# ETSI TS 103 096-2 V1.3.1 (2017-03)



Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 2: Test Suite Structure and Test Purposes (TSS & TP) Reference RTS/ITS-00535

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

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

#### **Copyright Notification**

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

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

© European Telecommunications Standards Institute 2017. All rights reserved.

DECT<sup>™</sup>, PLUGTESTS<sup>™</sup>, UMTS<sup>™</sup> and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members. **3GPP**<sup>™</sup> and LTE<sup>™</sup> are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

**GSM**® and the GSM logo are Trade Marks registered and owned by the GSM Association.

# Contents

Intelle	ectual Property Rights	б
Forew	vord	6
Moda	l verbs terminology	6
1	Scope	7
2	References	7
2.1	Normative references	
2.2	Informative references	
2	Definitions and abbreviations	0
3 3.1	Definitions and aboreviations	
3.1 3.2	Abbreviations	
5.2		
4	Test Suite Structure (TSS)	
4.1	Structure for Security tests	9
5	Test Purposes (TP)	9
5.1	Introduction	
5.1.1	TP definition conventions	
5.1.2	TP Identifier naming conventions	9
5.1.3	Rules for the behaviour description	9
5.1.4	Sources of TP definitions	10
5.1.5	Mnemonics for PICS reference	10
5	ITS-S Security	10
5.1	Overview	
5.2	Sending behaviour	
5.2.1	Check the message protocol version	
5.2.2	Check that AT certificate is used to sign communication messages of ITS-S	
5.2.3	Check Signature ECC point type	
5.2.4	CAM profile	
5.2.4.1	Check secured CAM its_aid value	12
5.2.4.2	2 Check header fields	13
5.2.4.3		13
5.2.4.4		
5.2.4.5		
5.2.4.6		
5.2.4.7		
5.2.4.8		
5.2.4.9		
5.2.4.1	- · · · · · · · · · · · · · · · · · · ·	
5.2.4.1 5.2.4.1	1	
5.2.4.1	DENM profile	
5.2.5	1	
5.2.5.2		
5.2.5.3		
5.2.5.4		
5.2.5.5		
5.2.5.6		
5.2.5.7	•	
5.2.5.8	e	
5.2.6	Generic signed message profile	
5.2.6.1		
5.2.6.2		
5.2.6.3		
5.2.6.4	8	
5.2.6.5	5 Check generation location	27

5.2.6.6	Check payload	
5.2.6.7	Check signature	
5.2.7	Profiles for certificates	
5.2.7.1	Check that certificate version is 2	
5.2.7.2	Check the certificate chain consistence	
5.2.7.3	Check rectangular region validity restriction	
5.2.7.4	Check polygonal region validity restriction	
5.2.7.5	Check identified region validity restriction	
5.2.7.6	Check region validity restrictions in the chain	
5.2.7.7	Check time validity restriction in the chain	
5.2.7.8	Check ECC point type of the certificate signature	
5.2.7.9	Check ECC point type of the certificate verification key	
5.2.7.10	Verify certificates signatures	
5.2.7.11	Check certificate assurance level in the chain	
5.2.7.12	AA certificate profile	
5.2.7.12.1	Check AA certificate subject type	
5.2.7.12.2	Check AA certificate subject name	
5.2.7.12.3	Check that signer info of AA certificate is a digest	
5.2.7.12.4	Check that AA cert is signed by Root cert	
5.2.7.12.5	Check AA ceretificate subject attributes presence and order	
5.2.7.12.6	Check ITS-AID list of AA certificate	
5.2.7.12.7	Check AA certificate validity restriction presence and order	
5.2.7.12.8	Check the AA certificate time_start_and_end validity restriction	
5.2.7.13	AT certificate profile	
5.2.7.13.1	Check AT certificate subject type	
5.2.7.13.2	Check AT certificate subject name	
5.2.7.13.3	Check that signer info of AT certificate is a digest	
5.2.7.13.4	Check AT ceretificate subject attributes presence and order	
5.2.7.13.5	Check presence of time_start_and_end validity restriction	
5.2.7.13.6	Check ITS-AID-SSP	
5.2.7.13.7	Check that AT certificate is signed by AA cert	
5.2.7.13.8	Check validity restriction presence and order	
	Receiver behaviour	
5.3.1	Overview	
5.3.2	CAM Profile	
5.3.2.1	Check that IUT accepts well-formed Secured CAM	
5.3.2.2	Check the message protocol version	
5.3.2.3	Check header fields	
5.3.2.4	Check signer info	
5.3.2.5	Check generation time	
5.3.2.6	Check its_aid	
5.3.2.7	Check payload	
5.3.2.8	Check presence of trailer field	
5.3.2.9	Check signature	
5.3.2.10	Check signing certificate type	
5.3.2.11	Check certificate validity	
5.3.3	DENM Profile	
5.3.3.1	Check that IUT accepts well-formed Secured DENM	
5.3.3.2 5.3.3.3	Check the message protocol version	
	Check header fields	
5.3.3.4 5.3.3.5	Check signer info	
5.3.3.5 5.3.3.6	Check generation time	
5.3.3.0	Check its_aid	
5.3.3.7	Check generation location Check Payload	
5.3.3.8	Check Payload	
5.3.3.9	-	
5.3.3.10	Check signature Check signing certificate type	
5.3.3.12	Check certificate validity	
5.3.4	Generic Signed Message Profile	
5.3.4.1	Check that IUT accepts well-formed GN Beacon message	
5.3.4.1	Check the message protocol version	
J.J. <b>H.</b> 4	Check the message protocol version	

5.3.4.3	Check header fields	111
5.3.4.4	Check signer info	118
5.3.4.5	Check generation time	
5.3.4.6	Check its_aid	
5.3.4.7	Check generation location	
5.3.4.8	Check Payload	
5.3.4.9	Check presence of trailer field	
5.3.4.10	Check signature	
5.3.4.11	Check signing certificate type	
5.3.4.12	Check certificate validity	
5.3.5	Profiles for certificates	
5.3.5.1	Check that certificate version is 2	
5.3.5.2	Check that enrolment certificate is not used for sign other certificates	
5.3.5.3	Check that authorization ticket certificate is not used for sign other certificates	
5.3.5.4	Check that AA certificate signed with other AA certificate is not accepted	
5.3.5.5	Check the certificate signature	
5.3.5.6	Check circular region of subordinate certificate	
5.3.5.7	Check rectangular region of subordinate certificate	145
5.3.5.8	Check polygonal region of subordinate certificate	151
5.3.5.9	Check identified region of subordinate certificate	158
5.3.5.10	Check time validity restrictions	168
5.3.5.10.1	Check time validity restriction presence	168
5.3.5.10.2	Check AT certificate time validity restriction presence	
5.3.5.11	Check time validity restriction conforming to the issuing certificate	171
5.3.5.12	Check AID-SSP subject attribute presence and value	173
5.3.5.13	Check AID-SSP subject attribute value conforming to the issuing certificate	175
5.3.5.14	Check the authorization ticket certificate signer info	
5.3.5.15	Check the authorization authority certificate signer info	
5.3.5.16	Check the subject_name of the AT certificate	
5.3.5.17	Check certificate assurance level presence and values	
5.3.5.18	Check certificate verification key presence	
5.3.5.19	Check invalid region type in validity restriction of certificates	
Annex A (i	nformative): Bibliography	
History		184

# Intellectual Property Rights

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

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

# Foreword

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

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

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

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

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

# Modal verbs terminology

In the present document "shall", "shall not", "should", "should not", "may", "need not", "will", "will not", "can" and "cannot" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (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 standard for the methodology of conformance testing (ISO/IEC 9646-1 [i.3] and ISO/IEC 9646-2 [i.4]) as well as the ETSI rules for conformance testing (ETSI ETS 300 406 [i.7]) are used as a basis for the test methodology.

#### 2 References

#### 2.1 Normative references

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

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

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

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

- [1] ETSI TS 103 097 (V1.2.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".
- [2] ETSI TS 103 096-1 (V1.3.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)".
- [3] ETSI TS 102 871-1 (V1.3.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 1: Test requirements and Protocol Implementation Conformance Statement (PICS) pro forma".
- [4] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes".
- [5] United Nations, Statistics Division (1996): "Standard Country or Area Codes for Statistical Use (Rev. 3), Series M: Miscellaneous Statistical Papers, No. 49", New York: United Nations.

#### 2.2 Informative references

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

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

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

- [i.1] ETSI EG 202 798 (V1.1.1): "Intelligent Transport Systems (ITS); Testing; Framework for conformance and interoperability testing".
- [i.2] ETSI TS 102 965 (V1.3.1): "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration".
- [i.3] ISO/IEC 9646-1 (1994): "Information technology -- Open Systems Interconnection --Conformance testing methodology and framework -- Part 1: General concepts".

- [i.5]ISO/IEC 9646-6 (1994): "Information technology -- Open Systems Interconnection --<br/>Conformance testing methodology and framework -- Part 6: Protocol profile test specification".
- [i.6] ISO/IEC 9646-7 (1995): "Information technology -- Open Systems Interconnection --Conformance testing methodology and framework -- Part 7: Implementation Conformance Statements".
- [i.7] ETSI ETS 300 406 (1995): "Methods for testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

# 3 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
CAM	Co-operative Awareness Messages
CAN	Controller Area Network
CERT	Certificate
DE	Data Element
DENM	Decentralized Environmental Notification Message
EA	Enrolment Authority
ECC	Elliptic Curve Cryptography
GN	GeoNetworking
ITS	Intelligent Transportation Systems
ITS-S	Intelligent Transport System - Station
IUT	Implementation under Test
MSG	Message
PICS	Protocol Implementation Conformance Statement
SSP	Service Specific Permissions
TP	Test Purposes
TSS	Test Suite Structure

# 4 Test Suite Structure (TSS)

# 4.1 Structure for Security tests

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

#### Table 1: TSS for Security

9

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>_<sgr>_<rn>_<sn>_<x></x></sn></rn></sgr></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
	<rn> = requirement sequential number</rn>		01 to 99
	<sn> = test purpose sequential number</sn>		01 to 99
	<x> = category</x>	BV	Valid Behaviour tests
		BO	Invalid Behaviour Tests

#### 5.1.3 Rules for the behaviour description

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

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

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

#### 5.1.4 Sources of TP definitions

All TPs have been specified according to ETSI TS 103 097 [1].

#### 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' column refers to tables and items of ETSI TS 103 096-1 [2] if not stated otherwise. The 'PICS item' as defined in ETSI TS 103 096-1 [2] and ETSI TS 102 871-1 [3] shall be used to determine the test applicability.

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

	Mnemonic	PICS item
1	PICS_GN_SECURITY	A.2/1 ETSI TS 102 871-1 [3]
2	PICS_CERTIFICATE_SELECTION	A.2/1
3	PICS_USE_CIRCULAR_REGION	A.3/2
4	PICS_USE_RECTANGULAR_REGION	A.3/3
5	PICS_USE_POLYGONAL_REGION	A.3/4
6	PICS_USE_IDENTIFIED_REGION	A.3/5
7	PICS_ITS_AID_OTHER_PROFILE	A.5/1
8	PICS_USE_ISO31661_REGION_DICTIONARY	A.4/1
9	PICS_USE_UN_STATS_REGION_DICTIONARY	A.4/2

# 5 ITS-S Security

#### 5.1 Overview

Void.

#### 5.2 Sending behaviour

#### 5.2.1 Check the message protocol version

TP ld	TP_SEC_ITSS_SND_MSG_01_01_BV	
Summary	Check that ITS-S sends a SecuredMessage containing protocol version set to 2	
Reference	ETSI TS 103 097 [1], clause 5.1	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with the IUT being in the 'auth ensure that when the IUT is requested to then the IUT sends a Secur containing protocol_ indicating value '2	o send a SecuredMessage edMessage version	

# 5.2.2 Check that AT certificate is used to sign communication messages of ITS-S

P_SEC_ITSS_SND_MSG_04_01_BV Check that when IUT sends the message signed with the digest, then this digest points to the AT certificate		
TSI TS 103 097 [1], clause 6.3		
PICS_GN_SECURITY		
Expected behaviour		
rized' state		
o send more than one CAM per second		
st CAM		
['signer_info'].signer.type		
the IUT is requested to send next CAM		
the IUT sends a SecuredMessage		
lds ['signer_info']		
containing signer		
containing type		
indicating certificate_digest_with_sha256		
and containing digest		
referencing the certificate		
containing subject_info.subject_type		
indicating 'authorization_ticket'		

TP_SEC_ITSS_SND_MSG_04_02_BV		
Check that IUT uses the AT certificate to sign messages		
ETSI TS 103 097 [1], clause 6.3		
PICS_GN_SECURITY		
Expected behaviour		
uthorized' state		
ed to include certificate in the next CAM		
the IUT is requested to send a next CAM		
then		
curedMessage		
containing header_fields ['signer_info']		
er		
containing type		
indicating 'certificate'		
and containing certificate		
containing subject_info.subject_type		
indicating 'authorization ticket'		

5.2.3	Check Signature ECC point type
-------	--------------------------------

TP ld	TP_SEC_ITSS_SND_MSG_05_01_BV		
Summary	Check that the SecuredMessage signature contains the ECC point of type set to either		
Summary	compressed_lsb_y_0, compressed_lsb_y_1 or x_coordinate_only		
Reference	ETSI TS 103 097 [1], clause 4.2.9		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT being in the 'au	thorized' state		
ensure that			
when			
the IUT is requested	the IUT is requested to send a CAM		
then			
the IUT sends a Sec	uredMessage		
containing header	_fields ['its_aid']		
containing its_a	containing its_aid		
indicating 'AID_CAM'			
and containing trailer_fields['signature']			
containing signature.ecdsa_signature			
containing R.type			
	indicating 'compressed_lsb_y_0'		
or indicatin	or indicating 'compressed_lsb_y_1'		
or indicatin	or indicating 'x_coordinate_only'		

# 5.2.4 CAM profile

# 5.2.4.1 Check secured CAM its\_aid value

TP ld	TP_SEC_ITSS_SND_CAM_01_01_BV
Summary	Check that the sent Secured CAM contains a HeaderField its_aid that is set to 'AID_CAM'
Reference	ETSI TS 103 097 [1], clauses 5.4 and 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with the IUT being in the 'auth ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing its_aid indicating 'AID_	o send CAM redMessage ields ['its_aid']

TP ld	TP_SEC_ITSS_SND_CAM_02_01_BV	
Summary	Check that the secured CAM contains exactly one element of these header fields: signer_info, generation_time, its_aid; Check that the header fields are in the ascending order according to the numbering of the enumeration except of the signer_info, which is encoded first; Check that generation_time_standard_deviation, expiration, encryption_parameters, recipient_info are not used	
Reference	ETSI TS 103 097 [1], clause 7.1	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'authorized' state		
ensure that		
when		
the IUT is requested to send a CAM		
then		
the IUT sends a Secur	•	
containing header_fields[0]		
containing type		
indicating 'signer_info'		
	and containing header_fields [1N]	
indicating header_fields [n].type < header_fields [n+1].type		
and containing header_fields ['generation_time']		
and containing header_fields['its_aid']		
	and not containing header_fields['generation_time_standard_deviation']	
	and not containing header_fields['expiration']	
and not containing header_fields['encryption_parameters']		
and not containing header_fields['recipient_info']		

#### 5.2.4.2 Check header fields

# 5.2.4.3 Check that IUT sends digest as sender info

TP ld	TP_SEC_ITSS_SND_CAM_05_01_BV		
Summary	Check that the secured CAM contains the signer_info field of certificate when over the time		
Summary	of one second no other SecuredMessage contained a signer_info of type certificate		
Reference	ETSI TS 103 097 [1], clause 7.1		
CS Selection PICS_GN_SECURITY			
	Expected behaviour		
with			
the IUT being in the 'aut	horized' state		
and the IUT is configure	d to send more than one CAM per second		
and the IUT having sent	a CAM		
containing header_fie	lds['signer_info'].signer.type		
indicating 'certificat			
and contains header_	fields['generation_time']		
indicating TIME_LA	NST		
ensure that			
when			
the IUT is sending CA	M		
containing header_	fields['signer_info']		
containing signer	r		
containing typ	e		
indicating 'c	ertificate'		
then			
this message is			
	fields['generation_time']		
indicating TIME (	(TIME >= TIME_LAST + 1sec)		

