEE Std 1609.2 [2], clauses 6.3.9, 8.2.4.2.3		
PICS Selection	PICS_GN_SECURITY		
r 103 Selection	AND PICS_SEC_P2P_AT_DISTRIBUTION		
	Expected behaviour		
with			
	AT certificate (CERT_IUT_A_AT)		
	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 secured CAM		
	containing headerInfo		
containing inlineP2p			
containing HashedId3 value			
indicating last 3 octets of currently used AT certificate			
- , -	TIME_2 < TIME_1+1 sec)		
ensure that			
when			
the IUT is requested to send a CAM			
,	< TIME_2 < TIME_3 < TIME_1+1 sec)		
then			
the IUT sends a SecuredMessage of type EtsiTs103097Data			
containing signer			
and containing certificate			
referenced by t	he requested digest		

6.2.2.9 Check that IUT sends AA certificate when requested

TP ld	TP_SEC_ITSS_SND_CAM_13_BV		
	Check that IUT sends the secured CAM containing the AA certificate in the		
Summary	requestedCertificate headerInfo field when it received a CAM containing a request for		
	unrecognized certificate that matches with the currently used AA certificate ID of the IUT		
Reference	ETSI TS 103 097 [1], clause 7.1.1		
Reference	IEEE Std 1609.2 [2], clauses 6.3.9, 8.2.4.2.3		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_P2P_AT_DISTRIBUTION		
	Expected behaviour		
with			
	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 a secured CAM		
containing signer			
containing certificate			
_	at TIME_1		
	and the IUT having received a secured CAM		
containing headerInfo			
	containing inlineP2pcdRequest		
containing HashedId3 value			
indicating last 3 octets of the digest of CERT_IUT_A_AA			
at TIME_2 (TIME_1 < TIME_2 < TIME_1+1 sec)			
ensure that			
when			
the IUT is requested to send a secured CAM			
at TIME_3 (TIME_1 < TIME_2 < TIME_3 < TIME_1+1 sec)			
then	adManaga of tupa EtaiTa102007Data		
the IUT sends a SecuredMessage of type EtsiTs103097Data			
containing headerInfo			
containing requestedCertificate indicating requested AA certificate CERT_IUT_A_AA			
indicating request	eu aa ceriiicale Cent_IUT_a_aa		

	1		
TP ld	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, 8.2.4.2.3		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_P2P_AA_DISTRIBUTION		
	Expected behaviour		
with			
	ith AT certificate (CERT_IUT_A_AT)		
	ed to send more than one CAM per second		
	ed to know the AA certificate (CERT_TS_B_AA)		
and the IUT has alread	y sent secured CAM		
containing signer			
containing certif	ricate		
at TIME_1			
and the IUT having rec			
containing headerInf			
containing inlineP2pcdRequest			
containing HashedId3 value			
indicating last 3 octets of the digest of CERT_TS_B_AA			
	ot 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			
at TIME_3 (TIME_1 < TIME_2 < TIME_3 < TIME_1+1 sec)			
then			
	uredMessage of type EtsiTs103097Data		
	containing headerInfo		
containing requestedCertificate			
indicating red	uested AA certificate (CERT_TS_B_AA)		

TP Id	TP_SEC_ITSS_SND_CAM_15_BV		
11.15	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		
Cummary	from another ITS-S		
	ETSI TS 103 097 [1], clause 7.1.1		
Reference	IEEE Std 1609.2 [2], clauses 6.3.9, 8.2.4.2.3		
PICS Selection	PICS_GN_SECURITY, PICS_SEC_P2P_AA_DISTRIBUTION		
	Expected behaviour		
with	•		
	th AT certificate (CERT_IUT_A_AT)		
issued by the AA cert	ificate (CERT_IUT_A_AA)		
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 rece	sived a secured CAM		
containing headerInfo	containing headerInfo		
containing inlineP2pcdRequest			
	containing HashedId3 value		
	3 octets of the digest of CERT_IUT_A_AA		
	: TIME_2 < TIME_1+0,8 sec)		
and the IUT having rece			
containing headerInfo			
containing request			
	sted AA certificate (CERT_IUT_A_AA)		
	IME_3 < TIME_2+0,1 sec)		
ensure that			
when			
the IUT is requested to send a secured CAM			
`	3 < TIME_4 < TIME_1+0,9 sec)		
then			
	redMessage of type EtsiTs103097Data		
containing headerl			
does not contain	requestedCertificate		

TP ld	TP_SEC_ITSS_SND_CAM_16_BV	
Summary	Check that the IUT does not send a secured CAM containing the AA certificate in the	
	requestedCertificate headerInfo field when it contains certificate in the signer field	
Reference	ETSI TS 103 097 [1], clause 7.1.1	
Reference	IEEE Std 1609.2 [2], clauses 6.3.9, 8.2.4.2.3	
PICS Selection	PICS_GN_SECURITY, PICS_SEC_P2P_AA_DISTRIBUTION	
	Expected behaviour	
with		
	n 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 a secured CAM	
containing signer		
containing certificate	containing certificate	
at TIME_1		
and the IUT having received a SecuredMessage		
containing headerInfo		
containing inlineP2p	containing inlineP2pcdRequest	
9	containing Hashedld3 value	
indicating last 3 octets of the digest of CERT_IUT_A_AA		
at TIME_2 (TIME2 = TIME_1+0,9 sec)		
ensure that		
when		
the IUT is requested to send a secured CAM		
at TIME_3 (TIME_2 < TIME_3 < TIME_1+1 sec)		
then		
the IUT sends a SecuredMessage of type EtsiTs103097Data		
containing signer		
containing certific		
and containing headerInfo		
does not contain requestedCertificate		

TP ld	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	
Deference	ETSI TS 103 097 [1], clause 7.1.1	
Reference		
PICS Selection	PICS_GN_SECURITY, PICS_SEC_P2P_AA_DISTRIBUTION	
	Expected behaviour	
with	•	
the IUT is authorized with	AT certificate (CERT_IUT_A_AT)	
issued by the AA certifi	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 receive	ved a SecuredMessage of type EtsiTs103097Data	
containing headerInfo		
containing inlineP2p	cdRequest	
containing Hashed	dld3 value	
indicating last 3 octets of the digest of CERT_IUT_A_AA		
at TIME_2 (TIME_1+0,9 sec < TIME2 < TIME_1+1 sec)		
ensure that		
when		
the IUT is sending a fire	st subsequent secured CAM	
containing signer		
containing digest		
then		
this message		
containing headerInf	io Company of the com	
	containing requestedCertificate	
indicating reque	ested AA certificate CERT_IUT_A_AA	

6.2.2.10 Check generation time

TP ld	TP_SEC_ITSS_SND_CAM_18_BV	
	Check that IUT sends the secured CAM containing generation time and this time is inside	
Summary	the validity period of the signing certificate	
	Check that message generation time value is realistic	
Reference	ETSI TS 103 097 [1], clause 7.1.1	
Kelerence	IEEE Std 1609.2 [2], clauses 5.2.3.2.2, 5.2.4.2.2, 5.2.4.2.3	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT is authorized wi	th AT certificate (CERT_IUT_A_AT)	
ensure that		
when		
the IUT is requested to send CAM		
containing certificate		
then		
the IUT sends a SecuredMessage of type EtsiTs103097Data		
containing headerInfo		
containing generationTime		
indicating GEN_TIME (CUR_TIME - 5 min <= GEN_TIME <= CUR_TIME + 5 min)		
and containing signer		
containing certificate		
containing toBeSigned		
containing validityPeriod		
containing start		
	ting value X_START_VALIDITY (X_START_VALIDITY <= GEN_TIME)	
	taining duration	
indica	ting value > GEN_TIME - X_START_VALIDITY	

6.2.2.11 Check payload

Summary Check that IUT sends the secured CAM containing the 'data' field in signed data payload, containing the EtsiTs103097Data of type unsecured, contained the CAM payload Reference ETSI TS 103 097 [1], clauses 5.2, 7.1.1 PICS Selection PICS_GN_SECURITY Expected behaviour with the IUT is authorized with AT certificate (CERT_IUT_A_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data contains content contains signedData		
Reference ETSLTS 103 097 [1], clauses 5.2, 7.1.1 PICS Selection PICS_GN_SECURITY Expected behaviour with the IUT is authorized with AT certificate (CERT_IUT_A_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data contains content contains signedData	TP ld	TP_SEC_ITSS_SND_CAM_19_BV
Reference ETSI TS 103 097 [1], clauses 5.2, 7.1.1 PICS Selection PICS_GN_SECURITY Expected behaviour with the IUT is authorized with AT certificate (CERT_IUT_A_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data contains content contains signedData		Check that IUT sends the secured CAM containing the 'data' field in signed data payload,
PICS Selection PICS_GN_SECURITY Expected behaviour with the IUT is authorized with AT certificate (CERT_IUT_A_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data contains content contains signedData		containing the EtsiTs103097Data of type unsecured, contained the CAM payload
Expected behaviour with the IUT is authorized with AT certificate (CERT_IUT_A_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data contains content contains signedData	Reference	ETSI TS 103 097 [1], clauses 5.2, 7.1.1
with the IUT is authorized with AT certificate (CERT_IUT_A_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data contains content contains signedData	PICS Selection	PICS_GN_SECURITY
the IUT is authorized with AT certificate (CERT_IUT_A_AT) ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data contains content contains signedData		Expected behaviour
ensure that when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data contains content contains signedData	with	
when the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data contains content contains signedData	the IUT is authorized with	AT certificate (CERT_IUT_A_AT)
the IUT is requested to send a secured CAM then the IUT sends a message of type EtsiTs103097Data contains content contains signedData	ensure that	
then the IUT sends a message of type EtsiTs103097Data contains content contains signedData	when	
the IUT sends a message of type EtsiTs103097Data contains content contains signedData	the IUT is requested to send a secured CAM	
contains content contains signedData	then	
contains signedData	the IUT sends a messa	ge of type EtsiTs103097Data
	contains content	
	contains signedData	
containing tbsData		
containing payload		
containing data		
containing content		
containing unsecuredData	conta	
containing 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 requested to send a secured CAM	
then	
the IUT sends a message of type EtsiTs103097Data	
containing signer	
containing certificate	
containing appPermissions	
containing an item of type PsidSsp	
containing psid = AID_CAM	

6.2.2.13 Check signature

TP ld	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, 6.3.31	
PICS Selection	PICS_GN_SECURITY AND X_PICS	
	Expected behaviour	
with		
the IUT is authorized witl	n AT certificate (X_CERTIFICATE)	
containing verifyKeyIn	dicator	
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		
containing signer		
containing digest		
referencing the certificate X_CERTIFICATE		
or containing certificate		
indicating X_CERTIFICATE		
and containing signature		
containing X_SIGNATURE verifiable using KEY		
verillable us	Permutation table	
	reilliutation 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_P256 R1
С	CERT_IUT_A_B3_AT	ecdsaBrainpoolP384r1	ecdsaBrainpoolP384r1Signature	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384 R1

TP ld	TP_SEC_ITSS_SND_CAM_22_BV	
Summary	Check that IUT sends the secured CAM containing signature containing the ECC point of	
	type set to either compressed_lsb_y_0, compressed_lsb_y_1 or x_coordinate_only	
Deference	ETSI TS 103 097 [1], clauses 5.2, 7.1.1	
Reference	IEEE Std 1609.2 [2], clauses 6.3.30, 6.3.31	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT is authorized witl	h 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 mess	age of type EtsiTs103097Data	
containing signedData		
containing signature		
containing one of the ecdsaNistP256Signature		
or containing ecdsaBrainpoolP256r1Signature		
or containing ecdsaBrainpoolP384r1Signature		
containing rSig		
containing x-only		
	ing compressed-y-0	
or containing compressed-y-1		

6.2.2.14 Check certificate consistency conditions

TP Id	TP_SEC_ITSS_SND_CAM_23_BV	
Summary	Check that IUT does not send secured CAMs if IUT is authorized with AT certificate does	
	not allow sending messages in this location	
Reference	IEEE Std 1609.2 [2], clause 5.2.3.2.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT is authorized with	the IUT is authorized with AT certificate (CERT_IUT_C1_AT)	
containing region	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 authori	ized with the AT certificate (CERT_IUT_CA3_AT)	
not containing region	\cdot	
and issued by the AA	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
Summary	Check that IUT does not send secured CAMs if all AT certificates installed on the IUT was
	expired
Reference	IEEE Std 1609.2 [2], clause 5.2.3.2.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
containing validity indicating start and the IUT has no ensure that	d with AT certificate (CERT_IUT_A1_AT) Period + duration < CURRENT_TIME other installed AT certificates
when the IUT is requested to send a secured CAM then the IUT does not send CAM	

TP Id	TP_SEC_ITSS_SND_CAM_26_BV	
Summary	Check that IUT does not send secured CAMs if all AT certificates installed on the IUT have	
	the starting time in the future	
Reference	IEEE Std 1609.2 [2], clause 5.2.3.2.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
	the IUT is authorized with AT certificate (CERT_IUT_A2_AT)	
	containing validityPeriod	
3	indicating start > CURRENT_TIME	
and the IUT has no other installed AT certificates		
ensure that		
when		
the IUT is requested to send a secured CAM		
then		
the IUT does not send CAM		

TP ld	TP_SEC_ITSS_SND_CAM_27_BV	
Summary	Check that IUT does not send secured CAMs if IUT does not possess an AT certificate	
	allowing sending CAM by its appPermissions	
Reference	IEEE Std 1609.2 [2], clause 5.2.3.2.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT is authorized with AT certificate (CERT_IUT_A3_AT)		
containing appPermiss	ions	
not containing PsidS	not containing PsidSSP	
containing psid		
indicating AID_CAM		
and the IUT has no other installed AT certificates		
ensure that		
when		
the IUT is requested to send a secured CAM		
then		
the IUT does not send CAM		