TP ld	TP_SEC_ITSS_SND_CAM_05_02_BV
Summary	Check that the secured CAM contains the signer_info field of certificate when the timeout of
Summary	one second has been expired after the previous CAM containing the certificate
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT is confi	gured to send more than one CAM per second
and the IUT having	sent a CAM
containing heade	r_fields['signer_info'].signer.type
indicating 'cert	ificate'
at TIME_LAST	
ensure that	
when	
the IUT is sendin	
	der_fields['generation_time']
•	ME >= TIME_LAST + 1sec
then	
this message is	
0	der_fields ['signer_info']
containing s	6
containing	
	ng 'certificate'
and conta	aining certificate

14

#### 5.2.4.4 Check that IUT sends cert to unknown ITS-S

TP ld	TP_SEC_ITSS_SND_CAM_06_01_BV	
Summary	Check that ITS-S sends a Secured CAM containing the signer_info of type certificate when	
-	the ITS-S received a CAM from an unknown ITS-S	
Reference	eference ETSI TS 103 097 [1], clause 7.1	
PICS Selection	CS Selection PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'a	uthorized' state	
	red to send more than one CAM per second	
	eady sent CAM at TIME_1	
	ields['signer_info'].signer.type	
indicating 'certific		
	ceived a SecuredMessage	
	_2 (TIME_1 < TIME_2 < TIME_1+1sec)	
	ler_fields['signer_info']	
containing signer		
containing type		
	ertificate_digest_with_sha256'	
and containing		
	ashedld3 value	
	g an unknown certificate	
ensure that		
when	to cond CAM	
the IUT is requested	TIME 1 < TIME 2 < TIME 3 < TIME 1 + 1sec)	
then	$HME_1 < HME_2 < HME_3 < HME_1 + Isec$	
the IUT sends a Sec	anceseMharus	
and containing he	•	
containing type		
indicating 'si		
and containing		
containing ty		
0,	'certificate'	
	ng certificate	

TP ld	TP_SEC_ITSS_SND_CAM_07_01_TI	
ummary Check that IUT restarts the certificate sending timer when the certificate has been sen		
Reference		
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	e 'authorized' state	
and the IUT is conf	igured to send more than one CAM per second	
and the IUT having	already sent CAM at TIME_1	
containing head	er_fields['signer_info'].signer.type	
indicating 'cer	tificate'	
and the IUT having	received a CAM	
at T	IME_2 (TIME_1 +0.3sec)	
containing head	er_fields['signer_info'].signer.type	
indicating 'cer	tificate_digest_with_ecdsap256'	
and containing h	eader_fields['signer_info'].signer.digest	
referencing ar	n unknown certificate	
and the IUT having	sent CAM at TIME_3 (TIME_3 > TIME_2)	
containing head	er_fields['signer_info'].signer.type	
indicating 'cer	tificate'	
ensure that		
when		
	ng the next CAM at TIME_4	
	ader_fields['signer_info'].signer.type	
indicating 'c	ertificate'	
then		
the difference be	etween TIME_4 and TIME_3 is about 1sec	

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

#### 5.2.4.6 Check that IUT sends certificate when requested

TP Id       TP_SEC_ITSS_SND_CAM_08_01_BV         Summary       Check that the IUT sends the Secured CAM containing the signer_info of type certificate when it received a CAM containing a request of unrecognized certificate that matches were the currently used AT certificate ID of the IUT         Reference       ETSI TS 103 097 [1], clause 7.1         PICS Selection       PICS_GN_SECURITY         Expected behaviour         with       the IUT being in the 'authorized' state         and the IUT is configured to send more than one CAM per second         and the IUT having already sent CAM at TIME_1         containing header_fields['signer_info'].signer.type         indicating 'certificate'       and the IUT having received a SecuredMessage         at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec)         containing header_fields['request_unrecognized_certificate']         containing digests	
Summary       when it received a CAM containing a request of unrecognized certificate that matches were the currently used AT certificate ID of the IUT         Reference       ETSI TS 103 097 [1], clause 7.1         PICS Selection       PICS_GN_SECURITY         Expected behaviour         with       the IUT being in the 'authorized' state         and the IUT is configured to send more than one CAM per second       and the IUT having already sent CAM at TIME_1         containing header_fields['signer_info'].signer.type       indicating 'certificate'         and the IUT having received a SecuredMessage       at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec)	
the currently used AT certificate ID of the IUT         Reference       ETSI TS 103 097 [1], clause 7.1         PICS Selection       PICS_GN_SECURITY         Expected behaviour         with       the IUT being in the 'authorized' state         and the IUT is configured to send more than one CAM per second         and the IUT having already sent CAM at TIME_1         containing header_fields['signer_info'].signer.type         indicating 'certificate'         and the IUT having received a SecuredMessage         at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec)         containing header_fields['request_unrecognized_certificate']         containing digests	
Reference         ETSI TS 103 097 [1], clause 7.1           PICS Selection         PICS_GN_SECURITY           Expected behaviour           with         the IUT being in the 'authorized' state           and the IUT is configured to send more than one CAM per second           and the IUT having already sent CAM at TIME_1           containing header_fields['signer_info'].signer.type           indicating 'certificate'           and the IUT having received a SecuredMessage           at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec)	۱h
PICS Selection         PICS_GN_SECURITY           Expected behaviour           with         the IUT being in the 'authorized' state           and the IUT is configured to send more than one CAM per second           and the IUT having already sent CAM at TIME_1           containing header_fields['signer_info'].signer.type           indicating 'certificate'           and the IUT having received a SecuredMessage           at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec)	
Expected behaviour         with         the IUT being in the 'authorized' state         and the IUT is configured to send more than one CAM per second         and the IUT having already sent CAM at TIME_1         containing header_fields['signer_info'].signer.type         indicating 'certificate'         and the IUT having received a SecuredMessage         at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec)	
with the IUT being in the 'authorized' state and the IUT is configured to send more than one CAM per second and the IUT having already sent CAM at TIME_1 containing header_fields['signer_info'].signer.type indicating 'certificate' and the IUT having received a SecuredMessage at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec) containing header_fields['request_unrecognized_certificate'] containing digests	
the IUT being in the 'authorized' state and the IUT is configured to send more than one CAM per second and the IUT having already sent CAM at TIME_1 containing header_fields['signer_info'].signer.type indicating 'certificate' and the IUT having received a SecuredMessage at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec) containing header_fields['request_unrecognized_certificate'] containing digests	
and the IUT is configured to send more than one CAM per second and the IUT having already sent CAM at TIME_1 containing header_fields['signer_info'].signer.type indicating 'certificate' and the IUT having received a SecuredMessage at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec) containing header_fields['request_unrecognized_certificate'] containing digests	
and the IUT having already sent CAM at TIME_1 containing header_fields['signer_info'].signer.type indicating 'certificate' and the IUT having received a SecuredMessage at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec) containing header_fields['request_unrecognized_certificate'] containing digests	
containing header_fields['signer_info'].signer.type indicating 'certificate' and the IUT having received a SecuredMessage at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec) containing header_fields['request_unrecognized_certificate'] containing digests	
indicating 'certificate' and the IUT having received a SecuredMessage at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec) containing header_fields['request_unrecognized_certificate'] containing digests	
and the IUT having received a SecuredMessage at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec) containing header_fields['request_unrecognized_certificate'] containing digests	
at TIME_2 (TIME_1 < TIME_2 < TIME_1+1sec) containing header_fields['request_unrecognized_certificate'] containing digests	
containing header_fields['request_unrecognized_certificate'] containing digests	
containing digests	
containing HashedId3 value	
referencing to the AT certificate	
and not containing HashedId3 value	
referencing to the AA certificate ensure that	
when	
the IUT is requested to send a CAM	
at TIME_3 (TIME_1 < TIME_2 < TIME_3 < TIME_1+1sec)	
then	
the IUT sends a SecuredMessage	
containing header_fields['signer_info']	
containing signer	
containing type	
indicating 'certificate'	
and containing certificate	
referenced by the requested digest	

TP ld	TR SEC ITSS SND CAM 00 01 RV
	TP_SEC_ITSS_SND_CAM_09_01_BV
Summany	Check that the sent secured CAM contains the signer_info of type certificate_chain when the ITS-S has received a CAM containing a request of unrecognized certificate that matches
Summary	
Deference	with the AA certificate ID that issued its currently used AT certificate ID of the IUT
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	authorized state
the IUT being in the	
	gured to send more than one CAM per second already sent a CAM
	r_fields['signer_info'].signer.type
indicating 'cert	
at TIME_1	licate
_	received a SecuredMessage
	r fields['request_unrecognized_certificate']
containing dige	
	lashedId3 value
	ing to the AA certificate
	1 < TIME_2 < TIME_1+1sec)
ensure that	
when	
the IUT is reques	ted to send a CAM
at TIME_3 (TIM	ME_1 < TIME_2 < TIME_3 < TIME_1+1sec)
then	
the IUT sends a S	SecuredMessage
and containing	header_fields['signer_info']
containing s	igner
containing	
	ng 'certificate_chain'
	aining certificates[last]
	ng the AT certificate
	aining certificates[last-1]
indicati	ng the AA certificate

16

# 5.2.4.7 Check that IUT send certificate\_chain when requested

TP ld	TP_SEC_ITSS_SND_CAM_10_01_BV	
	Check that Secured CAM generation time is inside the validity period of the signing	
Summary	certificate;	
	Check that message generation time value is realistic	
Reference	ETSI TS 103 097 [1], clauses 5.4 and 7.1	
PICS Selection	CS Selection PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'au		
	d to include certificate in the next CAM	
ensure that		
when	to sound OAM	
the IUT is requested	to send CAM	
then	urad Maaaaga	
the IUT sends a Sec	fields ['generation_time']	
containing gene		
	EN_TIME (CUR_TIME - 5min <= GEN_TIME <= CUR_TIME + 5min)	
	ader_fields ['signer_info']	
containing sign		
containing ty		
indicating		
and containir		
containing	validity_restrictions['time_end']	
containi	ng end_validity	
indica	ating value > GEN_TIME	
	ng validity_restrictions['time_start_and_end']	
	ng start_validity	
	ating value <= GEN_TIME	
	taining end_validity	
	ating value > GEN_TIME	
	ing validity_restrictions['time_start_and_duration']	
	ng start_validity (X_START_VALIDITY)	
	ating value <= GEN_TIME taining duration	
	ating value > GEN_TIME - X_START_VALIDITY	

17

# 5.2.4.8 Check generation time

5.2.4.9	Check sending certificate request to unknown station

TP ld	TP_SEC_ITSS_SND_CAM_12_01_BV	
_	Check that the IUT sends certificate request when it receives a message from unknown	
Summary	station	
Reference	ETSI TS 103 097 [1], clause 7.1	
CS Selection PICS_GN_SECURITY		
	Expected behaviour	
with		
the IUT being in the	e 'authorized' state	
and the IUT has rec	ceiving a SecuredMessage	
containing header_fields['signer_info'].signer		
containing type		
	ertificate_digest_with_sha256'	
and containing		
	ashedId3 value DIGEST_A	
	ng an unknown certificate	
ensure that		
when		
	sted to send CAM	
then		
	SecuredMessage	
	ider_fields['request_unrecognized_certificate']	
containing d		
	g Hashedld3 value	
indicati	ing DIGEST_A	

# 5.2.4.10 Check Payload

TP ld	TO SEC ITSS SND CAM 14 01 DV		
Summary	ummary Check that the Secured CAM contains non-empty payload of type signed		
Reference	eference ETSI TS 103 097 [1], clause 7.1		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT being in the 'auth	orized' state		
ensure that			
when			
the IUT is requested to send a CAM			
then			
the IUT sends a SecuredMessage			
and containing payload_field			
containing type			
indicating 'signed'			
and containing not-empty data			

# 5.2.4.11 Check presence of trailer field

Void.

TP ld	TP_SEC_ITSS_SND_CAM_16_01_BV
	Check that the secured CAM contains only one TrailerField of type signature;
Summary	Check that the signature contained in the SecuredMessage is calculated over the right fields
Caminary	by cryptographically verifying the signature
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
ensure that	
when	
the IUT is reques	ted to send a CAM
then	
the IUT sends a S	SecuredMessage
containing hea	der_fields ['signer_info']
containing s	igner
containing	g type
	ng 'certificate_digest_with_ecdsap256'
	ining digest
	cing the certificate
	aining subject_info.subject_type
	dicating 'authorization_ticket'
	containing subject_attributes['verification key'] (KEY)
or containing	
containing	
	ng 'certificate'
	ining certificate
	ing subject_info.subject_type
	ating 'authorization_ticket' (2)
	ntaining subject_attributes['verification key'] (KEY)
containing trailer_fields containing single instance of type TrailerField	
containing s	
	ng 'signature'
	ining signature
	le using KEY
verman	

#### 5.2.4.12 Check signature

# 5.2.5 DENM profile

# 5.2.5.1 Check secured DENM its\_aid value

TP ld	TP_SEC_ITSS_SND_DENM_01_01_BV
C	Check that the sent Secured DENM contains a HeaderField its_aid that is set to
Summary	'AID_DENM'
Reference	ETSI TS 103 097 [1], clauses 5.4 and 7.2
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 DENM
then	
the IUT sends a	SecuredMessage
containing header_fields ['its_aid']	
containing its_aid	
indicating 'AID_DENM'	

TP ld	TP_SEC_ITSS_SND_DENM_02_01_BV	
Summary	Check that the secured DENM contains exactly one element of these header fields: signer_info, generation_time, generation_location, message_type; Check that the header fields are in the ascending order according to the numbering of the enumeration except of the signer_info, which is encoded first; Check that generation_time_with_confidence (generation_time_standard_deviation) is not used	
Reference	ETSI TS 103 097 [1], clause 7.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'au	uthorized' state	
ensure that		
when		
the IUT is requested	to send DENM	
then		
the IUT sends a Sec	zuredMessage	
	containing header_fields[0]	
containing type		
	indicating 'signer_info'	
and containing header_fields [n].type		
indicating value less than header_fields [n+1].type		
and containing header_fields ['generation_time']		
•	ader_fields ['generation_location']	
and containing header_fields ['its_aid']		
and not containing header_fields ['generation_time_with_confidence']		

#### 5.2.5.2 Check header fields

#### 5.2.5.3 Check that signer info is a certificate

TP ld	TP_SEC_ITSS_SND_DENM_03_01_BV	
Summary	Check that secured DENM contains the certificate as a signer_info	
Reference	ETSI TS 103 097 [1], clause 7.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with	- · ·	
the IUT being in the	authorized' state	
ensure that		
when		
the IUT is reques	sted to send a DENM	
then		
the IUT sends a	SecuredMessage	
containing hea	ider_fields['signer_info']	
containing s	igner	
containing type		
indicati	indicating 'certificate'	
and containing certificate		

TP ld	TP_SEC_ITSS_SND_DENM_04_01_BV
	Check that Secured DENM generation time is inside the validity period of the signing
Summary	certificate;
-	Check that generation time value is realistic
Reference	ETSI TS 103 097 [1], clauses 5.4 and 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'au	uthorized' state
ensure that	
when	
the IUT is requested	to send a DENM
then	
the IUT sends a Sec	
• •	one header_fields['generation_time']
containing gene	
	EN_TIME (CUR_TIME - 10min <= GEN_TIME < CUR_TIME + 10min)
	r_fields['signer_info']
containing sign containing ty	
	certificate'
containing ce	
	validity_restrictions['time_end']
	itaining end_validity
	ating value > GEN_TIME
	ing validity_restrictions['time_start_and_end']
	ing start_validity
	ating value <= GEN_TIME
and cor	ntaining end_validity
	ating value > GEN_TIME
	ing validity_restrictions['time_start_and_duration']
containi	ing start_validity (X_START_VALIDITY)
	ating value <= GEN_TIME
	taining duration
indica	ating value > GEN_TIME - X_START_VALIDITY