6.2.3 DENM profile

6.2.3.1 Check secured DENM is signed

TP Id	TP SEC ITSS SND DENM 01 BV		
	Check that IUT sends the secured DENM using SignedData container		
Summary	Check that for sends the secured DENNI using SignedData container		
Reference	ETSI TS 103 097 [1], clause 7.1.2		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with	•		
the IUT is authorize	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	containing signedData		

6.2.3.2 Check secured DENM AID value

TP Id	TP_SEC_ITSS_SND_DENM_02_BV	
Summary	Check that IUT sends the secured DENM containing the HeaderInfo field psid set to	
	'AID_DENM'	
Reference	ETSI TS 103 097 [1], clause 7.1.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT is authorized with	AT certificate (CERT_IUT_A_AT)	
ensure that		
when		
the IUT is requested to	the IUT is requested to send a secured DENM	
then	then	
the IUT sends a EtsiTs103097Data		
containing content		
containing signedData		
containing tbsData		
containing headerInfo		
containing psid		
indicating 'AID_DENM'		

6.2.3.3 Check header fields

	Check that IUT sends the secured DENM with the HeaderInfo containing generationTime
	and proporation location and door not contain avairations are mutical (a).
ummary	and generationLocation and does not contain expiryTime, encryptionKey,
·	p2pcdLearningRequest, missingCrlIdentifier, inlineP2pcdRequest, requestedCertificate
eference	ETSI TS 103 097 [1], clauses 5.2, 7.1.2
ICS Selection	PICS_GN_SECURITY
	Expected behaviour
ith	
the IUT is authorized with	AT certificate (CERT_IUT_A_AT)
nsure 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 encryptionicey and not containing p2pcdLearningRequest	
and not containing perculearning Request and not containing missing Crildentifier	
and not containing missingormentine	
	ntaining 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	
Reference	ETSI TS 103 097 [1], clause 7.1.2	
	IEEE Std 1609.2 [2], clause 6.3.4	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT is authorized with	AT certificate (CERT_IUT_A_AT)	
ensure that		
when		
the IUT is requested to send a secured DENM		
then		
	the IUT sends a EtsiTs103097Data	
	containing content	
containing signedData		
containing signer		
containing certificate		
containing toBeSigned		
containing appPermissions		
containing the item of type PsidSsp		
containing psid		
indicating AID_DENM		

6.2.3.5 Check generation time

TP Id	TP_SEC_ITSS_SND_DENM_05_BV		
	Check that IUT sends the secured DENM containing generation time and this time is inside		
Summary	the validity period of the signing certificate		
-	Check that message generation time value is realistic		
Reference	ETSI TS 103 097 [1], clause 7.1.2		
Kelerence	IEEE Std 1609.2 [2], clauses 5.2.3.2.2, 5.2.4.2.2, 5.2.4.2.3		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
	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 to Be Signed			
containing to be signed containing to be signed			
containing start			
indicating value X_START_VALIDITY (X_START_VALIDITY <= GEN_TIME)			
and containing duration			
	indicating value > GEN_TIME - X_START_VALIDITY		

6.2.3.6 Check generation location

	T		
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		
Defenses	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 authori	ized with the AT certificate (CERT_IUT_A_AT)		
containing toBeSigned			
not containing regio	n		
and issued by the cert	and issued by the certificate AA (CERT_IUT_A_AA)		
containing toBeSigned			
not containing region			
and issued by the c	and issued by the certificate RCA (CERT_IUT_A_RCA)		
containing toBeSigned			
not containing region			
ensure that			
when			
the IUT is requested to send a secured DENM			
then			
the IUT sends a message of type EtsiTs103097Data			
containing headerIn	containing headerInfo		
•	containing generationLocation		

TP Id	TP_SEC_ITSS_SND_DENM_07_BV_XX	
	Check that IUT sends the secured DENM containing generation location which is inside the circular region defined by the validity restriction of the certificate pointed by the	
	message signer	
Reference	ETSI TS 103 097 [1], clause 7.1.2	
	IEEE Std 1609.2 [2], clause 5.2.3.2.2	
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_CERTIFICATE_SELECTION AND X_PICS	

Expected behaviour

with

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

containing toBeSigned containing region containing X_FIELD indicating REGION

ensure that

when

the IUT is requested to send a secured DENM

then

the IUT sends a message of type EtsiTs103097Data

containing headerInfo

containing generationLocation

indicating value inside the REGION

Permutation Table			
_ XX	X_FIELD	X_AT_CERTIFICATE	X_PICS
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_08_BV	
Summary	Check that IUT sends the secured DENM containing generation location which is inside the region defined by the validity restriction of the certificate pointed by the message signer	
Reference	ETSI TS 103 097 [1], clause 7.1.2 IEEE Std 1609.2 [2], clause 5.2.3.2.2	
PICS Selection	PICS_GN_SECURITY AND NOT PICS_SEC_CERTIFICATE_SELECTION	
Expected behaviour		
with		

the IUT has been authorized with some AT certificate containing toBeSigned

containing region

ensure that

when

the IUT is requested to send a secured DENM

the IUT sends a message of type EtsiTs103097Data

containing headerInfo

containing generationLocation

indicating value inside the REGION

TP ld	TP_SEC_ITSS_SND_DENM_09_BV		
	Check that IUT sends the secured DENM containing generation location which is inside		
Summary	the identified region defined by the validity restriction of the AA certificate used to sign the		
	certificate pointed by the message signer does not contain any region restriction		
Reference	ETSI TS 103 097 [1], clause 7.1.2		
Reference	IEEE Std 1609.2 [2], clauses 5.2.3.2.2, 6.4.8		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_CERTIFICATE_SELECTION		
	Expected behaviour		
with	•		
the IUT has been author	ized with the AT certificate (CERT_IUT_CA1_AT)		
containing toBeSigned	d · · · · · · · · · · · · · · · · · · ·		
not containing region	on		
	ificate AA (CERT_IUT_CC_AA)		
containing toBeSigr	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 valu	e inside the REGION		

TP ld	TP_SEC_ITSS_SND_DENM_10_BV	
	Check that IUT sends the secured DENM containing generation location which is inside	
Summary	the identified region defined by the validity restriction of the root certificate when	
-	subordinate AA and AT certificates do not contain any region restriction	
Reference	ETSI TS 103 097 [1], clause 7.1.2	
Reference	IEEE Std 1609.2 [2], clauses 5.2.3.2.2, 6.4.8	
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_CERTIFICATE_SELECTION	
	Expected behaviour	
with		
the IUT has been authori	zed with the AT certificate (CERT_IUT_CA2_AT)	
containing toBeSigned		
not containing region		
and issued by the certi	ificate AA (CERT_IUT_CA_AA)	
containing toBeSigned		
not containing region		
and issued by the certificate RCA (CERT_IUT_C_RCA)		
containing toBeSigned		
containing circularRegion		
indicating REGION		
ensure that		
when		
the IUT is requested to send a secured DENM		
then		
the IUT sends a message of type EtsiTs103097Data		
	containing headerInfo	
containing generationLocation		
indicating value	e inside the REGION	