# 5.2.5.4 Check generation time

# 5.2.5.5 Check generation location

TP ld	TP_SEC_ITSS_SND_DENM_05_01_BV
Cummer of the	Check that the secured DENM contains exactly one HeaderField generation_location when
Summary	AT certificate does not contain any region restrictions
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION
	Expected behaviour
with	
the IUT has been authori	zed with the AT certificate (CERT_IUT_A_AT)
not containing validity_	_restrictions['region']
ensure that	
when	
the IUT is requested to send DENM	
then	
the IUT sends a SecuredMessage	
containing exactly one header_field ['generation_location']	
containing generation_location	

21

TP ld	TP_SEC_ITSS_SND_DENM_05_02_BV
	Check that the secured DENM contains exactly one HeaderField generation_location whic
Summary	is inside the circular region defined by the validity restriction of the certificate pointed by the
	signer_info field
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND
	PICS_USE_CIRCULAR_REGION
	Expected behaviour
with	
	uthorized with the AT certificate (CERT_IUT_B_AT)
containing validit	y_restrictions ['region']
containing reg	
containing r	
indicating	
	sircular_region
	REGION
ensure that	
when	
	sted to send a DENM
then	
	SecuredMessage
	ctly one header_field ['generation_location']
containing c	generation_location
	value inside the REGION

TP ld	TP_SEC_ITSS_SND_DENM_05_03_BV
Summary	Check that the secured DENM contains exactly one HeaderField generation_location which is inside the rectangular region defined by the validity restriction of the certificate pointed by the signer_info field
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND PICS_USE_RECTANGULAR_REGION
	Expected behaviour
with	
containing validity_rest containing region containing region_ indicating 'recta containing rectan containing insta indicating RE	_type angle' gular_region ance of RectangularRegion
ensure that	
when the IUT is requested to then	send DENM
the IUT sends a Secur	edMessage ne header_field ['generation_location']
containing genera	

TP ld	TP_SEC_ITSS_SND_DENM_05_04_BV
-	Check that the secured DENM contains exactly one HeaderField generation_location which
Summary	is inside the polygonal region defined by the validity restriction of the certificate pointed by
	the signer_info field
Reference	ETSI TS 103 097 [1], clause 7.2
DICC Calastian	PICS GN SECURITY AND PICS CERTIFICATE SELECTION AND
PICS Selection	PICS_USE_POLYGONAL_REGION
	Expected behaviour
with	·
the IUT has been autho	rized with the AT certificate (CERT_IUT_D_AT)
containing validity_re	strictions ['region']
containing region	
containing region_type	
indicating 'polygon'	
containing polyc	
indicating REGION	
ensure that	
when	
the IUT is requested	to send a DENM
then	
the IUT sends a Secu	uredMessage
	one header_field ['generation_location']
containing gene	
indicating value inside the REGION	

TP ld	TP_SEC_ITSS_SND_DENM_05_05_BV
	Check that the secured DENM contains exactly one HeaderField generation_location which
Summary	is inside the identified region defined by the validity restriction of the certificate pointed by
	the signer_info field
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND
	PICS_USE_IDENTIFIED_REGION
	Expected behaviour
with	
the IUT has been aut	norized with the AT certificate (CERT_IUT_E_AT)
containing validity_	restrictions ['region']
containing region	
containing reg	
indicating 'i	d_region'
containing ide	ntified_region
indicating F	EGION
ensure that	
when	
the IUT is requeste	d to send a DENM
then	
the IUT sends a Se	0
containing head	
	actly one instance of HeaderField
containing t	
	g 'generation_location'
	generation_location
indicating	y value inside the REGION

TP ld	TP_SEC_ITSS_SND_DENM_05_06_BV	
Cummer and	Check that the secured GeoNetworking message contains exactly one HeaderField	
Summary	generation_location and this location is inside the certificate validation restriction	
Reference	ETSI TS 103 097 [1], clause 7.2	
PICS Selection	PICS_GN_SECURITY AND NOT PICS_CERTIFICATE_SELECTION	
	Expected behaviour	
with		
the IUT being in the 'auth	orized' state	
ensure that		
when		
the IUT is requested to	send a DENM	
then		
the IUT sends a Secur		
	ields['signed_info'].certificate	
	r_restrictions ['region']	
	containing region.region_type	
indicating 'circle' containing region.circular_region		
containing region.circular_region indicating REGION		
or containing region_region_type		
indicating 'rectangle'		
containing region.rectangular_region		
containing array of rectangles		
indicating REGION		
or containing region.region_type		
indicating 'polygonal'		
containing region.polygonal_region		
indicating REGION		
or containing region.region_type		
indicating 'id_region' containing region.circular_region		
indicating REGION and containing exactly one header_field ['generation_location']		
containing genera		
	ion inside the REGION	
indicating locat		

24

# 5.2.5.6 Check Payload

TP ld	TP_SEC_ITSS_SND_DENM_08_01_BV	
Summary	Check that the Secured DENM contains non-empty payload of type signed	
Reference	ETSI TS 103 097 [1], clause 7.2	
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 DENM	
then		
the IUT sends a	SecuredMessage	
containing pay	/load_field	
containing type		
indicating	indicating 'signed'	
and containing not-empty data		

# 5.2.5.7 Check trailer field presence

Void.

TP Id	TP_SEC_ITSS_SND_DENM_10_01_BV
	Check that the secured DENM contains only one TrailerField of type signature;
Summary	Check that the signature contained in the SecuredMessage is calculated over the right fields
· · · · ·	by cryptographically verifying the signature
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
ensure that	
when	
the IUT is reque	sted to send DENM
then	
	SecuredMessage
	ader_field ['signer_info']
containing	
containin	
	ting 'certificate'
	aining certificate
	ning subject_info.subject_type
	cating 'authorization_ticket' (2)
	ontaining subject_attributes['verification key'] (KEY)
and containing	
	single instance of type TrailerField
containin	
	ting 'signature'
	aining signature
verifia	ble using KEY

#### 5.2.5.8 Check signature

# 5.2.6 Generic signed message profile

#### 5.2.6.1 Check secured its\_aid value

TP ld	TP_SEC_ITSS_SND_GENMSG_01_01_BV
C	Check that the sent Secured Message contains HeaderField its_aid that is set to other value
Summary	then AID_CAM and AID_DENM
Reference	ETSI TS 103 097 [1], clause 5.4
PICS Selection	PICS_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE
	Expected behaviour
with	
the IUT being in the	'authorized' state
ensure that	
when	
the IUT is request	ted to send a Beacon
then	
the IUT sends a S	;ecuredMessage
containing header_fields ['its_aid']	
containing its_aid	
indicating 'AID_BEACON'	

TP ld	TP_SEC_ITSS_SND_GENMSG_02_01_BV
	Check that the generic secured message contains exactly one element of these header
0	fields: signer_info, generation_time, generation_location;
Summary	Check that the header fields are in the ascending order according to the numbering of the
	enumeration except of the signer_info, which is encoded first
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
ensure that	
when	
the IUT is reques	sted to send a Beacon
then	
the IUT sends a	SecuredMessage
containing hea	ader_fields [0].type
indicating 's	signer_info'
	g header_fields [1n]
	ler_fields [i].type < header_fields [i+1].type
	g header_fields ['generation_time']
	g header_fields ['generation_location']
and containing header_fields ['its_aid']	

#### 5.2.6.2 Check header field

# 5.2.6.3 Check that signer info is a certificate

TP ld	TP_SEC_ITSS_SND_GENMSG_03_01_BV	
Summary	Check that generic secured message contains the certificate as a signer_info	
Reference	ETSI TS 103 097 [1], clause 7.3	
PICS Selection	PICS_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE	
	Expected behaviour	
with		
the IUT being in the 'a	authorized' state	
ensure that		
when		
the IUT is requeste	d to send a Beacon	
then		
the IUT sends a Se	curedMessage	
containing exact	ly one header_fields ['signer_info']	
containing sig	ner	
containing type		
indicating 'certificate'		
and containing certificate		

TP ld	TP_SEC_ITSS_SND_GENMSG_04_01_BV
Summary	Check that message generation time is inside the validity period of the signing certificate;
Summary	Check that message generation time value is realistic
Reference	ETSI TS 103 097 [1], clauses 5.4 and 7.3
PICS Selection	PICS_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE
	Expected behaviour
with	
the IUT being in the 'auth	norized' state
ensure that	
when	
the IUT is requested to	o send a Beacon
then	
the IUT sends a Secur	
<b>u</b> .	ne header_fields['generation_time']
containing genera	
	I_TIME (CUR_TIME - 10min <= GEN_TIME < CUR_TIME + 10min)
	der_fields['signer_info']
containing signer	
containing type	
indicating 'ce	
containing cert	
	alidity_restrictions['time_end'] ining end_validity
	ng value > GEN_TIME
	g validity_restrictions['time_start_and_end']
	g start_validity
	ng value <= GEN_TIME
	ining end_validity
	ng value > GEN_TIME
	g validity restrictions ['time start and duration']
	g start_validity (X_START_VALIDITY)
	ng value <= GEN_TIME
	ining duration
indicati	ng value > GEN_TIME - X_START_VALIDITY

# 5.2.6.4 Check generation time

# 5.2.6.5 Check generation location

TP ld	TP_SEC_ITSS_SND_GENMSG_05_01_BV	
Cummon (	Check that the secured GeoNetworking message contains exactly one HeaderField	
Summary	generation_location when AT certificate does not contain any region restrictions	
Reference	ETSI TS 103 097 [1], clause 7.3	
PICS Selection	PICS_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE AND	
FICS Selection	PICS_CERTIFICATE_SELECTION	
	Expected behaviour	
with		
the IUT has been auth	norized with the AT certificate (CERT_AT_A)	
not containing valid	ity_restrictions['region']	
ensure that		
when		
the IUT is requeste	the IUT is requested to send a Beacon	
then		
the IUT sends a SecuredMessage		
containing exactly one header_fields['generation_location']		
containing generation_location		
00		

TP ld	TP_SEC_ITSS_SND_GENMSG_05_02_BV		
	Check that the secured GeoNetworking message contains exactly one HeaderField		
Summary	generation_location which is inside the circular region containing in the validity restriction of		
	the certificate pointed by the signer_info field		
Reference	ETSI TS 103 097 [1], clause 7.3		
PICS Selection	PICS_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE AND		
FICS Selection	PICS_CERTIFICATE_SELECTION AND PICS_USE_CIRCULAR_REGION		
	Expected behaviour		
with			
the IUT has been au	uthorized with the AT certificate (CERT_AT_B)		
containing validity	/_restrictions ['region']		
containing regi	on		
containing re	∋gion_type		
indicating	'circle'		
	and containing circular_region		
indicating	indicating REGION		
ensure that			
when			
the IUT is reques	ted to send a Beacon		
then			
the IUT sends a S	SecuredMessage		
	ctly one header_fields['generation_location']		
containing generation_location			
indicating value inside the REGION			

TP ld	TP_SEC_ITSS_SND_GENMSG_05_03_BV
	Check that the secured GeoNetworking message contains exactly one HeaderField
Summary	generation_location which is inside the rectangular region containing in the validity
	restriction of the certificate pointed by the signer_info field
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE AND PICS_CERTIFICATE_SELECTION AND PICS_USE_RECTANGULAR_REGION
	Expected behaviour
with	
the IUT has been au	ithorized with the AT certificate (CERT_AT_C)
containing validity	_restrictions ['region']
containing regi	on
containing re	gion_type
indicating	'rectangle'
containing re	ectangular_region
containing	instance of RectangularRegion
indicati	ng REGION
ensure that	
when	
the IUT is reques	ted to send a Beacon
then	
the IUT sends a S	
	ctly one header_fields['generation_location']
	eneration_location
indicating	value inside the REGION

TP ld	TP_SEC_ITSS_SND_GENMSG_05_04_BV		
	Check that the secured GeoNetworking message contains exactly one HeaderField		
Summary	generation_location which is inside the polygonal region containing in the validity restriction of the certificate pointed by the signer_info field		
Reference	ETSI TS 103 097 [1], clause 7.3		
PICS Selection	PICS_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE AND PICS_CERTIFICATE_SELECTION AND PICS_USE_POLYGONAL_REGION		
	Expected behaviour		
with			
the IUT has been au	thorized with the AT certificate (CERT_AT_D)		
	_restrictions ['region']		
containing regio			
containing re			
indicating			
• .	lygonal_region		
	indicating REGION		
ensure that			
when			
the IUT is requested to send a Beacon			
then			
the IUT sends a S	6		
0	tly one header_fields['generation_location']		
containing generation_location indicating value inside the REGION			
indicating			

<b></b>	
TP ld	TP_SEC_ITSS_SND_GENMSG_05_05_BV
	Check that the secured GeoNetworking message contains exactly one HeaderField
Summary	generation_location which is inside the identified region containing in the validity restriction
	of the certificate pointed by the signer_info field
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE AND
FICS Selection	PICS_CERTIFICATE_SELECTION AND PICS_USE_IDENTIFIED_REGION
	Expected behaviour
with	
the IUT has been autho	rized with the AT certificate (CERT_AT_E)
containing validity_re	estrictions ['region']
containing region	
containing regio	n_type
indicating 'id_	
containing ident	ified_region
indicating RE	GION
ensure that	
when	
the IUT is requested	to send a Beacon
then	
the IUT sends a Sec	uredMessage
containing header	_fields ['its_aid']
indicating 'AID_	BEACON'
	one header_fields['generation_location']
containing gene	ration_location
indicating val	ue inside the REGION

TP ld	TP_SEC_ITSS_SND_GENMSG_05_06_BV		
	Check that the secured GeoNetworking message contains exactly one HeaderField		
Summary	generation_location and this location is inside the certificate validation restriction		
eference ETSI TS 103 097 [1], clause 7.3			
	PICS_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE AND NOT		
PICS Selection	PICS_CERTIFICATE_SELECTION		
	Expected behaviour		
with			
the IUT being in the 'aut	horized' state		
ensure that			
when			
the IUT is requested t	to send a Beacon		
then			
the IUT sends a Secu	0		
	_fields['signed_info'].certificate		
	ty_restrictions ['region']		
	jion.region_type		
indicating 'r			
	or containing region.region_type		
indicating 'c			
	jion.circular_region		
indicating F			
or containing reg			
indicating 'r	8		
containing region.rectangular_region			
containing array of rectangles			
	indicating REGION		
	or containing region.region_type indicating 'polygonal'		
	containing region.polygonal_region		
indicating REGION			
or containing region_type			
	indicating 'id_region'		
	jion.circular_region		
indicating R			
	ictly one header_fields['generation_location']		
	containing generation_location		
indicating location inside the REGION			

# 5.2.6.6 Check payload

TP Id	TP_SEC_ITSS_SND_GENMSG_06_01_BV
Summary	Check that the secured message contains the Payload element of type signed, signed_external or signed_and_encrypted
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE
	Expected behaviour
with the IUT being in the 'auth ensure that when the IUT is requested to then the IUT sends a Secur containing payload_ containing type indicating 'signe	send a Beacon edMessage

TP ld	TO SEC ITSS SND CENINSC 07 01 DV
	TP_SEC_ITSS_SND_GENMSG_07_01_BV
_	Check that the secured message contains only one TrailerField of type signature;
Summary	Check that the signature contained in the SecuredMessage is calculated over the right fields
	by cryptographically verifying the signature
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY AND NOT PICS_ITS_AID_OTHER_PROFILE
	Expected behaviour
with	
the IUT being in the	'authorized' state
ensure that	
when	
the IUT is request	ted to send a Beacon
then	
the IUT sends a S	SecuredMessage
containing hea	der_fields ['signer_info']
containing si	gner
containing	type
indicati	ng 'certificate'
containing certificate	
	ng CERT
	trailer_fields ['signature']
containing si	
verifiable using CERT.subject_attributes['verification_key']	

# 5.2.7 Profiles for certificates

#### 5.2.7.1 Check that certificate version is 2

TP ld	TP_SEC_ITSS_SND_CERT_01_01_BV
Summary	Check that AT certificate has version 2
Reference	ETSI TS 103 097 [1], clauses 6.1 and 7.4.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'auth	orized' state
the IUT being requested t	to include certificate in the SecuredMessage
ensure that	
when	
	send a SecuredMessage
then	
the IUT sends a Secure	
	ields['signer_info'].signer
containing type	
indicating certificate	
containing certificate	
containing version	
indicating '2'	

TP ld	TP_SEC_ITSS_SND_CERT_01_02_BV
Summary	Check that AA certificate has version 2
Reference	ETSI TS 103 097 [1], clauses 6.1 and 7.4.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
the IUT being reque	sted to include certificate chain in the next CAM
ensure that	
when	
the IUT is reques	ted to send a CAM
then	
	SecuredMessage
	der_fields['signer_info'].signer
containing type	
indicating 'certificate_chain'	
and containing certificates	
indicating length $N > 0$	
and containing certificates [n] (0N)	
containing version	
indic	ating '2'

#### 5.2.7.2 Check the certificate chain consistence

TP ld	TO SEC ITSS SND CEDT 02 01 BV
	TP_SEC_ITSS_SND_CERT_02_01_BV
	Check that the references in the certificate chain are valid
Summary	Check that signer_info type of all certificates in the chain are
	certificate_digest_with_sha256', 'certificate_digest_with_other_algorithm'or 'self'
	ETSI TS 103 097 [1], clauses 4.2.10, 6.1 and 7.4.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'author	
•	o include certificate chain in the next CAM
ensure that	
when the IUT is requested to	cond a CAM
then	
the IUT sends a Secure	edMessage
	elds['signer_info'].signer
containing type	
indicating 'certif	icate chain'
and containing cer	
indicating length	
and containing	certificates[0]
containing sig	gner_info
containing	type
	ng 'certificate_digest_with_sha256'
	ating 'certificate_digest_with_other_algorythm'
	ning digest
	sing the trusted certificate
or containing	
containing	
indicatin	g seir certificates[n] (1N)
containing sig	
containing	
	ig 'certificate_digest_with_sha256'
	ating 'certificate_digest_with_other_algorythm'
	ning digest
	sing the certificates[n-1]
reference	

5.2.7.5 Che	
TP ld	TP_SEC_ITSS_SND_CERT_04_01_BV
	Check that the rectangular region validity restriction of the message signing certificate
Summany	contains not more than six valid rectangles;
Summary	Check that the rectangular region validity restriction of the message signing certificate is
	continuous and does not contain any holes
Reference	ETSI TS 103 097 [1], clauses 4.2.20 and 4.2.23
PICS Selection	PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND
PICS Selection	PICS_USE_RECTANGULAR_REGION
	Expected behaviour
with	
the IUT being in the '	authorized' state
the IUT being reques	ted to include certificate in the next CAM
ensure that	
when	
the IUT is requeste	ed to send a CAM
then	
the IUT sends a Se	•
	er_fields['signer_info'].signer
containing typ	
indicating '	
containing ce	
•	validity_restrictions['region']
	ng region
	ning region_type
	cating 'rectangle'
	ontaining rectangular_region
	cating length <= 6
	I containing elements of type RectangularRegion
	ndicating continuous region without holes
a	ind containing northwest and southeast
	indicating northwest is on the north from southeast

33

#### 5.2.7.3 Check rectangular region validity restriction

TP ld	TP_SEC_ITSS_SND_CERT_04_02_BV
	Check that the rectangular region validity restriction of all certificates contains not more than
_	six valid rectangles;
	Check that the rectangular region validity restriction of the AT certificate is continuous and
Summary	does not contain any holes
	Check that the rectangular certificate validity region of the subordinate certificate is well
	formed and inside the validity region of the issuing certificate
Reference	ETSI TS 103 097 [1], clauses 4.2.20 and 4.2.23
PICS Selection	PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND
PICS Selection	PICS_USE_RECTANGULAR_REGION
	Expected behaviour
with	
the IUT being in the	
0 1	ested to include certificate chain in the next CAM
ensure that	
when	
	sted to send a CAM
then	
	SecuredMessage
	ider_fields['signer_info'].signer
containing t	
	'certificate_chain'
containing c	
	length $N > 0$
	aining certificates [n] (0N)
	ning validity_restrictions['region']
	aining region
CC	ontaining region_type
	indicating 'rectangle'
and containing rectangular_region	
	indicating length <= 6
	and containing elements of type RectangularRegion
	containing northwest and southeast
	indicating northwest on the north from southeast
	and indicating continuous region without holes

# 5.2.7.4 Check polygonal region validity restriction

TP ld	TP_SEC_ITSS_SND_CERT_05_01_BV
	Check that the polygonal certificate validity region contains at least three and no more than
Summary	12 points;
	Check that the polygonal certificate validity region does not contain intersections and holes
Reference	ETSI TS 103 097 [1], clause 4.2.24
PICS Selection	PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND
PICS Selection	PICS_USE_POLYGONAL_REGION
	Expected behaviour
with	
the IUT being in the	'authorized' state
the IUT being reque	sted to include certificate in the next CAM
ensure that	
when	
the IUT is reques	ted to send a CAM
then	
the IUT sends a S	0
	der_fields['signer_info'].signer
containing ty	
	'certificate'
containing c	
	validity_restrictions['region']
	ing region
	aining region_type
	dicating 'polygon'
	containing polygonal_region
	dicating length $>=3$ and $<=12$
an	d indicating continuous region without holes and intersections

	35	ETSI TS 103 096-2 V1.3.1 (2017-03)
TP Id	TP_SEC_ITSS_SND_CERT_05_02_E	31/
Summary	Check that the polygonal certificate va certificate;	lidity region is inside the validity region of the issuing ficate validity region contains at least three and no
-		icate validity region does not contain intersections and
Reference	ETSI TS 103 097 [1], clause 4.2.24	
PICS Selection	PICS_GN_SECURITY AND PICS_CE PICS_USE_POLYGONAL_REGION	RTIFICATE_SELECTION AND
	Expected behave	<i>v</i> iour
ensure that when the IUT is request then the IUT sends a S containing head containing ty indicating and containin indicating and containin containin containin	der_fields['signer_info'].signer	
an	d containing polygonal_region indicating length >=3 and <=12 and indicating continuous region without hol	les and intersections

TP ld	TP_SEC_ITSS_SND_CERT_06_01_BV
	Check that the identified certificate validity region contains values that correspond to
Summary	numeric country codes as defined in ISO 3166-1 [4] or defined by United Nations Statistics
	Division [5]
Reference	ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND
PICS Selection	PICS_USE_IDENTIFIED_REGION
	Expected behaviour
with	
the IUT being in the	'authorized' state
the IUT being reque	sted to include certificate in the next CAM
ensure that	
when	
the IUT is reques	ted to send a CAM
then	
the IUT sends a S	SecuredMessage
containing hea	der_fields['signer_info'].signer
containing ty	
	'certificate'
and containi	ng certificate
containing	g validity_restrictions['region']
	ing region
	aining region_type
	dicating 'id'
	containing id_region
	ntaining region_dictionary
	indicating 'iso_3166_1'
	d containing region_identifier
	indicating valid value according to ISO-3166-1
and containing local_region	
	ntaining id_region
	ntaining region_dictionary
	indicating 'un_stats'
	d containing region_identifier
	indicating valid value according to UN STATS
an	d containing local_region

# 5.2.7.5 Check identified region validity restriction

TP ld	TP_SEC_ITSS_SND_CERT_06_02_BV	
	Check that the identified certificate validity region contains values that correspond to	
	numeric country codes as defined in ISO 3166-1 [4] or defined by United Nations Statistics	
Summary	Division [5];	
_	Check that the identified certificate validity region contains values defining the region which	
	is inside the validity region of the issuing certificate	
Reference	ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1	
PICS Selection	PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND	
	PICS_USE_IDENTIFIED_REGION	
	Expected behaviour	
with		
the IUT being in the 'auth		
<b>.</b> .	to include certificate chain in the next CAM	
ensure that		
when		
the IUT is requested to	Send a CAIVI	
then the IUT conde a Secur	odMossago	
the IUT sends a Secur		
	containing header_fields['signer_info'].signer	
	containing type	
	indicating 'certificate_chain' and containing certificates	
	indicating length N > 1	
and containing certificates[n](0N)		
	containing validity_restrictions['region']	
containing		
containi	ing region_type	
indica	ating 'id'	
	ntaining id_region	
	aining region_dictionary	
	indicating 'iso_3166_1'	
and containing region_identifier		
indicating valid value according to ISO_3166-1 dictionary		
	and containing local_region	
or containing region		
containing region_type		
indicating 'id'		
and containing id_region containing region_dictionary		
	dicating 'un_stats'	
	containing region_identifier	
indicating valid value according to UN STATS dictionary		
and containing local_region		

TP ld	TP_SEC_ITSS_SND_CERT_07_01_BV	
	Check that the region of the subordinate certificate validity restriction is inside the region of	
Summary	the issuing certificate validity restriction	
Reference	ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1	
PICS Selection	PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION	
	Expected behaviour	
with		
the IUT being in the 'au	thorized' state	
	d to include certificate chain in the next CAM	
ensure that		
when		
the IUT is requested	to send a CAM	
then		
the IUT sends a Secu		
	_fields['signer_info'].signer	
containing type	tificate chairl	
	rtificate_chain'	
and containing o indicating len		
	g certificates[n](0N)	
indicating of		
	aining validity_restrictions['region']	
	taining signer_info	
	ining digest	
	erencing the certificate	
r	not containing validity_restrictions['region']	
	g certificate	
	ng validity_restrictions['region']	
	ning region.region_type	
	cating 'none'	
	taining signer_info	
	ining digest	
	erencing the certificate not containing validity_restrictions['region']	
	or containing validity_restrictions['region']	
	containing region.region_type	
	indicating 'none'	
or indicatin	g certificate	
	ng validity_restrictions['region']	
contai	ining region.region_type	
indicated 'circle'		
	ndicated 'rectangle'	
	ndicated 'polygon'	
_	or indicated 'id'	
and containing region (X_CERTREGION)		
	taining signer_info ining digest	
	erencing the certificate	
	not containing validity_restrictions['region']	
	or containing validity_restrictions['region']	
	containing region.region_type	
	indicating 'none'	
c	or containing validity_restrictions['region']	
	containing region	
indicating region fully covering the X_CERT_REGION		

# 5.2.7.6 Check region validity restrictions in the chain

39	

TP ld	TP_SEC_ITSS_SND_CERT_07_02_BV
Cummon.	Check that the identified region validity restriction of the subordinate certificate is included in
Summary	the identified region validity restriction of the issuing certificate
Reference	ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1
	PICS_GN_SECURITY AND PICS_CERTIFICATE_SELECTION AND
PICS Selection	PICS_USE_IDENTIFIED_REGION
	Expected behaviour
with	
the IUT being in the 'a	authorized' state
	AA and AT certificates with identified region validity restriction
•	ted to include certificate chain in the next CAM
ensure that	
when	
the IUT is requeste	ed to send a CAM
then	
the IUT sends a Se	
	er_fields['signer_info'].signer
containing typ	
	certificate_chain'
containing ce	
indicating le	
	ning certificates [n] (0N)
	ig validity_restrictions['region']
containing region	
containing region_type	
	ndicating 'id'
	taining id_region
C	ontaining region_dictionary
indicating 'iso_3166_1'	
_	or indicating 'un_stats'
containing region_identifier (X_CERT_REGION_ID)	
_	indicating valid value according to ISO_3166-1 or UN STATS dictionary
	ontaining local_region (X_CERT_LOCAL_REGION)
	aining signer_info
containing digest	
referencing the certificate	
containing validity_restrictions['region']	
containing region	
containing region_type	
indicating 'id'	
containing id_region	
containing region_dictionary	
indicating 'iso_3166_1' or indicating 'un_stats'	
and containing region_identifier	
	indicating value == X_CERT_REGION_ID
	and containing local_region
	indicating value == X_CERT_LOCAL_REGION
	or indicating 0
	or containing id_region
	containing region_dictionary
	indicating 'un_stats'
	and containing region_identifier
indicating value fully covering the X_CERT_REGION_ID	

TP ld	TP_SEC_ITSS_SND_CERT_08_01_BV	
Summary	Check the certificate chain to ensure that the time validity restriction of the subordinate certificate is inside the time validity restriction of the issuing certificate	
Reference	ETSI TS 103 097 [1], clause 7.4.4	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'aut	thorized' state	
	d to include certificate chain in the next CAM	
ensure that		
when		
the IUT is requested	to send a CAM	
then		
the IUT sends a Secu	uredMessage	
	_fields['signer_info'].signer	
containing type		
indicating 'cer	tificate_chain'	
containing certif	icates	
indicating leng	yth N > 1	
and containin	g certificates[n] (0N)	
	validity_restrictions	
	ng validity_restrictions['time_end']	
	ning end_validity	
	cating X_END_VALIDITY_AT	
	ining validity_restrictions['time_start_and_end']	
	ning start_validity	
	cating X_START_VALIDITY_AT	
	cating X_END_VALIDITY_AT >X_START_VALIDITY_AT	
	ining validity_restrictions['time_start_and_duration']	
	ning start_validity cating X_START_VALIDITY_AT	
	calling X_START_VALIDITT_AT	
	cating X_DURATION_AT > 0	
	and containing signer_info containing digest	
	ncing the certificate	
	taining validity_restrictions['time_end']	
	containing end_validity	
	indicating value >= X_END_VALIDITY_AT if defined	
	or indicating value >= X_START_VALIDITY_AT + X_DURATION_AT	
ord	containing validity_restrictions['time_start_and_end']	
c	containing start_validity	
	indicating value <= X_START_VALIDITY_AT if defined	
	or indicating value <= CURRENT_TIME	
a	and containing end_validity	
	indicating value >= X_END_VALIDITY_AT if defined	
	or indicating value >= X_START_VALIDITY_AT + X_DURATION_AT	
	containing validity_restrictions['time_start_and_duration']	
C	containing start_validity	
	indicating X_START_VALIDITY_AA <= X_START_VALIDITY_AT if defined	
	or indicating X_START_VALIDITY_AA <= CURRENT_TIME	
a	ind containing duration	

## 5.2.7.7 Check time validity restriction in the chain

or indicating X\_START\_VALIDITY\_AA <= CURRENT\_TIME and containing duration indicating value >= X\_END\_VALIDITY\_AT - X\_START\_VALIDITY\_AA if defined or indicating value >= X\_START\_VALIDITY\_AT + X\_DURATION\_AT -X\_START\_VALIDITY\_AA

5.2.7.8	Check ECC point	type of the ce	ertificate signature
			in allo orginalaro

TP ld	TP_SEC_ITSS_SND_CERT_09_01_BV	
Summary	Check that the certificate signature contains ECC point of type set to either	
Reference	compressed_lsb_y_0, compressed_lsb_y_1 or x_coordinate_only ETSI TS 103 097 [1], clause 4.2.9	
PICS Selection	PICS_GN_SECURITY	
PICS Selection		
with	Expected behaviour	
with		
the IUT being in the	ested to include certificate in the next CAM	
ensure that		
when		
	sted to send a CAM	
then		
	SecuredMessage	
	ader_fields['signer_info'].signer	
containing t		
indicating	j 'certificate'	
containing c		
containin	g signature.ecdsa_signature	
	ning R.type	
	cating compressed_lsb_y_0	
	idicating compressed_lsb_y_1	
or in	dicating x_coordinate_only	
TP ld	TP_SEC_ITSS_SND_CERT_09_02_BV	
	Check that the all certificates in a chain have signatures contains ECC point of type set to	
Summary	either compressed_lsb_y_0, compressed_lsb_y_1 or x_coordinate_only	
Reference	ETSI TS 103 097 [1], clause 4.2.9	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	a 'authorized' state	
	ested to include certificate in the next CAM	
ensure that		
when		
the IUT is requested to send a CAM		
then		
the IUT sends a	SecuredMessage	
containing header_fields['signer_info'].signer		
containing t	ype	
indicating	y 'certificate_chain'	
containing certificates		
	indicating length N > 1	
	aining certificates[n](0N)	
	ning signature.ecdsa_signature	
	aining R.type	
	dicating compressed_lsb_y_0	
or indicating compressed_lsb_y_1		
or indicating x_coordinate_only		