6.2.3.7 Check payload

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

6.2.3.8 Check signing permissions

TP Id	TP_SEC_ITSS_SND_DENM_12_BV
Summary	Check that the IUT sends the secured DENM signed with the certificate containing
	appPermissions allowing to sign DEN messages
Reference	ETSI TS 103 097 [1], clause 7.1.2
Reference	IEEE Std 1609.2 [2], clause 5.2.3.2.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	·
the IUT has been a	uthorized with the AT certificate (CERT_IUT_A_AT)
ensure that	·
when	
the IUT is reques	sted to send a secured DENM
then	
the IUT sends a	message of type EtsiTs103097Data
containing signer	
containing of	ertificate
containin	g appPermissions
contair	ing an item of type PsidSsp
cont	aining psid = AID_DENM

6.2.3.9 Check signature

	TD 050 1700 01D D5111 40 DV
TP ld	TP_SEC_ITSS_SND_DENM_13_BV
Summary	Check that IUT sends the secured DENM containing signature
	Check that the signature is calculated over the right fields and using right hash algorithm
	by cryptographically verifying the signature
Reference	ETSI TS 103 097 [1], clauses 5.2, 7.1.2
Reference	IEEE Std 1609.2 [2], clauses 5.3.1, 6.3.4, 6.3.29, 6.3.30, 6.3.31
PICS Selection	PICS_GN_SECURITY AND X_PICS
	Expected behaviour
with	
the IUT is authorized	d with AT certificate (<i>X_CERTIFICATE</i>)
containing verifyK	eyIndicator
containing verif	icationKey
containing X	
indicating	
ensure that	
when	
the IUT is request	ted to send a secured DENM
then	
the IUT sends a m	nessage of type EtsiTs103097Data
containing signedData	
containing signer	
containing certificate	
9	ng X_CERTIFICATE
	sining verifyKeyIndicator
	ntaining verificationKey

	and containing signature containing X_SIGNATURE verifiable using 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	ecdsaBrainpoolP256r1Signatur e	PICS_SEC_BRAINPOOL_P25 6R1
С	CERT_IUT_A_B3_A T	ecdsaBrainpoolP384r1	ecdsaBrainpoolP384r1Signatur e	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P38 4R1

6.2.3.10 Check certificate consistency conditions

containing **X_KEY** indicating KEY

TP ld	TP_SEC_ITSS_SND_DENM_14_BV	
Summary	Check that IUT does not send secured DENMs if IUT does not possess an AT certificate	
	allowing sending messages in this location	
Reference	IEEE Std 1609.2 [2], clause 6.2.3.2.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT has been a	the IUT has been authorized with the AT certificate (CERT_IUT_C1_AT)	
containing region	containing region	
	indicating rectangular region	
not contain	not containing current IUT position	
ensure that		
when		
the IUT is requested to send a secured DENM		
then		
the IUT does not send DENM		

TP Id	TP_SEC_ITSS_SND_DENM_15_BV	
	Check that IUT does not send the secured DENM if IUT is configured to use an AT	
Summary	certificate without region validity restriction and generation location is outside of the region	
	of the issuing AA certificate	
Reference	IEEE Std 1609.2 [2], clause 6.2.3.2.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT has been authori:	zed with the AT certificate (CERT_IUT_CA3_AT)	
not containing region		
1	and issued by the AA certificate (CERT_IUT_C3_AA)	
	containing region	
indicating rectangular region		
not containing current IUT position		
ensure that		
when		
the IUT is requested to send a secured DENM		
then		
the IUT does not send DENM		

TP ld	TP_SEC_ITSS_SND_DENM_16_BV	
Summary	Check that IUT does not send secured DENMs if all AT certificates installed on the IUT are	
	expired	
Reference	IEEE Std 1609.2 [2], clause 6.2.3.2.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with	•	
the IUT is authorized v	with AT certificate (CERT_IUT_A1_AT)	
containing validityPe	eriod	
indicating start +	indicating start + duration < CURRENT_TIME	
and the IUT has no other installed AT certificates		
ensure that	ensure that	
when		
the IUT is requested to send a secured DENM		
then		
the IUT does not se	nd DENM	

TP Id	TP_SEC_ITSS_SND_DENM_17_BV	
Summary	Check that IUT does not send secured DENMs if all AT certificates installed on the IUT have the starting time in the future	
Reference	IEEE Std 1609.2 [2], clause 6.2.3.2.2	
PICS Selection	PICS_GN_SECURITY	
Expected behaviour		
containing validityPe indicating start > 0 and IUT has no other cer ensure that when	CURRENT_TIME tificates installed send a secured DENM	

TP Id	TP_SEC_ITSS_SND_DENM_18_BV		
Summary	Check that IUT does not send secured DENMs if IUT does not possess an AT certificate		
	allowing sending DENM by its appPermissions		
Reference	IEEE Std 1609.2 [2], clause 5.2.3.2.2		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT has been a	uthorized with the AT certificate (CERT_IUT_A4_AT)		
containing appPe	ermissions		
not containing	not containing PsidSSP		
containing p	containing psid		
indicating AID DENM			
and IUT has no other certificates installed			
ensure that			
when			
the IUT is reques	ted to send a secured DENM		
then			
the IUT does not	send DENM		

6.2.4 Generic signed message profile

6.2.4.1 Check that secured message is signed

TP Id	TP_SEC_ITSS_SND_GENMSG_01_BV	
Summary	Check that IUT sends the secured message using signedData container	
Reference	ETSI TS 103 097 [1], clause 7.1.3	
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER	
	Expected behaviour	
ensure that when the IUT is requesthen	ed with AT certificate (CERT_IUT_A_AT) sted to send a secured Beacon	
the IUT sends a message of type EtsiTs103097Data containing content containing signedData		

6.2.4.2 Check secured AID value

TP ld	TP_SEC_ITSS_SND_GENMSG_02_BV	
Summary	Check that the sent Secured Message contains HeaderField its_aid that is set to other	
	value then AID_CAM and AID_DENM	
Reference		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER	
	Expected behaviour	
with		
the IUT is authorized	with AT certificate (CERT_IUT_A_AT)	
ensure that		
when		
the IUT is requested to send a secured Beacon		
then		
the IUT sends a message of type EtsiTs103097Data		
containing conte	containing content	
containing signedData		
containing tbsData		
containing headerInfo		
containing psid		
indicating AID_GNMGMT		

6.2.4.3 Check header field

TP ld	TP_SEC_ITSS_SND_GENMSG_03_BV	
Summary	Check that IUT sends the secured GeoNetworking message with the headerInfo	
	containing generationTime	
Reference	ETSI TS 103 097 [1], clauses 5.2, 7.1.3	
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER	
	Expected behaviour	
with		
the IUT is authorized with AT certificate (CERT_IUT_A_AT)		
ensure that		
when		
the IUT is requested to send a secured Beacon		
then		
the IUT sends a messa	age of type EtsiTs103097Data	
containing content		
containing signedData		
containing tbsData		
containing headerInfo		
containing generationTime		
and not containing p2pcdLearningRequest		
and not containing missingCrlldentifier		