# 5.2.7.9 Check ECC point type of the certificate verification key

TP ld	TP_SEC_ITSS_SND_CERT_10_01_BV	
Summary	Check that the certificate verification key contains ECC point of type set to either	
Summary	compressed_lsb_y_0, compressed_lsb_y_1 or uncompressed	
Reference	ETSI TS 103 097 [1], clause 4.2.4	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'auth	orized' state	
	to include certificate in the next CAM	
ensure that		
when		
the IUT is requested to	o send a CAM	
then		
the IUT sends a Secur		
	ields['signer_info'].signer	
containing type		
indicating 'certi		
and containing ce		
	ect_attributes['verification_key']	
	ey.public_key.type compressed_lsb_y_0	
	ng compressed_lsb_y_1	
	ng uncompressed	
of indicati	ig uncompressed	
TP ld	TP_SEC_ITSS_SND_CERT_10_02_BV	
<b>0</b>	Check that all certificate in a chain have verification keys contains ECC point of type set to	
Summary	either compressed_lsb_y_0, compressed_lsb_y_1 or uncompressed	
Reference	ETSI TS 103 097 [1], clause 4.2.4	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'auth	orized' state	
the IUT being requested	to include certificate in the next CAM	
ensure that		
when		
the IUT is requested to send a CAM		
then		
the IUT sends a SecuredMessage		
containing header_fields['signer_info'].signer		
containing type		
indicating 'certificate_chain'		
and containing certificates		
	indicating length N > 0 containing certificates [n] (0N)	
	ubject_attributes['verification_key']	
	j key.public_key.type	
	ng compressed lsb_y_0	
or indicating compressed_lsb_y_1		
or indicating uncompressed		
or indicating uncompressed		

TO LL		
TP ld	TP_SEC_ITSS_SND_CERT_11_01_BV	
Summary Check the certificate signature		
Reference	ETSI TS 103 097 [1], clauses 6.1 and 7.4.1	
PICS Selection	PICS_GN_SECURITY	
Expected behaviour		
with		
the IUT being in the 'auth		
	to include certificate in the next CAM	
ensure that		
when		
the IUT is requested to	o send a CAM	
then		
the IUT sends a Secur		
	ields['signer_info'].signer	
containing type		
indicating 'certi	ficate'	
and containing ce		
containing sign		
containing ty		
	'certificate_digest_with_sha256'	
and containi		
	g the certificate CERT	
and containing		
verifiable us	ing CERT.subject_attributes['verification_key'].key	
TP ld		
	TP_SEC_ITSS_SND_CERT_11_02_BV	
Summary	Check the validity of signatures of all certificates in the chain	
Reference	ETSI TS 103 097 [1], clauses 6.1 and 7.4.1	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
-		
the IUT being in the 'auth		
the IUT being in the 'auth the IUT being requested	norized' state to include certificate chain in the next CAM	
the IUT being in the 'auth the IUT being requested ensure that		
the IUT being in the 'auth the IUT being requested ensure that when	to include certificate chain in the next CAM	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to	to include certificate chain in the next CAM	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then	to include certificate chain in the next CAM	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur	to include certificate chain in the next CAM o send a CAM redMessage	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f	to include certificate chain in the next CAM	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type	to include certificate chain in the next CAM o send a CAM redMessage ields['signer_info'].signer	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi	to include certificate chain in the next CAM o send a CAM redMessage ields['signer_info'].signer	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi	to include certificate chain in the next CAM o send a CAM redMessage ields['signer_info'].signer ficate_chain' ertificates	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi indicating lengt	to include certificate chain in the next CAM o send a CAM redMessage ields['signer_info'].signer ficate_chain' ertificates th N > 1	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi and containing certi and containing lengt and containing	to include certificate chain in the next CAM o send a CAM redMessage ields['signer_info'].signer ficate_chain' ertificates th N > 1 certificates[0]	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi and containing containing containing s	to include certificate chain in the next CAM o send a CAM redMessage ields['signer_info'].signer ficate_chain' ertificates th N > 1 certificates[0] igner_info	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi and containing end indicating lengt and containing s containing s	to include certificate chain in the next CAM o send a CAM redMessage ields['signer_info'].signer ficate_chain' ertificates th N > 1 certificates[0] igner_info g type	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi and containing certi and containing containing containing containing containing containing containing containing	to include certificate chain in the next CAM o send a CAM redMessage ields['signer_info'].signer ficate_chain' ertificates th N > 1 certificates[0] igner_info g type ng 'certificate_digest_with_sha256'	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi and containing certi and containing containing s containing indicati and containing containing containing containing containing	to include certificate chain in the next CAM o send a CAM redMessage ields['signer_info'].signer ficate_chain' ertificates th N > 1 certificates[0] igner_info g type ng 'certificate_digest_with_sha256' ining digest	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi and containing containing containing s containing s indicati and containing referen	to include certificate chain in the next CAM o send a CAM redMessage ields['signer_info'].signer ficate_chain' ertificates th N > 1 certificates[0] igner_info g type ng 'certificate_digest_with_sha256' ining digest cing the trusted certificate (CERT_ROOT)	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi and containing containing containing s containing s indicati and containing referen and containing	to include certificate chain in the next CAM o send a CAM redMessage ields['signer_info'].signer ficate_chain' ertificates th N > 1 certificates[0] igner_info g type ng 'certificate_digest_with_sha256' ining digest cing the trusted certificate (CERT_ROOT) ng signature	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi and containing containing containing s containing s containing indicati and containing verifiable	to include certificate chain in the next CAM o send a CAM redMessage ields['signer_info'].signer ficate_chain' ertificates th N > 1 certificates[0] igner_info g type ng 'certificate_digest_with_sha256' ining digest cing the trusted certificate (CERT_ROOT) ng signature using CERT_ROOT	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi and containing containing containing s containing s containing indicati and containing s containing indicati and containing s containing indicati and containing s containing indicati	to include certificate chain in the next CAM o send a CAM redMessage ields['signer_info'].signer ficate_chain' ertificates th N > 1 certificates[0] igner_info g type ng 'certificate_digest_with_sha256' ining digest cing the trusted certificate (CERT_ROOT) ng signature using CERT_ROOT ect_attributes['verification_key'].key	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi and containing certi and containing containing s containing indicati and containing s containing containing s containing indicati and containing s containing indicati and containing s contain containing s contain contai contain contai contai contai contai contai co	to include certificate chain in the next CAM o send a CAM redMessage ields['signer_info'].signer ficate_chain' ertificates th N > 1 certificates[0] igner_info 0 type ng 'certificate_digest_with_sha256' ining digest cing the trusted certificate (CERT_ROOT) ng signature using CERT_ROOT ect_attributes['verification_key'].key certificates[n] (1N)	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi and containing containing containing s containing indicati and containing s containing s containing indicati and containing s containing s containing s containing s containing s containing containing s containing containing s	to include certificate chain in the next CAM o send a CAM redMessage ields['signer_info'].signer ficate_chain' prificates th N > 1 certificates[0] igner_info o type ng 'certificate_digest_with_sha256' ining digest cing the trusted certificate (CERT_ROOT) ng signature using CERT_ROOT ect_attributes['verification_key'].key certificates[n] (1N) igner_info	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi and containing containing containing s containing indicati and containing s containing s containing indicati and containing s containing s containing containing containing s containing containing containing containing containing containing containing containing	to include certificate chain in the next CAM o send a CAM redMessage ields['signer_info'].signer ficate_chain' rtificates th N > 1 certificates[0] igner_info o type ng 'certificate_digest_with_sha256' ining digest cing the trusted certificate (CERT_ROOT) ng signature using CERT_ROOT ect_attributes['verification_key'].key certificates[n] (1N) igner_info o type	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi and containing containing containings containings containings containings indicati and containing containings containing scontaining verifiable .subj and containing containing containing containing containing containing containing containing containing	to include certificate chain in the next CAM p send a CAM redMessage ields['signer_info'].signer ficate_chain' rtificates th N > 1 certificates[0] igner_info g type ng 'certificate_digest_with_sha256' ining digest cing the trusted certificate (CERT_ROOT) ng signature using CERT_ROOT ect_attributes['verification_key'].key certificates[n] (1N) igner_info g type ng 'certificate_digest_with_sha256'	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi and containing containing containing s containing indicati and containing s containing s containing indicati and containing containing containing containing containing containing containing containing containing containing containing containing containing containing containing containing containing containing containing	to include certificate chain in the next CAM edMessage ields['signer_info'].signer ficate_chain' ertificates th N > 1 certificates[0] igner_info g type ng 'certificate_digest_with_sha256' ining digest cing the trusted certificate (CERT_ROOT) ng signature using CERT_ROOT ect_attributes['verification_key'].key certificates[n] (1N) igner_info g type ng 'certificate_digest_with_sha256' ining digest	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi and containing containing containing s containing s containing indicati and containing s containing indicati and containing	to include certificate chain in the next CAM p send a CAM redMessage ields['signer_info'].signer ficate_chain' prtificates th N > 1 certificates[0] igner_info g type ng 'certificate_digest_with_sha256' ining digest cing the trusted certificate (CERT_ROOT) ng signature using CERT_ROOT ect_attributes['verification_key'].key certificates[n] (1N) igner_info g type ng 'certificate_digest_with_sha256' ining digest cing the certificates[n-1]	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi and containing containing containing s containing containing s containing containing s containing indicati and containing verifiable .subj and containing containing containing containing s containing containing and containing containing containing containing containing containing containing containing containing containing containing containing containing containing containing containing containing containing containing	to include certificate chain in the next CAM edMessage ields['signer_info'].signer ficate_chain' rttificates th N > 1 certificates[0] igner_info 1 type ng 'certificate_digest_with_sha256' ining digest cing the trusted certificate (CERT_ROOT) ng signature using CERT_ROOT ect_attributes['verification_key'].key certificates[n] (1N) igner_info 1 type ng 'certificate_digest_with_sha256' ining digest cing the certificates[n-1] ng signature	
the IUT being in the 'auth the IUT being requested ensure that when the IUT is requested to then the IUT sends a Secur containing header_f containing type indicating 'certi and containing certi and containing containing containing s containing indicati and containing s containing s containing indicati and containing verifiable .subj and containing containing containing s containing s containing s containing contain contain containing contain contain contain contain contain contai	to include certificate chain in the next CAM p send a CAM redMessage ields['signer_info'].signer ficate_chain' prtificates th N > 1 certificates[0] igner_info g type ng 'certificate_digest_with_sha256' ining digest cing the trusted certificate (CERT_ROOT) ng signature using CERT_ROOT ect_attributes['verification_key'].key certificates[n] (1N) igner_info g type ng 'certificate_digest_with_sha256' ining digest cing the certificates[n-1]	

# 5.2.7.10 Verify certificates signatures

TP ld	TP_SEC_ITSS_SND_CERT_12_01_BV	
Summony	Check that the assurance level of the subordinate certificate is equal to or less than the	
Summary	assurance level of the issuing certificate	
Reference	ETSI TS 103 097 [1], clause 7.4.1	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	authorized' state	
the IUT being reque	ested to include certificate chain in the next CAM	
ensure that		
when		
the IUT is reques	ted to send a CAM	
then		
the IUT sends a	•	
	ider_fields['signer_info'].signer	
containing ty		
	'certificate_chain'	
containing c		
0	length N > 1	
and containing certificates[n](0N)		
containing subject_attributes ['assurance_level']		
containing assurance_level		
containing bits [5-7]		
indicating assurance level CERT_AL		
and containing signer_info		
containing digest		
referencing the certificate		
	containing subject_attributes ['assurance_level']	
	containing assurance_level	
	containing bits [5-7]	
indicating value <= CERT_AL		

### 5.2.7.11 Check certificate assurance level in the chain

### 5.2.7.12 AA certificate profile

### 5.2.7.12.1 Check AA certificate subject type

	TP_SEC_ITSS_SND_CERT_AA_01_01_BV
Summary	Check that the subject_type of the AA certificate is set to authorization_authority
Reference	ETSI TS 103 097 [1], clause 7.4.4
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'autho	prized' state
the IUT being requested to	o include certificate chain in the next CAM
ensure that	
when	
the IUT is requested to send a CAM	
then	
the IUT sends a Secure	edMessage
containing header_fields['signer_info'].signer	
containing type	
indicating 'certificate_chain'	
and containing certificates	
containing certificates[last-1]	
containing subject_info.subject_type	
indicating 'authorization_authority'	

Check that the AA certificsate subject_name variable-length vector contains 32 bytes maximum           Reference         ETSI TS 103 097 [1], clause 6.2           ICS Selection         PICS_GN_SECURITY           Expected behaviour           rith         the IUT being in the 'authorized' state           the IUT being requested to include certificate chain in the next CAM           nsure that         when           the IUT is requested to send a CAM           then         the IUT sends a SecuredMessage           containing header_fields['signer_info'].signer           containing type         indicating 'certificate_chain'	TP Id	TP SEC ITSS SND CERT AA 02 01 BV		
maximum         teference       ETSI TS 103 097 [1], clause 6.2         ICS Selection       PICS_GN_SECURITY         Expected behaviour         ith       the IUT being in the 'authorized' state         the IUT being requested to include certificate chain in the next CAM         nsure that         when         the IUT is requested to send a CAM         then         the IUT sends a SecuredMessage         containing header_fields['signer_info'].signer         containing type         indicating 'certificate_chain'				
Iteration         ETSI TS 103 097 [1], clause 6.2           ICS Selection         PICS_GN_SECURITY           Expected behaviour           ith         the IUT being in the 'authorized' state           the IUT being requested to include certificate chain in the next CAM           nsure that         when           the IUT is requested to send a CAM           then         the IUT sends a SecuredMessage           containing header_fields['signer_info'].signer           containing type         indicating 'certificate_chain'	Summary			
IDEX Selection         PICS_GN_SECURITY           Expected behaviour           rith         the IUT being in the 'authorized' state           the IUT being requested to include certificate chain in the next CAM           nsure that           when           the IUT is requested to send a CAM           then           the IUT sends a SecuredMessage           containing header_fields['signer_info'].signer           containing type           indicating 'certificate_chain'				
Expected behaviour         vith         the IUT being in the 'authorized' state         the IUT being requested to include certificate chain in the next CAM         nsure that         when         the IUT is requested to send a CAM         then         the IUT sends a SecuredMessage         containing header_fields['signer_info'].signer         containing type         indicating 'certificate_chain'	Reference	ETSI TS 103 097 [1], clause 6.2		
ith the IUT being in the 'authorized' state the IUT being requested to include certificate chain in the next CAM nsure that when the IUT is requested to send a CAM then the IUT sends a SecuredMessage containing header_fields['signer_info'].signer containing type indicating 'certificate_chain'	PICS Selection	PICS_GN_SECURITY		
the IUT being in the 'authorized' state the IUT being requested to include certificate chain in the next CAM nsure that when the IUT is requested to send a CAM then the IUT sends a SecuredMessage containing header_fields['signer_info'].signer containing type indicating 'certificate_chain'		Expected behaviour		
the IUT being requested to include certificate chain in the next CAM nsure that when the IUT is requested to send a CAM then the IUT sends a SecuredMessage containing header_fields['signer_info'].signer containing type indicating 'certificate_chain'	with			
nsure that when the IUT is requested to send a CAM then the IUT sends a SecuredMessage containing header_fields['signer_info'].signer containing type indicating 'certificate_chain'	the IUT being in the 'auth	norized' state		
when the IUT is requested to send a CAM then the IUT sends a SecuredMessage containing header_fields['signer_info'].signer containing type indicating 'certificate_chain'	the IUT being requested	to include certificate chain in the next CAM		
the IUT is requested to send a CAM then the IUT sends a SecuredMessage containing header_fields['signer_info'].signer containing type indicating 'certificate_chain'	ensure that	5 1		
then the IUT sends a SecuredMessage containing header_fields['signer_info'].signer containing type indicating 'certificate_chain'				
the IUT sends a SecuredMessage containing header_fields['signer_info'].signer containing type indicating 'certificate_chain'	the IUT is requested to	the IUT is requested to send a CAM		
containing header_fields['signer_info'].signer containing type indicating 'certificate_chain'	then			
containing typeindicating 'certificate_chain'	the IUT sends a SecuredMessage			
containing typeindicating 'certificate_chain'	5			
	0 - 10 - 10			
	0.51			
and containing certificates				
containing certificates[last-1]				
containing subject_info.subject_name	5			
indicating length <= 32 bytes				

## 5.2.7.12.2 Check AA certificate subject name

## 5.2.7.12.3 Check that signer info of AA certificate is a digest

TP ld	TP_SEC_ITSS_SND_CERT_AA_03_01_BV
Summary	Check that signer_info type of AA certificates is set to 'certificate_digest_with_sha256'
Reference	ETSI TS 103 097 [1], clause 7.4.4
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
the IUT being reque	sted to include certificate chain in the next CAM
ensure that	
when	
the IUT is reques	ted to send a CAM
then	
the IUT sends a	5
•	der_fields['signer_info'].signer
containing ty	
0	'certificate_chain'
	ng certificates
	g certificates[last-1]
containing signer_info	
	aining type
in	dicating 'certificate_digest_with_sha256'

TP ld	TP_SEC_ITSS_SND_CERT_AA_04_01_BV
Summary	Check that AA certificate is signed by Root CA or other authority.
Summary	NOTE: There is no clear specification that AA cert shall be signed by the Root CA only.
ETSI TS 103 097 [1], clause 6.3	
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'auth	norized' state
•	to include certificate chain in the next CAM
ensure that	
when	
the IUT is requested to	o send a CAM
then	
the IUT sends a Secur	0
	fields['signer_info'].signer
containing type	ificate chain!
indicating 'certificate_chain'	
and containing certificates	
containing certificates[last-1] containing signer_info	
containing type	
indicating 'certificate_digest_with_ecdsap256'	
and containing digest	
referencing to the trusted certificate	
	aining subject_info.subject_type
	dicating 'root_ca'
or	indicating 'authorisation_authority'

### 5.2.7.12.4 Check that AA cert is signed by Root cert

#### 5.2.7.12.5 Check AA ceretificate subject attributes presence and order

TP ld	TP_SEC_ITSS_SND_CERT_AA_05_01_BV
Summary	Check that all necessary subject attributes are present and arranged in ascending order
Reference	ETSI TS 103 097 [1], clauses 6.1, 7.4.1 and 7.4.4
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
the IUT being reque	ested to include certificate chain in the next CAM
ensure that	
when	
the IUT is reques	ted to send a CAM
then	
the IUT sends a s	SecuredMessage
•	der_fields['signer_info'].signer
containing ty	
0	'certificate_chain'
	ng certificates
	g certificates[last-1]
	ing subject_attributes [0N]
indic	ating subject_attributes[n].type
	< subject_attributes[n+1].type
	containing subject_attributes['verification_key']
	containing subject_attributes['assurance_level']
and	containing subject_attributes['its_aid_list']

TP ld	TP_SEC_ITSS_SND_CERT_AA_08_01_BV	
Summary	Check that all AIDs containing in the its_aid_list in AA certificate are unique	
	Check that AID list contains not more than 31 items	
Reference	ETSI TS 103 097 [1], clause 7.4.4	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'au	ithorized' state	
the IUT being requeste	d to include certificate chain in the next CAM	
ensure that		
when		
the IUT is requested to send a CAM		
then		
the IUT sends a Sec	uredMessage	
containing header	_fields['signer_info'].signer	
containing type		
indicating certificate_chain		
and containing certificates		
containing certificates[last-1]		
containing subject_attributes['its_aid_list']		
	ng its_aid_list	
conta	ining not more than 31 unique items	

#### 5.2.7.12.6 Check ITS-AID list of AA certificate

#### 5.2.7.12.7 Check AA certificate validity restriction presence and order

TP ld	TP_SEC_ITSS_SND_CERT_AA_10_01_BV
Summary	Check that all mandatory validity restrictions are present and arranged in ascending order
Reference	ETSI TS 103 097 [1], clauses 6.1, 6.7 and 7.4.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'au	uthorized' state
the IUT being requeste	ed to include certificate chain in the next CAM
ensure that	
when	
the IUT is requested	to send a CAM
then	
the IUT sends a Sec	0
5	r_fields['signer_info'].signer
containing type	
	ertificate_chain'
and containing	
•	ertificates[last-1]
	validity_restrictions[0N]
	ng validity_restrictions[n].type
	/alidity_restrictions[n+1].type
	ntaining validity_restrictions['time_start_and_end'] containing validity_restrictions['time_end']
and not	containing validity_restrictions['time_start_and_duration']

TP ld	TP_SEC_ITSS_SND_CERT_AA_11_01_BV
	Check that time_start_and_end is included in the AA certificate validation restrictions;
Summen	Check that end_validity is greater than start_validity;
Summary	Check that validity restriction of AA certificate is inside the validity restriction of its issuing
	certificate
Reference	ETSI TS 103 097 [1], clause 7.4.4
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'aut	
5 1	to include certificate chain in the next CAM
ensure that	
when	
the IUT is requested t	io send a CAM
then	
the IUT sends a Secu	
	fields['signer_info'].signer
containing type	
indicating 'cer	
containing certifi	
	tificates[last-1]
	validity_restrictions
	g validity_restrictions['time_start_and_end']
	ning start_validity
	cating START_VALIDITY_AA
	ning end_validity
indicating END_VALIDITY_AA >=START_VALIDITY_AA and containing signer_info	
containin	
	ncing the trusted certificate
	taining validity_restrictions['time_end']
	ontaining values_restrictions[ time_end ]
indicating value > END_VALIDITY_AA	
or containing validity_restrictions['time_start_and_end']	
	ontaining start_validity
	indicating value <= START_VALIDITY_AA
and containing end_validity	
indicating value > END_VALIDITY_AA	
or c	ontaining validity_restrictions['time_start_and_duration']
	ontaining start_validity
-	indicating X_START_VALIDITY <= START_VALIDITY_AA
а	nd containing duration
	indicating value > END_VALIDITY_AA - X_START_VALIDITY

## 5.2.7.12.8 Check the AA certificate time\_start\_and\_end validity restriction

## 5.2.7.13 AT certificate profile

TP ld	TP_SEC_ITSS_SND_CERT_AT_01_01_BV
Summary	Check that the subject_type of the AT certificate is set to 'authorization_ticket'
Reference	ETSI TS 103 097 [1], clause 7.4.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	9 'authorized' state
the IUT being reque	ested to include certificate in the next CAM
ensure that	
when	
the IUT is reques	sted to send a CAM
then	
the IUT sends a	SecuredMessage
containing hea	ider_fields['signer_info'].signer
containing t	ype
	'certificate'
and containing certificate	
	g subject_info.subject_type
	ng 'authorization_ticket'

### 5.2.7.13.1 Check AT certificate subject type

### 5.2.7.13.2 Check AT certificate subject name

TP Id	TP SEC ITSS SND CERT AT 02 01 BV
	Check that the subject_name variable-length vector is empty for AT certificates
eference ETSI TS 103 097 [1], clause 7.4.2	
	PICS GN SECURITY
	Expected behaviour
with	•
the IUT being in the 'auth	orized' state
0	to include certificate in the next CAM
ensure that	
when	
the IUT is requested to	send a CAM
then	
the IUT sends a Secur	edMessage
	elds['signer_info'].signer
containing type	
indicating 'certificate'	
and containing certificate	
containing subject_info.subject_name	
indicating length = 0	

TP ld	TP_SEC_ITSS_SND_CERT_AT_03_01_BV
Summary	Check that signer_info type of AT certificates is set to 'certificate_digest_with_sha256'
Reference	ETSI TS 103 097 [1], clause 7.4.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
the IUT being reque	ested to include certificate in the next CAM
ensure that	
when	
the IUT is reques	sted to send a CAM
then	
the IUT sends a	SecuredMessage
containing hea	ader_fields['signer_info'].signer
containing t	уре
indicating	g 'certificate'
and contain	ing certificate
containing signer_info.	
contair	ning type
indic	cating 'certificate_digest_with_sha256'

### 5.2.7.13.3 Check that signer info of AT certificate is a digest

### 5.2.7.13.4 Check AT ceretificate subject attributes presence and order

TP ld	TP_SEC_ITSS_SND_CERT_AT_04_01_BV	
Summary	Check that subject attributes are present and arranged in ascending order	
Reference	ETSI TS 103 097 [1], clauses 7.4.1 and 7.4.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'author	orized' state	
the IUT being requested t	o include certificate in the next CAM	
ensure that		
when		
the IUT is requested to	send a CAM	
then		
the IUT sends a Secure		
	elds['signer_info'].signer	
containing type		
indicating 'certificate'		
containing certificate		
containing subject_attributes [0N]		
indicating subject_attributes[n].type		
< subject_attributes[n+1].type		
	containing subject_attributes['verification_key']	
	ibject_attributes['assurance_level']	
containing su	ibject_attributes['its_aid_ssp_list']	

TP Id	TP_SEC_ITSS_SND_CERT_AT_05_01_BV
	Check that time_start_and_end is included in the AT certificate validation restrictions;
	Check that time_start_and_end is included in the AT certificate time restrictions,
Summary	Check that validity restriction of AT certificate is inside the validity restriction of its issuing
	certificate
Reference	ETSI TS 103 097 [1], clause 7.4.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'aut	
the IUT being requested	to include certificate chain in the next CAM
ensure that	
when	
the IUT is requested t	to send a CAM
then	
the IUT sends a Secu	
	_fields['signer_info'].signer
containing type	····
indicating cert	
containing certifi	
	pject_info.subject_type
	authorization_ticket' g validity_restrictions['time_end']
	ntaining validity_restrictions['time_start_and_duration']
	g validity_restrictions['time_start_and_end']
	start_validity
	g START_VALIDITY_AT
	end_validity
	g END_VALIDITY_AT
containing certifi	
	idity_restrictions['time_end']
	end_validity
	g value > END_VALIDITY_AT
or containing	validity_restrictions['time_start_and_end']
containing	start_validity
indicating	g value <= START_VALIDITY_AT
	ning end_validity
	g value > END_VALIDITY_AT
	validity_restrictions['time_start_and_duration']
	start_validity
	g X_START_VALIDITY <= START_VALIDITY_AT
indicating	g value > END_VALIDITY_AT - X_START_VALIDITY

51

## 5.2.7.13.5 Check presence of time\_start\_and\_end validity restriction

TP ld	TP_SEC_ITSS_SND_CERT_AT_07_01_BV	
	Check that all AIDs containing in the its_aid_ssp_list in AT certificate are unique;	
Summary	Check that all AIDs containing in the its_aid_ssp_list in AT certificate are also containing in	
	the its_aid_list in the correspondent AA certificate;	
	Check that the length of SSP of each AID is 31 octets maximum	
Reference		
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'aut		
	to include certificate chain in the next CAM	
ensure that		
when		
the IUT is requested t	o send a CAM	
then		
	the IUT sends a SecuredMessage	
	fields['signer_info'].signer	
0.11	containing type indicating certificate_chain	
containing certific		
	oject_info.subject_type	
	authorization_authority'	
and containing subject_attributes['its_aid_list'] containing its_aid_list[0N]		
indicating ITS_AID_LIST_AA		
and containing certificates[last]		
containing subject_info.subject_type		
indicating 'authorization_ticket'		
and containing subject_attributes['its_aid_ssp_list']		
containing it	ts_aid_ssp_list[0N]	
containing its_aid_ssp_list[n]		
contair	ning its_aid	
	cating unique value containing in the ITS_AID_LIST_AA	
	ntaining service_specific_permissions	
indic	cating length <= 31 octet	

52

#### 5.2.7.13.6 Check ITS-AID-SSP

TP ld	TP_SEC_ITSS_SND_CERT_AT_08_01_BV
Summary	Check that AT certificate is signed by AA cert
Reference ETSI TS 103 097 [1], clause 6.3	
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'aut	horized' state
	to include certificate chain in the next CAM
ensure that	
when	
the IUT is requested t	o send a CAM
then	
the IUT sends a Secu	5
	fields['signer_info'].signer
containing type indicating cert	ificato, chain
	cates[last-1] (CERT_AA)
	oject_info.subject_type
	uthorization_authority'
	g subject_attributes['verification key'] (KEY)
containing certifi	
	pject_info.subject_type
indicating 'a	uthorization_ticket
and containing	g signer_info
containing t	
	g 'certificate_digest_with_ecdsap256'
and contain	
	ng to CERT_AA
and containing	
verifiable us	

## 5.2.7.13.7 Check that AT certificate is signed by AA cert

### 5.2.7.13.8 Check validity restriction presence and order

TP ld	TP_SEC_ITSS_SND_CERT_AT_10_01_BV
Summary	Check that all necessary validity restrictions are present and arranged in ascending order
Reference	ETSI TS 103 097 [1], clause 6.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
the IUT being reque	ested to include certificate in the next CAM
ensure that	
when	
the IUT is reques	sted to send a CAM
then	
the IUT sends a	SecuredMessage
	ader_fields['signer_info'].signer
containing t	
	l'certificate'
containing c	
containin	g validity_restrictions
	ing validity_restrictions[n].type < validity_restrictions[n+1].type
	ntaining validity_restrictions['time_start_and_end']
	t containing validity_restrictions['time_end']
and no	t containing validity_restrictions['time_start_and_duration']

# 5.3 Receiver behaviour

## 5.3.1 Overview

All test purposes of receiving behaviour are considered optional.

## 5.3.2 CAM Profile

## 5.3.2.1 Check that IUT accepts well-formed Secured CAM

TP ld	TP_SEC_ITSS_RCV_CAM_01_01_BV
Summary	Check that IUT accepts a well-formed Secured CAM containing certificate in signer_info
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'aut	horized' state
	e is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receiving a	SecuredMessage
containing protocol	
indicating value	2'
and containing hea	
containing type	
indicating 'sigr	ner info'
and containing s	
containing typ	
indicating 'c	
	g certificate (CERT_TS_A_AT)
	subject_info.subject_type
	g 'authorization_ticket'
and contain	ing subject_attributes['verification key'] (KEY)
and containing hea	
containing type	
indicating 'ger	neration_time'
and containing g	eneration_time
indicating CUI	RRENT_TIME
and containing hea	der_fields[2]
containing type	
indicating 'its_	
and containing it	s_aid
indicating 'AID	
and containing pay	load_field
containing type	
indicating 'sigr	
and containing d	
indicating leng	
containing CA	
and containing trail	
containing trailer	
containing typ	
indicating 's	
containing sig	
verifiable us	Sing KEY
then	
the IUT accepts the m	nessage
	efined in this test purpose is used in the subsequent test purposes with the snippet name
	V_CAM_01'. Only differences to this snippet are mentioned in subsequent test purposes.

TP ld	TP_SEC_ITSS_RCV_CAM_01_02_BV
Summary	Check that IUT accepts a well-formed Secured CAM containing certificate digest of the know
Summary	certificate in signer_info
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'au	uthorized' state
and the IUT current tim	ne is inside the time validity period of CERT_TS_A_AT
and the IUT already re	ceived a Secured message containing certificate (CERT_TS_A_AT)
containing subject_i	nfo.subject_type
indicating 'authori	zation_ticket
	ect_attributes['verification key'] (KEY)
ensure that	
when	
the IUT is receiving	a SecuredMessage
containing protoc	
indicating value	
and containing he	
containing type	
indicating 'si	
and containing	
containing ty	•
	/certificate_digest_with_sha256'
and containin	
	g to certificate (CERT_TS_A_AT)
and containing he	
containing type	
	eneration_time'
	generation_time
	JRRENT_TIME
and containing he	
containing type	
indicating 'its	
and containing	
indicating 'Al	
and containing pa	
containing type	
indicating 'si	
and containing	
indicating ler	
containing C	
and containing trait	
containing traile	
containing ty	
	'signature'
containing si	
	using KEY
then	maaaaa
the IUT accepts the	
	defined in this test purpose is used in the subsequent test purposes with the snippet name
	CV_CAM_02'. Only differences to this snippet are mentioned in subsequent test purposes.