6.2.4.4 Check that signer info is a certificate or digest

TP ld	TP_SEC_ITSS_SND_GENMSG_04_BV						
Summary	Check that IUT sends the secured GeoNetworking message containing certificate or digest						
Summary	as a signer						
Reference	ETSI TS 103 097 [1], clauses 5.2, 7.1.3						
Reference	IEEE Std 1609.2 [2], clause 6.3.4						
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER						
Expected behaviour							
with							
the IUT is authorized with	AT certificate (CERT_IUT_A_AT)						
ensure that							
when							
•	send a secured Beacon						
then							
the IUT sends a messa	age of type EtsiTs103097Data						
containing content							
containing signedData							
containing signer							
containing digest							
or containing certificate							
containing toBeSigned							
containing appPermissions							
containing the item of type PsidSsp							
containing psid							
	indicating AID_GNMGMT						

6.2.4.5 Check generation time

TP_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, 7.1.3							
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER						
	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 Beacon							
containing certificate							
then							
	age of type EtsiTs103097Data						
containing headerInfo							
	containing generationTime						
indicating GEN_TIME (CUR_TIME - 10 min <= GEN_TIME <= CUR_TIME + 10 min)							
and containing signer							
containing certificate							
containing toBeSigned							
containing validityPeriod							
containing start indicating value X_START_VALIDITY (X_START_VALIDITY <= GEN_TIME)							
and containing duration							
indicating value > GEN_TIME - X_START_VALIDITY							
indicatii	ING VALID - OLIVETIME - A_OTAKT_VALIDITI						

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							
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 with AT certificate (CERT_IUT_A_AT)							
ensure that							
when							
the IUT is requested to send a secured Beacon							
then							
the IUT sends a message of type EtsiTs103097Data							
contains content							
contains signedData							
containing tbsData							
containing payload							
containing data							
containing content							
containing unsecuredData							
	containing not-empty data						

6.2.4.7 Check signing permissions

TP Id	d TP_SEC_ITSS_SND_GENMSG_07_BV					
Summary	Check that the IUT sends the secured messages signed with the certificate containing					
	appPermissions allowing to sign these messages					
Reference	ETSI TS 103 097 [1], clause 7.1.3					
	IEEE Std 1609.2 [2], clause 5.2.3.2.2					
PICS Selection PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER						
	Expected behaviour					
with						
the IUT has been at	uthorized with the AT certificate (CERT_IUT_A_AT)					
ensure that						
when						
the IUT is reques	ted to send Beacon					
then						
the IUT sends a r	message of type EtsiTs103097Data					
containing sign	ner					
containing c	ertificate					
containing	gappPermissions					
contain	ing an item of type PsidSsp					
conta	aining psid = AID_GNMGMT					

6.2.4.8 Check signature

TP Id	TP_SEC_ITSS_SND_GENMSG_08_BV				
	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 by				
	cryptographically verifying the signature				
Reference	ETSI TS 103 097 [1], clauses 5.2, 7.1.3				
Reference	IEEE Std 1609.2 [2], clauses 5.3.1, 6.3.4, 6.3.29, 6.3.30, 6.3.31				
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_ITS_AID_OTHER AND X_PICS				
	Expected behaviour				
with					
the IUT is authorized with	AT certificate (X_CERTIFICATE)				
containing verifyKeyInd					
containing verification	onKey				
containing X_KE Y					
indicating KEY					
ensure that					
when					
· ·	send a secured Beacon				
then					
	age of type EtsiTs103097Data				
containing signedDa					
containing signer					
containing digest					
referencing the certificate X_CERTIFICATE					
or containing certificate					
indicating X_CERTIFICATE					
and containing signature					
containing X_SIGNATURE					
verifiable using KEY					
Permutation table					

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_P25 6R1			
С	CERT_IUT_A_B3_A T	ecdsaBrainpoolP384r1	ecdsaBrainpoolP384r1Signature	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P38 4R1			

6.2.5 Encrypted messages profile

6.2.5.1 Check encrypted message generation

TP ld	TP_SEC_ITSS_SND_ENC_01_BV			
Summary	Check that the IUT can generate encrypted message			
Reference	Reference ETSI TS 103 097 [1], clause 5.3			
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_ENCRYPTION_SUPPORT			
	Expected behaviour			
ensure that when the IUT is requested to then	n AT certificate (CERT_IUT_A_AT) o send an encrypted message age of type EtsiTs103097Data dData			

6.2.5.2 Check recipient information

TP Id	TP_SEC_ITSS_SND_ENC_02_BV		
Summary	Check that the encrypted message contains at least one RecipientInfo		
Reference	IEEE Std 1609.2 [2], clause 6.3.31		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_ENCRYPTION_SUPPORT		
	Expected behaviour		
with			
the IUT is authorized	with AT certificate (CERT_IUT_A_AT)		
ensure that			
when			
the IUT is requeste	ed to send an encrypted message		
then			
the IUT sends a m	essage of type EtsiTs103097Data		
containing encry	/ptedData		
containing red	containing recipients		
containing	at least one item of type RecipientInfo		

TP Ic	TP Id TP_SEC_ITSS_SND_ENC_03_BV_XX					
		Check that when the certRecipInfo is used to specify the RecipientInfo then the recipientId				
Sum	mary	contains the HashID8 of the receiver's certificate and the encKey contains encrypted				
	symmetric kay that can be used to decrypt cyphertext					
Refe	rence	IEEE Std 1609.2 [2], clauses 5.3.4, 5.3.5, 6.3.31, 6.3.34				
PICS	Selection	PICS_GN_SECURITY ANI	D PICS_SEC_ENCRYPTIC	ON_SUPPORT AND X_PICS		
		Exped	ted behaviour			
with						
		n AT certificate (CERT_IUT_	_A_AT)			
	re that					
	hen					
		send an encrypted messag				
		orized with the certificate X	_REC_CERT			
	containing encryp					
	containing publ	•				
	containing X	_REC_KEY				
the	***		4-			
		age of type EtsiTs103097Da	ıta			
	containing encrypted					
	containing recipie					
	containing an item of type RecipientInfo containing certRecipInfo					
		recipientId				
			Y REC CERT			
	indicating HashID8 of the certificate X_REC_CERT and containing encKey					
	containing enckey					
	containing v					
	indicating sender public key					
	and containing c					
	indicating encoded symmetric key <i>ENC_SYM_KEY</i>					
	and containing t					
	indicating the authentication tag					
	and containing ciphertext					
	which can be d	ecrypted using decrypted E	NC_SYM_KEY			
		Pern	utation table			
XX	X_REC_CERT	X_REC_KEY	X_ENC_KEY	X_PICS		
Α	CERT_TS_A_AA	eciesNistP256	eciesNistP256			
В	CERT_TS_A_AA_B	eciesBrainpoolP256r1	eciesBrainpoolP256r1	PICS_SEC_BRAINPOOL_P256R1		

6.2.5.3 Check encrypted data content

TP Id	TP_SEC_ITSS_SND_ENC_04_BV
Summary	Check that the ciphertext of encrypted message contains encrypted EtsiTs103097Data structure
Reference IEEE Std 1609.2 [2], clause 6.3.31 ETSI TS 103 097 [1], clause 7.1.4	
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_ENCRYPTION_SUPPORT
	Expected behaviour
ensure that when the IUT is requested to then	AT certificate (CERT_IUT_A_AT) send an encrypted message
the IUT sends a message of type EtsiTs103097Data containing encryptedData containing ciphertext containing encrypted data containing COER encoded data containing structure of type EtsiTs103097Data	

6.2.5.4 Check encrypted and signed data

TP Id	TP_SEC_ITSS_SND_ENC_05_BV
Summary	Check that when the IUT sends SignedAndEcrypted message then it sends the EtsiTs103097Data-Encrypted message containing the EtsiTs103097Data-Signed structure as the ToBeSignedDataContent
Reference	IEEE Std 1609.2 [2], clause 6.3.31 ETSI TS 103 097 [1], clause 7.1.5
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_ENCRYPTION_SUPPORT
	Expected behaviour
ensure that when	ed with AT certificate (CERT_IUT_A_AT) sted to send an encrypted and signed message
containing end containing d containin contair cont	,

6.2.6 Profiles for certificates

6.2.6.1 Check that certificate version is 3

TP ld	TP_SEC_ITSS_SND_CERT_01_BV		
Summary	Check that IUT certificate is explicit and has version 3		
Deference	ETSI TS 103 097 [1], clause 6		
Reference	IEEE Std 1609.2 [2], clause 6.4.3		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
ensure that	•		
when			
the AA is issued	the certificate		
then			
this certificate is	of type EtsiTs103097Certificate		
containing vers	sion		
indicating 3			
and containing	ı type		
indicating 'e	xplicit'		
and containing	and containing toBeSigned		
	rerifyKeyIndicator		
containing	g verificationKey		

6.2.6.2 Check basic certificate conformance to ETSI TS 103 097

TP_SEC_ITSS_SND_CERT_03_BV			
Check that IUT certificate is conformed to ETSI TS 103 097 [1], clause 6			
Reference	Reference ETSI TS 103 097 [1], clause 6		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
ensure that			
when			
the AA is issued the ce	ertificate		
then			
	e EtsiTs103097Certificate		
containing toBeSign	ed		
•	containing id		
indicating 'none			
•	or indicating 'name'		
•	and containing cracald		
indicating '000000'H			
and containing crlSeries			
indicating '0'D			
1	g certRequestPermissions		
	g canRequestRollover		
and containing sig	gnature		

6.2.6.3 Check the issuer reference of the certificate

TP I					
Sum	mary	Check that	the certificate issuer of ce	ertificates is referenced using digest	
Summary		Check that	Check that right digest field is used to reference to the certificate		
Refe	erence	IEEE Std 10	609.2 [2], clause 6.4.3		
PICS	S Selection	PICS_GN_	SECURITY AND X_PICS		
			Expected beha	viour	
with					
th	e CA is authorized v	with certificate C	_ISSUER		
ensu	ire that				
W	hen en				
	the CA is issued the	e certificate			
th	en				
	this certificate is of		097Certificate		
	containing issue				
	containing sel				
	or containing 2				
			e hash of the certificate ca	alculated using X_ALGORITHM	
		ed to certificate			
		ning toBeSigned			
		taining verifyKey			
	CC	ntaining verifica			
		containing X_K			
	ı		Permutation to	able	
X	X_DIGEST	X_ALGORIT M	X_KEY	X_PICS	
Α	sha256AndDigest	SHA-256	ecdsaNistP256 or ecdsaBrainpoolP256r1	PICS_SEC_SHA256 AND PICS_SEC_BRAINPOOL_P256R1	
В	sha384AndDigest	SHA-384	ecdsaBrainpoolP384r1	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1	

6.2.6.4 Check rectangular region validity restriction

TP Id TP_SEC_ITSS_SND_CERT_05_BV			
Summary	Check that the rectangular certificate validity region of the subordinate certificate is well		
Summary	formed and inside the validity region of the issuing certificate		
Reference	Reference IEEE Std 1609.2 [2], clauses 6.4.20, 6.4.17, 5.1.2.4		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_RECTANGULAR_REGION		
	Expected behaviour		
with			
the CA is authorized with	AA certificate		
containing toBeSigned			
containing region			
indicating REGIO	N		
ensure that			
when			
the IUT issued the AT certificate			
then			
	type EtsiTs103097Certificate		
containing toBeSign			
containing region			
containing recta			
containing items of type RectangularRegion			
containing northwest indicating a point inside the REGION			
	ining southeast		
	ng a point on the south from northwest		
and inside the REGION			
and moldo the NEOIOI			

TP ld	TP SEC ITSS SND CERT 06 BV		
Summary	Check that the IUT supports at least 8 entries in the rectangular certificate validity region in		
	the AT certificate		
Reference	IEEE Std 1609.2 [2], clause 6.4.17		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_RECTANGULAR_REGION		
	Expected behaviour		
With			
the IUT is authorized w	ith AT certificate (CERT_IUT_C_AT_8)		
containing toBeSign	ed		
containing region			
	containing rectangularRegion		
containing 8 entries			
	containing one entry (<i>ENTRY</i>)		
containi	ng 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		
0.0	containing generationLocation		
indicating po	sition inside the ENTRY		

6.2.6.5 Check polygonal region validity restriction

TP Id	TP_SEC_ITSS_SND_CERT_07_BV		
	Check that the polygonal certificate validity region contains at least three points		
	Check that the polygonal certificate validity region does not contain intersections		
Summary	Check that the polygonal certificate validity region is inside the validity region of the issuing		
	certificate		
Reference	IEEE Std 1609.2 [2], clauses 6.4.21, 6.4.17, 5.1.2.4		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_POLYGONAL_REGION		
	Expected behaviour		
with			
the CA is authorized with	AA certificate		
containing toBeSigned			
containing region			
3	indicating REGION		
ensure that			
when			
the IUT issued the AT certificate			
then			
	this AT certificate is of type EtsiTs103097Certificate		
containing toBeSigned			
containing region			
containing polygonalRegion			
_	containing more than 2 items of type TwoDLocation		
indicating points inside the REGION			
and indicating unintercepting segments			

	TD 050 IT00 0VD 05DT 00 DV		
TP Id	TP_SEC_ITSS_SND_CERT_08_BV		
Summary	Check that the IUT supports at least 8 points in the polygonal certificate validity region in		
Summary	the AT certificate		
Reference	IEEE Std 1609.2 [2], clause 6.4.17		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_POLYGONAL_REGION		
	Expected behaviour		
with			
the IUT is authorized with	n AT certificate (CERT_IUT_D_AT_8)		
containing toBeSigned	1		
containing region			
containing polygo	onalRegion		
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 genera	containing generationLocation		
indicating posit	tion inside the P		