	TP_SEC_ITSS_RCV_CAM_01_03_BV Check that IUT accepts a well-formed Secured CAM containing certificate chain in signer_info
-	Check that for accepts a weil-formed Secured CAW containing certificate chain in signer line
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'aut	
	e is inside the time validity period of CERT_TS_A_AT
ensure that when	
the IUT is receiving a	SecuredMessage
containing protocol	
indicating value	
and containing hea	der_fields[0]
containing type	
indicating 'sigr	
and containing s containing typ	
	e :ertificate_chain'
and containing	
	certificates[0] (CERT_TS_A_AA)
	g subject_info.subject_type
	ing 'authorization_authority'
	aining subject_attributes['verification key'] (KEY_TS_AA)
	ing certificates[1] (CERT_TS_A_AT)
	g subject_info.subject_type ing 'authorization_ticket'
	aining signer_info
	ning type
	cating 'certificate_digest_with_sha256'
	ontaining digest
	rencing to the CERT_TS_A_AA
	aining signature
	ble using KEY_TS_AA aining subject_attributes['verification key'] (KEY_TS_AT)
and containing hea	
containing type	
indicating 'ger	neration_time'
and containing g	
indicating CUI	
and containing hea	der_fields[2]
containing type	aid
indicating 'its_ and containing it	diu s aid
indicating 'AID	
and containing pay	
containing type	
indicating 'sigr	
and containing d	
indicating leng	
containing CA and containing trail	
containing trailer	
containing typ	
indicating 's	
and containing	g signature
	sing KEY_TC_AT
then	
the IUT accepts the m	
	efined in this test purpose is used in the subsequent test purposes with the snippet name V_CAM_03'. Only differences to this snippet are mentioned in subsequent test purposes.

## 5.3.2.2 Check the message protocol version

TP ld	TP_SEC_ITSS_RCV_CAM_02_01_BO
	Check that IUT discards a Secured CAM containing protocol version set to a value less than
Summary	2
Reference	ETSI TS 103 097 [1], clause 5.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
and the IUT current	t time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receive	ing a SecuredMessage (MSG_SEC_RCV_CAM_01)
containing pro	tocol_version
indicating 1	
then	
the IUT discards	a SecuredMessage

TP ld	TP_SEC_ITSS_RCV_CAM_02_02_BO
C	Check that IUT discards a Secured CAM containing protocol version set to a value greater
Summary	than 2
Reference	ETSI TS 103 097 [1], clause 5.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'au	
	e is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
	a SecuredMessage (MSG_SEC_RCV_CAM_01)
containing protoco	ol_version
indicating 3	
then	
the IUT discards a S	ecuredMessage

## 5.3.2.3 Check header fields

TP ld	TP SEC ITSS RCV CAM 04 01 BO
_	Check that IUT discards a secured CAM if the header_fields contains more than header field
Summary	'signer_info'
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'aut	horized' state
and the IUT current time	e is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
•	SecuredMessage (MSG_SEC_RCV_CAM_01)
containing header_	
indicating 'signer	
and containing hea	
indicating 'signer	
and containing hea	
indicating 'gener	
and containing hea	• • • •
indicating 'its_aid	other header fields
then	
the IUT discards a Se	ouredMessage
	oureumessage

TP ld	TP_SEC_ITSS_RCV_CAM_04_02_BO
Summony	Check that IUT discards a secured CAM if the header_fields does not contain the header
Summary	'signer_info'
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivi	ng a SecuredMessage (MSG_SEC_RCV_CAM_01)
containing hea	der_fields[0].type
indicating 'g	eneration_time'
and containing	header_fields[1].type
indicating 'it	s_aid'
and not contai	ning other header fields
then	
the IUT discards	a SecuredMessage

TP ld	TP_SEC_ITSS_RCV_CAM_04_03_BO
Summary	Check that IUT is able to receive a secured CAM where the header fields 'signer_info' is not
	encoded first
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
and the IUT is send	
ensure that	
when	
the IUT is receivi	ng a SecuredMessage (MSG_SEC_RCV_CAM_01)
	der_fields[0].type
	eneration_time'
0.0	header_fields[1].type
indicating 'its	
5	header_fields[2].type
indicating 'si	• • • •
	ning other header fields
then	
the IUT discards	the SecuredMessage

TP ld	TP_SEC_ITSS_RCV_CAM_04_04_BO
	Check that IUT discards a secured CAM if the header fields contains more than one header
Summary	field 'generation' time'
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS GN SECURITY
	Expected behaviour
with	· · · · · · · · · · · · · · · · · · ·
the IUT being in the 'aut	horized' state
and the IUT current time	e is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receiving a	SecuredMessage (MSG_SEC_RCV_CAM_01)
containing header_	fields[0].type
indicating 'signer	r_info'
and containing hea	ider_fields[1].type
indicating 'gener	ation_time'
and containing hea	ider_fields[2].type
indicating 'gener	ation_time'
and containing hea	ider_fields[3].type
indicating 'its_aid	d'
and not containing	other header fields
then	
the IUT discards a Se	curedMessage

TP ld	TP_SEC_ITSS_RCV_CAM_04_05_BO
Summary	Check that IUT discards a secured CAM if the header_fields does not contain the header
	field 'generation_time'
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivi	ng a SecuredMessage (MSG_SEC_RCV_CAM_01)
containing hea	der_fields[0].type
indicating 's	igner_info'
and containing	header_fields[1].type
indicating 'it	s_aid'
and not contail	ning other header fields
then	
the ILIT discords	a SecuredMessage

TP ld	TP_SEC_ITSS_RCV_CAM_04_06_BO	
Summary	Check that IUT discards a secured CAM if the header_fields contain more than one element	
	of header field 'its_aid'	
Reference	ETSI TS 103 097 [1], clause 7.1	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	authorized' state	
and the IUT current	ime is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
	g a SecuredMessage (MSG_SEC_RCV_CAM_01)	
	ler_fields[0].type	
indicating 'sig		
and containing header_fields[1].type		
indicating 'generation_time'		
	header_fields[2]	
containing type		
indicating 'its_aid'		
and containing its_aid		
indicating 'AID_CAM'		
and containing header_fields[3]		
containing type		
indicating 'its_aid' and containing its_aid		
indicating 'AID_DENM'		
	ing other header fields	
then		
	SecuredMessage	

TP ld	TP_SEC_ITSS_RCV_CAM_04_06a_BO	
Summary	Check that IUT discards a secured CAM if the header_fields does not contain the header	
	field 'its_aid'	
Reference	ETSI TS 103 097 [1], clause 7.1	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	authorized' state	
and the IUT current	time is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
the IUT is receivi	ng a SecuredMessage (MSG_SEC_RCV_CAM_01)	
containing hea	ader_fields[0].type	
indicating 'signer_info'		
and containing header_fields[1].type		
indicating 'generation_time'		
and not containing other header fields		
then		
the ILIT discards	a SecuredMessage	

TP ld	TP_SEC_ITSS_RCV_CAM_04_07_BO	
Summary	Check that IUT discards a secured CAM if the header fields are not in the ascending order	
Sammary	according to the numbering of the enumeration.	
Reference	ETSI TS 103 097 [1], clause 7.1	
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 SecuredMessage (MSG_SEC_RCV_CAM_01)		
containing header_fields[0].type		
indicating 'signer_		
and containing header_fields[1].type		
indicating 'its_aid'		
and containing header_fields[2].type		
indicating 'generation_time'		
and not containing other header fields		
then		
the IUT discards the SecuredMessage		

TP ld	TP_SEC_ITSS_RCV_CAM_04_08_BO	
Summary	Check that IUT discards the Secured CAM containing the header field	
	'generation_time_standard_deviation'.	
Reference	ETSI TS 103 097 [1], clause 7.1	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	'authorized' state	
and the IUT current	time is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
	ng a SecuredMessage (MSG_SEC_RCV_CAM_01)	
	der_fields[0].type	
indicating 's		
and containing header_fields[1]		
containing type		
	'generation_time'	
	ng generation_time	
	GEN_TIME inside the validity period of the signer certificate	
	header_fields[2]	
containing t		
	'generation_time_with_standard_deviation'	
and containing generation_time_with_standard_deviation		
indicating GEN_TIME inside the validity period of the signer certificate		
and containing header_fields[3].type		
indicating 'its_aid' and not containing other header fields		
then	ning other neader neids	
	the SecuredMessage	
the full discards	the Seculativessage	

TP ld	TP_SEC_ITSS_RCV_CAM_04_10_BO		
Summary Check that IUT discards the Secured CAM containing the header field 'expiry_time'			
Reference ETSI TS 103 097 [1], clause 7.1			
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			
	SecuredMessage (MSG_SEC_RCV_CAM_01)		
containing header_f			
	indicating 'signer_info'		
and containing header_fields[1]			
containing type			
indicating 'generation_time' containing generation_time			
indicating CURRENT_TIME and containing header_fields[2]			
containing type			
indicating 'expiration'			
and containing expiry_time			
indicating CURRENT_TIME + 1h			
and containing header_fields[3].type			
indicating 'its_aid'			
and not containing other header fields			
then			
the IUT discards the S	ecuredMessage		

TP ld	TP_SEC_ITSS_RCV_CAM_04_11_BO	
Summary	Check that IUT discards the Secured CAM containing the header field 'generation_location'	
Reference	ETSI TS 103 097 [1], clause 7.1	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'a	nuthorized' state	
and the IUT current tir	ne is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
the IUT is receiving	a SecuredMessage (MSG_SEC_RCV_CAM_01)	
containing heade	er_fields[0]	
containing type	e	
indicating 's	igner_info'	
and containing signer		
containing type		
indicating certificate		
	ing certificate (CERT_TS_B_AT)	
	g validity_restrictions['region']	
containing region (X_CERT_REGION)		
and containing header_fields[1].type		
indicating 'generation_time'		
and containing header_fields[2]		
containing type		
indicating 'generation_location'		
and containing generation_location		
indicating position outside of the validity restriction of X_CERT_REGION		
and containing header_fields[3].type		
indicating 'its_		
	ng other header fields	
then		
the IUT discards the	e Secureamessage	

TP ld	TP_SEC_ITSS_RCV_CAM_04_12_BV		
Summary	Check that IUT accepts the Secured CAM containing additional non-standard HeaderField		
Reference	ETSI TS 103 097 [1], clause 7.1		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT being in the 'auth	orized' state		
and the IUT current time i	s inside the time validity period of CERT_TS_A_AT		
ensure that			
when			
•	SecuredMessage (MSG_SEC_RCV_CAM_01)		
•	containing header_fields[0].type		
indicating 'signer_info'			
and containing head			
indicating 'generation_time'			
and containing header_fields[2].type			
indicating 'its_aid'			
and containing header_fields[3]			
containing type			
indicating non-standard header field type (1000)			
and containing other_header			
indicating non-empty data			
and not containing other header fields			
then	aurad Maaaaaa		
the IUT accepts the SecuredMessage			

TP ld	TP_SEC_ITSS_RCV_CAM_04_13_BO		
	Check that IUT discards the Secured CAM containing the header field		
Summary	'encryption_parameter' and 'recipient_info'		
Reference	ETSI TS 103 097 [1], clause 7.1		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
-	thorized' state with CERT_IUT_A_AT		
	e is inside the time validity period of CERT_TS_A_AT		
ensure that			
when			
the IUT is receiving a	a SecuredMessage (MSG_SEC_RCV_CAM_01)		
containing header			
indicating 'signe			
and containing he			
indicating 'gene			
	ader_fields[2].type		
indicating 'its_a			
and containing header_fields[3]			
containing type	cryption_parameters'		
	and containing enc_params containing symm_algorithm		
	aes_128_ccm'		
and containing nonce			
and containing header_fields[4]			
containing type			
	indicating 'recipient_info'		
and containing recipients			
containing recipients[0]			
containing cert_id			
referencing to CERT_IUT_A_AT			
and containing pk_encryption			
indicating 'ecies_nistp256'			
and containing enc_key			
then	and not containing other header fields		
the IUT discards the	SecuredMessage		
	Coourodinosodago		

# 5.3.2.4 Check signer info

TP ld	TP SEC ITSS RCV CAM 05 01 BO
	Check that IUT discards a secured CAM if the header_fields contains a signer of type 'self'
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
ensure that when	s inside the time validity period of CERT_TS_A_AT SecuredMessage (MSG_SEC_RCV_CAM_01) elds['signer_info'] type

TP ld	TP_SEC_ITSS_RCV_CAM_05_02_BO		
C	Check that IUT discards a secured CAM if the header_fields contains a signer of type		
Summary	certificate_digest_with_other_algorithm		
Reference	ETSI TS 103 097 [1], clause 7.1		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT being in the			
and the IUT current	and the IUT current time is inside the time validity period of CERT_TS_A_AT		
ensure that	ensure that		
when			
the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_02)			
containing header_fields['signer_info']			
containing signer.type			
indicating 'certificate_digest_with_other_algorithm'			
then			
the IUT discards a SecuredMessage			

TP Id	TP SEC ITSS RCV CAM 05 03 BO		
Summary	Check that IUT discards a secured CAM if the header fields contains a signer of type		
	certificate_chain and the chain is empty		
Reference	ETSI TS 103 097 [1], clause 7.1		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with	·		
the IUT being in the 'aut	horized' state		
	e is inside the time validity period of CERT_TS_A_AT		
ensure that			
when			
	the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_03)		
5	_fields['signer_info']		
containing signe			
containing type			
	indicating 'certificate_chain'		
and containing certificates			
indicating length = $0$			
then	angur – v		
	nourad Magaaga		
the IUT discards a Se	scureamessage		

TP ld	TP_SEC_ITSS_RCV_CAM_05_04_BO		
Summany	Check that IUT discards a secured CAM if the header_fields contains a signer of type		
Summary	certificate_chain and the chain contains only one certificate		
Reference	ETSI TS 103 097 [1], clause 7.1		
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 SecuredMessage (MSG_SEC_RCV_CAM_03))			
containing header_fields['signer_info']			
containing signer			
containing type			
indicating certificate_chain			
and containing certificates			
indicating length = 1			
then	-		
the IUT discards a Sec	uredMessage		

TP ld	TP_SEC_ITSS_RCV_CAM_05_05_BO
Cummon v	Check that IUT discards a secured CAM if the header_fields contains a signer info of
Summary	unknown or reserved type
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
and the IUT current	t time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivi	ng a SecuredMessage (MSG_SEC_RCV_CAM_02)
containing hea	ader_fields['signer_info']
containing s	
indicating	X_UNKNOWN_SIGNERINFO_TYPE
then	
the IUT discards	a SecuredMessage

TP ld	TP_SEC_ITSS_RCV_CAM_06_01_BO
Summary	Check that IUT discards message containing generation_time before the certificate validity
Summary	period.
Reference	ETSI TS 103 097 [1], clauses 5.4 and 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivi	ng a SecuredMessage (MSG_SEC_RCV_CAM_01)
	der_fields['signer_info'].signer
	ertificate (CERT_TS_MSG_06_01_BO_AT)
	g validity_restrictions['time_start_and_end']
	ing start_validity
	ating START_VALIDITY_AT
	ntaining end_validity
	ating END_VALIDITY_AT
	header_fields ['generation_time']
	eneration_time
•	GEN_TIME < START_VALIDITY_AT
then	
the IUT discards	the message

# 5.3.2.5 Check generation time

TP ld	TP_SEC_ITSS_RCV_CAM_06_02_BO
Summany	Check that IUT discards message containing generation_time after the certificate validity
Summary	period.
Reference	ETSI TS 103 097 [1], clauses 5.4 and 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	authorized' state
and the IUT current t	ime is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
	g a SecuredMessage (MSG_SEC_RCV_CAM_01)
	er_fields['signer_info'].signer
	rtificate (CERT_TS_MSG_06_02_BO_AT)
	validity_restrictions['time_start_and_end']
	ng start_validity
	ting START_VALIDITY_AT
	taining end_validity
	ting END_VALIDITY_AT
	neader_fields ['generation_time']
•	GEN_TIME > END_VALIDITY_AT
then	
the IUT discards the	ne message

## 5.3.2.6 Check its\_aid

TP ld	TP_SEC_ITSS_RCV_CAM_07_01_BO
Summary	Check that IUT discards secured CAM when its_aid value is defined but not the AID_CAM
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	authorized' state
	ime is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivin	g a SecuredMessage (MSG_SEC_RCV_CAM_01)
containing head	er_fields['its_aid']
indicating 'Al	D DENM'
and containing	
containing ty	
indicating	signed'
and containin	
	ČAM payload
then	
به مانت مانت ماند ماند ماند	ne message

TP ld	TP_SEC_ITSS_RCV_CAM_07_02_BO
Summary	Check that IUT discards secured CAM when its_aid value is undefined
Reference	ETSI TS 103 097 [1], clause 7.1
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 S	SecuredMessage (MSG_SEC_RCV_CAM_01)
containing header_fi	
indicating 'AID_UI	
and containing paylo	pad_field
containing type	
indicating 'signed'	
and containing da	
containing CAN	/l payload
then	
the IUT discards the m	essage