6.2.6.6 Check identified region validity restriction

TP Id	TP_SEC_ITSS_SND_CERT_09_BV	
Summary	Check that the identified certificate validity region contains values that correspond to	
Summary	numeric country codes as defined by United Nations Statistics Division [5]	
Reference IEEE Std 1609.2 [2], clause 6.4.23		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_IDENTIFIED_REGION	
	Expected behaviour	
ensure that		
when		
the IUT issued the cert	tificate	
containing toBeSign	ed	
containing region		
containing iden	containing identifiedRegion	
then		
this certificate is of type	e EtsiTs103097Certificate	
containing toBeSign		
containing region		
containing iden		
containing 1	entry of type IdentifiedRegion	
	containing countryOnly	
indicatir	ng integer representation of the identifier of country or area	
	ing countryAndRegions	
	ing countryOnly	
	ating integer representation of the identifier of country or area	
	ing countryAndSubregions	
	ing country	
l india	ating integral representation of the identifier of accepts or one	

indicating integer representation of the identifier of country or area

TP ld	TP_SEC_ITSS_SND_CERT_10_BV	
Summony	Check that the IUT supports at least 8 points in the polygonal certificate validity region in	
Summary	the AT certificate	
Reference IEEE Std 1609.2 [2], clause 6.4.17		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_IDENTIFIED_REGION	
	Expected behaviour	
with		
the IUT is authorized with	AT certificate (CERT_IUT_E_AT_8)	
containing toBeSigned		
containing region		
containing identifi		
containing 8 entries		
containing one of the items (<i>I</i>)		
containing current IUT position		
ensure that		
when		
the IUT is requested to send a secured DENM		
then		
the IUT sends a message of type EtsiTs103097Data		
containing headerInfo		
	containing generationLocation	
indicating posit	ion inside the I	

	TD 050 TD0 010 050T 11 01		
TP ld	TP_SEC_ITSS_SND_CERT_11_BV		
Summary	Check that the identified region validity restriction of the subordinate certificate is included		
	in the identified region validity restriction of the issuing certificate		
Reference	,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_IDENTIFIED_REGION		
	Expected behaviour		
with			
the CA is authorized with			
containing toBeSigned			
containing region			
containing identifi			
containing coul			
indicating Co			
	ountryAndRegions		
containing co			
	COUNTRY		
and containi	REGIONS		
	ountryAndSubregions		
containing of			
	COUNTRY		
	ing regionAndSubregions		
	REGIONS and SUBREGIONS		
ensure that	TREGIONO UNU GOBILEGIONO		
when			
the IUT issued the cert	tificate		
containing toBeSign			
containing region			
containing iden			
then			
this certificate is of type	e EtsiTs103097Certificate		
containing toBeSign	containing toBeSigned		
containing region			
containing identifiedRegion			
containing countryOnly			
indicating value = COUNTRY			
or containing countryAndRegions			
containing countryOnly			
	indicating value = COUNTRY		
and containing regions			
containing region identifiers contained in REGIONS			
or containing countryAndSubregions			
containing country			
	indicating value = COUNTRY		
	and containing regionAndSubregions		
	containing region identifiers contained in REGIONS		
and cor	ntaining subRegion identifiers contained in SUBREGIONS for every region		

6.2.6.7 Check time validity restriction in the chain

TP_SEC_ITSS_SND_CERT_12_BV		
Summary	Check that the validityPeriod of the subordinate certificate is inside the validityPeriod of the	
Summary	issuing certificate	
Reference IEEE Std 1609.2 [2], clause 5.1.2.4		
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the CA is authorized with	AA certificate	
containing toBeSigned		
containing validityPe	eriod	
containing start		
	TART_VALIDITY_AA	
containing duration		
indicating X_START_DURATION_AA		
	ensure that	
***************************************	when	
the IUT issued the certificate		
then		
7.	this certificate is of type EtsiTs103097Certificate	
	containing toBeSigned	
containing validityPeriod		
containing start		
	indicating X_START_VALIDITY_AT (X_START_VALIDITY_AT >= X_START_VALIDITY_AA)	
containing dura		
Indicating va	lue <= X_START_VALIDITY_AT + X_DURATION_AT - X_START_VALIDITY_AA	

6.2.6.8 Check ECC point type of the certificate signature

TP Id	i l	TP_SEC_ITSS_SND_CERT_13_BV_XX	
Summary		Check that the certificate signature contains ECC point of type set to either	
	compressed_lsb_y_0, compressed_lsb_y_1 or x_coordinate_only		
Refe	Reference IEEE Std 1609.2 [2], clauses 6.3.29, 6.3.30, 6.3.31		
PICS		PICS_GN_SECURITY AND X_PICS	
		Expected behaviour	
ensu	re that	•	
wh	nen		
	the IUT issued the certi	ficate	
the	en		
	this certificate is of type	EtsiTs103097Certificate	
	containing signature		
	and containing sig	nature	
	containing X_S I		
	containing rS		
	containing		
	•	ng compressed-y-0	
		ng compressed-y-1	
		Permutation table	
XX	X_SIGNATURE	X_PICS	
Α	ecdsaNistP256Signatu	re	
В	ecdsaBrainpoolP256r1	Signature PICS_SEC_BRAINPOOL_P256R1	
С	ecdsaBrainpoolP384r1	Signature PICS SEC SHA384 AND PICS SEC BRAINPOOL P384R1	

6.2.6.9 Check ECC point type of the certificate public keys

TP Ic	1	TP_SEC_ITSS_SND_CERT_14_BV	
Summary	4	Check that the certificate verification key contains ECC point of type set to either	
	mary	compressed_lsb_y_0, compressed_lsb_y_1 or uncompressed	
-			
PICS	Selection	PICS_GN_SECURITY AND X_PICS	
		Expected behaviour	
	re that		
	nen <u> </u>		
	the IUT issued the cert	ificate	
the		T. 17	
		e EtsiTs103097Certificate	
	containing toBeSign		
	containing verifyK		
	containing verif		
	containing X		
		uncompressed	
		ng compressed-y-0	
	or containii	ng compressed-y-1	
		Permutation table	
XX	X X_KEY X_PICS		
Α	ecdsaNistP256		
В	ecdsaBrainpoolP256r1	PICS_SEC_BRAINPOOL_P256R1	
С	ecdsaBrainpoolP384r1	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1	

P Id TP_SEC_ITSS_SND_CERT_15_BV			
Summary	Check that the certificate encryption key contains ECC point of type set to either		
	compressed_lsb_y_0, compressed_lsb_y_1 or uncompressed		
eference IEEE Std 1609.2 [2], clause 6.4.38			
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
ensure that			
when			
the IUT issued the cert	ificate		
then			
this certificate is of type	e EtsiTs103097Certificate		
containing toBeSigned			
	containing encryptionKey		
containing publi			
containing X			
containing	uncompressed		
or containing compressed-y-0			
or containing compressed-y-1			
	Permutation table		
XX X_KEY	X_PICS		
A eciesNistP256			
B eciesBrainpoolP256r1	PICS_SEC_BRAINPOOL_P256R1		

6.2.6.10 Verify certificate signatures

TP I	d IT	P_SEC_ITSS_SND_CERT_16_BV		
	Summary Check the certificate signature			
	•	ETSI TS 103 097 [1], clause 6		
PICS		PICS GN SECURITY AND X PICS		
		Expected behaviour		
With				
th	e CA authorized with cert	ficate		
	containing toBeSigned			
	containing verifyKeyIn			
	containing verification			
onoi	containing X_KE ure that	Y		
	ne mai hen			
VV	the IUT issued the certific	cate		
th	en	, die		
	this certificate is of type E	EtsiTs103097Certificate		
	containing issuer			
	referencing the certi			
	containing toBeS			
	containing veri			
		erificationKey		
	containing			
	indicati			
	and containing signatu containing X_SIGN			
	verifiable using K			
	Permutation table			
XX				
Α	ecdsaNistP256	ecdsaNistP256Signature		
В	ecdsaBrainpoolP256r1	ecdsaBrainpoolP256r1Signature	PICS_SEC_BRAINPOOL_P256R1	
С	ecdsaBrainpoolP384r1	ecdsaBrainpoolP384r1Signature	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1	

6.2.6.11 Verify certificate permissions

TP Id	TP_SEC_ITSS_SND_CERT_17_BV	
Summary	Check that all PSID entries of the appPermissions component of the certificate are unique	
Reference	eference IEEE Std 1609.2 [2], clauses 6.4.28, 5.1.2.4	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
ensure that		
when		
the CA issued th	e certificate	
containing toBeSigned		
containing appPermissions		
then		
this certificate is	of type EtsiTs103097Certificate	
containing toBeSigned		
containing appPermissions		
containin	containing items of type PsidSsp	
contair	containing psid	
indic	cating unique values in this sequence	

TP Id	TP_SEC_ITSS_SND_CERT_18_BV	
Summary	Check that IUT supports at least 8 items in the appPermissions component of the	
Summary	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 appPerm		
containing 8 entrie	e s	
indicating the la		
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 content	
containing signedData		
	containing tbsData	
	containing headerInfo	
_	containing psid	
indicatir	ng 'AID_CAM'	

TP ld	TP_SEC_ITSS_SND_CERT_19_BV
Summary	Check that all PSID entries of the certIssuePermissions component of the certificate are
	unique
Reference	IEEE Std 1609.2 [2], clauses 6.4.28, 5.1.2.4
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
ensure that	
when	
the IUT issued th	ne certificate
containing to E	BeSigned
containing of	pertissuePermissions
then	
this certificate is	of type EtsiTs103097Certificate
containing to E	BeSigned
containing of	pertissuePermissions
containin	g items of type PsidGroupPermissions
and co	ontaining subjectPermissions
conf	taining explicit
containing items of type PsidSspRange	
	containing psid
	indicating unique values in this sequence

```
TP Id
                          TP_SEC_ITSS_SND_CERT_20_BV
                          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
  the IUT is authorized with AT certificate (CERT_IUT_A_AT_A8)
    containing appPermissions
       conformed to the certIssuePermissions
    issued by AA certificate (CERT_IUT_A_AA_C8)
       containing toBeSigned
         containing certIssuePermissions
           containing 8 entries
              indicating the last item
                containing psid
                  indicating the 'AID_CAM'
ensure that
  when
    the IUT is requested to send a secured CAM
    the IUT sends a message of type EtsiTs103097Data
       containing content
         containing signedData
           containing tbsData
              containing headerInfo
                containing psid
                  indicating 'AID_CAM'
```

TP ld	TP_SEC_ITSS_SND_CERT_19_BV
Cummani	Check that all PSID entries of the appPermissions component of the certificate are also
Summary	contained in the certIssuePermissions component in the issuing certificate
Reference	IEEE Std 1609.2 [2], clauses 6.4.28, 5.1.2.4
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
ensure that	
when	
the IUT issued the	certificate
containing toBe	Signed
containing ap	pPermissions
then	
this certificate is of	f type EtsiTs103097Certificate
containing issue	
	the certificate
	toBeSigned
	ng certIssuePermissions
	ining items of type PsidGroupPermissions
	ntaining eeType
	ndicating app(0)
	d containing subjectPermissions
(containing explicit
	containing items of type PsidSspRange
	indicating X_PSID_RANGE_LIST
	or containing all
containing toBe	
	pPermissions
•	items of type PsidSsp
containii	
	ined in the X_PSID_RANGE_LIST
as	a psid

TP ld	TP_SEC_ITSS_SND_CERT_20_BV			
Summary	Check that SSP field in each entry of the appPermissions component of the AT certificate			
	is equal to or a subset of the SSP Range in the corresponding issuing entry			
Reference	IEEE Std 1609.2 [2], clauses 6.4.28, 5.1.2.4			
PICS Selection	PICS_GN_SECURITY			
Expected behaviour				
ensure that				
when				
the IUT issued the cert				
containing toBeSigned				
containing appPe	rmissions			
then	Ft 'T 4000070 ('C)			
this certificate is of type EtsiTs103097Certificate				
containing issuer				
referenced to the certificate				
containing toBeSigned				
containing certIssuePermissions containing items of type PsidGroupPermissions				
containing terms of type I studiouply enhissions containing eeType				
indicating app(0)				
and containing subjectPermissions				
containing explicit				
containing items of type PsidSspRange				
containing psid				
indicating X_PSID_AA				
containing sspRange				
indicating X_SSP_AA [X_PSID_AA]				
or containing all				
containing toBeSigned				
containing appPermissions				
containing items of type PsidSsp				
containing psid				
indicating value equal to X_PSID_AA				
containing ssp indicating value permitted by X_SSP_AA [X_PSID_AA]				
indicating value permitted by A_SSF_AA [A_FSID_AA]				

6.2.6.12 AT and AA certificate profiles

TP Id	TP_SEC_ITSS_SND_CERT_AT_01_BV		
Summary	Check that the IUT signs messages with Authorization Ticket certificate		
	Check that AT certificate certificate_id is set to none		
	Check that AT certificate contains appPermission		
	Check that AT certificate does not contain certIssuePermissions		
Reference	ETSI TS 103 097 [1], clause 7.2.1		
PICS Selection	PICS_GN_SECURITY		
Expected behaviour			
with			
the IUT is in 'authorized' state			
the IUT being requested to include certificate in the next CAM			
ensure that			
when			
the IUT is requested to send a secured CAM			
then			
the IUT sends a message of type EtsiTs103097Data			
containing signer			
containing certificate			
containing toBeSigned			
containing id			
indicating 'none'			
and containing appPermissions			
and not containing certIssuePermissions			

Annex A (informative): Bibliography

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

History

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