## 5.3.2.7 Check payload

TP ld	TP_SEC_ITSS_RCV_CAM_09_02_BO
Summary	Check that IUT discards the Secured CAM containing empty payload of type 'signed'
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivi	ng a SecuredMessage (MSG_SEC_RCV_CAM_01)
containing pay	load_field
containing t	уре
indicating	'signed'
and contain	ing data
indicating	length 0
then	
the IUT discards	

TP ld	TP_SEC_ITSS_RCV_CAM_09_03_BO
Summory	Check that IUT discards the Secured CAM containing non-empty payload of type
Summary	'unsecured'
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'aut	norized' state
and the IUT current time	is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
	SecuredMessage (MSG_SEC_RCV_CAM_01)
containing payload	field
containing type	
indicating 'uns	
and containing d	
indicating leng	th > 0
then	
the IUT discards the n	nessage

TP ld	TP_SEC_ITSS_RCV_CAM_09_04_BO
Summary	Check that IUT discards the Secured CAM containing non-empty payload of type 'encrypted'
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivin	g a SecuredMessage (MSG_SEC_RCV_CAM_01)
containing payle	bad field
containing ty	
indicating	encrypted'
and containin	ng data
indicating	
then	•
the IUT discards t	he message

TP ld	TP_SEC_ITSS_RCV_CAM_09_05_BO
C	Check that IUT discards the Secured CAM containing non-empty payload of type
Summary	'signed_external'
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	a 'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivi	ng a SecuredMessage (MSG_SEC_RCV_CAM_01)
containing pay	rload_field
containing t	уре
indicating	, 'signed_external'
and contain	ing data
indicating	length > 0
then	
the IUT discards	the message

TP ld	TP_SEC_ITSS_RCV_CAM_09_06_BO
	Check that IUT discards the Secured CAM containing non-empty payload of type
Summary	'signed and encrypted'
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'aut	horized' state
and the IUT current time	is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
	SecuredMessage (MSG_SEC_RCV_CAM_01)
containing payload	_field
containing type	
indicating 'sigr	ned_and_encrypted'
and containing d	ata
indicating leng	th > 0
then	
the IUT discards the r	nessage

TP ld	TP_SEC_ITSS_RCV_CAM_09_07_BO
Summary	Check that IUT discards the Secured CAM containing non-empty payload of unknown type
Reference	ETSI TS 103 097 [1], clause 7.1
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 S	SecuredMessage (MSG_SEC_RCV_CAM_01)
containing payload_f	field
containing type	
indicating X_UN	NKNOWN_PAYLOAD_TYPE
and containing da	
indicating lengt	h > 0
then	
the IUT discards the m	essage
NOTE: Proposed values	to be used as X_UNKNOWN_PAYLOAD_TYPE are 5 and 255.
· · · · · · · · · · · · · · · · · · ·	

TP ld	TP_SEC_ITSS_RCV_CAM_10_01_BO
0	Check that IUT discards the Secured CAM if the message does not contain the trailer field
Summary	of type 'signature'
Reference	ETSI TS 103 097 [1], clause 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
and the IUT curren	t time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receiv	ing a SecuredMessage (MSG_SEC_RCV_CAM_01)
containing tra	iler_fields
not contain	ing any instance of type TrailerField
containin	ig type
indicat	ting 'signature'
then	
ulen	

## 5.3.2.8 Check presence of trailer field

TP ld	TP_SEC_ITSS_RCV_CAM_10_02_BO		
0	Check that IUT discards the Secured CAM containing more than one instance of TrailerField		
Summary	of type 'signature'		
Reference	ETSI TS 103 097 [1], clause 7.1		
PICS Selection	PICS_GN_SECURITY		
Expected behaviour			
with			
the IUT being in the 'au	horized' state		
and the IUT current time	e is inside the time validity period of CERT_TS_A_AT		
ensure that			
when			
the IUT is receiving a	SecuredMessage (MSG_SEC_RCV_CAM_01)		
containing trailer_f	ields[0]		
containing type			
indicating signature			
and containing trailer_fields[1]			
containing type			
indicating signature			
then			
the IUT discards the message			

## 5.3.2.9 Check signature

TP ld	TP_SEC_ITSS_RCV_CAM_11_01_BO
Summary	Check that the IUT discards Secured message containing signature that is not verified using
	the verification key from the certificate contained in the message's signer info
Reference	ETSI TS 103 097 [1], clauses 4.2.2 and 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivir	ng a SecuredMessage (MSG_SEC_RCV_CAM_01)
containing hea	der_fields ['signer_info'].signer
containing ce	ertificate
containing	g subject_attributes['verification key']
	ing key (KEY)
	trailer_fields[0]
containing ty	
•	'signature'
and containing	
	iable using KEY
then	
the IUT discards t	he message

	TP_SEC_ITSS_RCV_CAM_11_02_BO	
	Check that the IUT discards Secured message containing signature that is not verified using	
Summary	the verification key from the certificate, referenced by the digest contained in the message's	
	signer info	
Reference	ETSI TS 103 097 [1], clauses 4.2.2 and 7.1	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'au	Ithorized' state	
	e is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
•	a SecuredMessage (MSG_SEC_RCV_CAM_02)	
	_fields ['signer_info'].signer	
containing dige		
6	o the certificate (CERT_TS_A_AT)	
	subject_attributes['verification key']	
	ng key (KEY) itar fielde[0]	
and containing tra containing type	••	
indicating 'sig		
and containing signature NOT verifiable using KEY		
then		
the IUT discards the	message	

TP ld	TP_SEC_ITSS_RCV_CAM_11_03_BO
Summary	Check that IUT discards the Secured CAM if the message contains trailer field of type
	signature' with reserved public key algorythms
Reference	ETSI TS 103 097 [1], clauses 4.2.2 and 7.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivi	ng a SecuredMessage (MSG_SEC_RCV_CAM_01)
containing trail	
	n instance of type TrailerField
containing	
indicati	ng 'signature'
	aining signature.algorithm
	ng X_RESERVED_PK_ALGORYTHM
then	<u> </u>
the IUT discards	the message
	e provided as X_RESERVED_PK_ALGORYTHM are: 240, 255.

# 5.3.2.10 Check signing certificate type

TP ld	TP SEC ITSS RCV CAM 12 01 BO	
Summary	Check that IUT discards a Secured CAM if the signer certificate of the message contains the	
	subject type 'enrolment_credential'	
Reference	ETSI TS 103 097 [1], clause 6.3	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'a	nuthorized' state	
and the IUT current til	me is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
	a SecuredMessage (MSG_SEC_RCV_CAM_01)	
containing header_fields ['signer_info']		
containing signer		
containing t		
	'certificate'	
	certificate (CERT_TS_A_EC)	
containing subject_info.subject_type		
	ing 'enrolment_credentials'	
then		
the IUT discards the message		

TP ld	TP_SEC_ITSS_RCV_CAM_12_02_BO		
Summary	Check that IUT discards a Secured CAM if the signer certificate of the message contains the		
Summary	subject type 'authorization_authority'		
Reference	ETSI TS 103 097 [1], clause 6.3		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT being in the	'authorized' state		
and the IUT current	time is inside the time validity period of CERT_TS_A_AT		
ensure that			
when			
the IUT is receiving	ng a SecuredMessage (MSG_SEC_RCV_CAM_01)		
containing hea	der_fields ['signer_info']		
containing signer			
containing	containing type		
indicati	indicating 'certificate'		
containing certificate (CERT_TS_A_AA)			
containing subject_info.subject_type			
indicating 'authorization_authority'			
then			
the IUT discards the message			

TP ld	TP_SEC_ITSS_RCV_CAM_12_03_BO		
Summary	Check that IUT discards a Secured CAM if the signer certificate of the message contains the		
	subject type 'enrolment_authority'		
Reference	ETSI TS 103 097 [1], clause 6.3		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT being in the	a 'authorized' state		
and the IUT current	time is inside the time validity period of CERT_TS_A_AT		
ensure that			
when	when		
	ng a SecuredMessage (MSG_SEC_RCV_CAM_01)		
	ider_fields ['signer_info']		
containing signer			
	containing type		
indicat	indicating 'certificate'		
containing certificate (CERT_TS_A_EA)			
containing subject_info.subject_type			
indicating 'enrolment_authority'			
then			
the IUT discards	the IUT discards the message		

TP ld	TP_SEC_ITSS_RCV_CAM_12_04_BO		
Summary	Check that IUT discards a Secured CAM if the signer certificate of the message contains the		
Summary	subject type 'root_ca'		
Reference	ETSI TS 103 097 [1], clause 6.3		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT being in the 'a	uthorized' state		
and the IUT current tim	and the IUT current time is inside the time validity period of CERT_TS_A_AT		
ensure that			
when			
the IUT is receiving	the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)		
containing heade	containing header_fields ['signer_info']		
containing signer			
containing ty	containing type		
indicating 'certificate'			
containing certificate (CERT_TS_ROOT)			
containing subject_info.subject_type			
indicating 'root_ca'			
then			
the IUT discards the	message		

# 5.3.2.11 Check certificate validity

TP ld	TP SEC ITSS RCV CAM 13 01 BO	
-		
Summary Check that IUT discards secured CAM signed with the not yet valid certificate		
eference ETSI TS 103 097 [1], clause 6.1		
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'auth	orized' state	
and the IUT current time	is before the time validity period of CERT_TS_MSG_13_01_BO_AT	
ensure that		
when		
the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)		
containing header_fields['signer_info'].signer		
containing certificate (CERT_TS_MSG_13_01_BO_AT)		
containing validity_restrictions['time_start_and_end']		
containing start_validity		
indicating START_VALIDITY_AT > CURRENT_TIME		
and containing end_validity		
indicating END_VALIDITY_AT > START_VALIDITY_AT		
then		
the IUT discards the message		

TP ld	TP_SEC_ITSS_RCV_CAM_13_02_BO	
Summary	Check that IUT discards secured CAM signed with the expired certificate	
Reference	ETSI TS 103 097 [1], clause 6.1	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the		
and the IUT current	time is before the time validity period of CERT_TS_MSG_13_02_BO_AT	
ensure that		
when		
	ng a SecuredMessage (MSG_SEC_RCV_CAM_01)	
	der_fields['signer_info'].signer	
	ertificate (CERT_TS_MSG_13_02_BO_AT)	
	g validity_restrictions['time_start_and_end']	
	ing start_validity	
	ating START_VALIDITY_AT < CURRENT_TIME	
	ntaining end_validity	
	ating END_VALIDITY_AT < CURRENT_TIME	
then		
the IUT discards	ine message	
TP ld	TP_SEC_ITSS_RCV_CAM_13_03_BO	
Summan.	Check that IUT discards secured CAM when IUT location is outside the circular validity	
Summary	restriction of the signing certificate	
Reference	ETSI TS 103 097 [1], clause 6.1	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'authorized' state and the IUT current time is inside the validity period of CERT_TS_MSG_13_03_BO_AT		
ensure that		
when		
	ng a SecuredMessage (MSG_SEC_RCV_CAM_01)	

the forms receiving a Securedivessage (MSG_SEC_RCV_CAM_01)
containing header_fields['signer_info'].signer
containing certificate (CERT_TS_MSG_13_03_BO_AT)
containing validity_restrictions['region']
containing region
containing region_type
indicating 'circle'
and containing circular_region
indicating RECION

indicating REGION not containing the CURRENT\_IUT\_LOCATION

then

the IUT discards the message

TP ld	TP_SEC_ITSS_RCV_CAM_13_04_BO	
<b>6</b>	Check that IUT discards secured CAM when IUT location is outside the rectangular validity	
Summary	restriction of the signing certificate	
Reference	ETSI TS 103 097 [1], clause 6.1	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	e 'authorized' state	
and the IUT current time is inside the validity period of CERT_TS_MSG_13_04_BO_AT		
and the IUT current location is set to CURRENT_IUT_LOCATION		
ensure that		
when		
the IUT is receiv	ing a SecuredMessage (MSG_SEC_RCV_CAM_01)	
containing header_fields['signer_info'].signer		
containing certificate (CERT_TS_MSG_13_04_BO_AT)		
containing validity_restrictions['region']		
containing region		
con	taining region_type	
ir	ndicating 'rectangle'	
and containing rectangular_regions		
indicating REGION		
	not containing the CURRENT_IUT_LOCATION	
4		

then

the IUT discards the message

TP Id TP_SEC_ITSS_RCV_CAM_13_05_BO		
Summary	Check that IUT discards secured CAM when IUT location is outside the polygonal validity	
	restriction of the signing certificate	
Reference ETSI TS 103 097 [1], clause 6.1		
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	'authorized' state	
and the IUT current time is inside the validity period of CERT_TS_MSG_13_05_BO_AT		
and the IUT current location is set to CURRENT_IUT_LOCATION		
ensure that		
when		
the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)		
containing header_fields['signer_info'].signer		
	ertificate (CERT_TS_MSG_13_05_BO_AT)	
	validity_restrictions['region']	
	ng region	
	ining region_type	
indicating 'polygon'		
	containing polygonal_region	
indicating REGION		
	not containing the CURRENT_IUT_LOCATION	
then	ha maaaaaa	
the IUT discards t	ne message	

TP ld	TP_SEC_ITSS_RCV_CAM_13_06_BO		
Summary	Check that IUT discards secured CAM when IUT location is outside the identified validity		
Summary	restriction of the signing certificate		
eference ETSI TS 103 097 [1], clause 6.1			
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT being in the 'auth			
and the IUT current time	and the IUT current time is inside the validity period of CERT_TS_MSG_13_06_BO_AT		
and the IUT current loca	and the IUT current location is set to CURRENT_IUT_LOCATION		
ensure that			
when			
the IUT is receiving a SecuredMessage (MSG_SEC_RCV_CAM_01)			
5	containing header_fields['signer_info'].signer		
	containing certificate (CERT_TS_MSG_13_06_BO_AT)		
containing validity_restrictions['region']			
•	containing region		
	containing region_type		
indicating 'id'			
and containing id_region			
	indicating REGION		
not containing the CURRENT_IUT_LOCATION			
then			
the IUT discards the message			

#### 5.3.3 DENM Profile

### 5.3.3.1 Check that IUT accepts well-formed Secured DENM

ſP ld	TP_SEC_ITSS_RCV_DENM_01_01_BV	
Summary Check that IUT accepts a well-formed Secured DENM signed with the certific		
summary	region validity restriction	
Reference	ETSI TS 103 097 [1], clause 7.2	
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 S	SecuredMessage	
containing header_fi	elds[0]	
containing type		
indicating 'signe	er_info'	
and containing sig	iner	
containing type		
indicating 'ce	urtificate'	
	certificate (CERT_TS_A_AT)	
containing su	ubject_info.subject_type	
	'authorization_ticket'	
	ng subject_attributes['verification key']	
	key (KEY)	
	aining validity_restrictions['region']	
and containing head		
containing type		
indicating 'generation_time'		
and containing generation_time		
indicating CURRENT_TIME		
and containing header_fields [2]		
containing type		
indicating 'gene	aration location'	
and containing ge		
and containing head		
containing type		
indicating 'its_aid'		
and containing its_aid		
indicating 'AID_		
and containing paylo		
containing type		
indicating 'signe	ed'	
and containing da		
indicating length > 0		
and containing DENM payload		
and containing being payload and containing being barbad		
containing single instance of type TrailerField		
containing type		
indicating 'signature'		
and containing signature		
verifiable using KEY		
then	······································	
the IUT accepts the me	906224	
	fined in this test purpose is used in the subsequent test purposes with the snippet name	
NOTE. THE THESSAUE GET	aneo in una teat purpose la useu in the subsequent test purposes with the shippet name	

	TP_SEC_ITSS_RCV_DENM_01_02_BV	
Check that II IT accepts a well-formed Secured DENM signed with the certificate with a		
Summary	circular region validity restriction	
Reference	ETSI TS 103 097 [1], clause 7.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'auth		
	is inside the time validity period of CERT_TS_B_AT	
	tion is inside the region validity period of CERT_TS_B_AT	
ensure that		
when		
the IUT is receiving a		
and containing head		
containing type	ar infal	
indicating 'sign		
and containing si		
containing type		
indicating 'co	ertificate   certificate (CERT_TS_B_AT)	
	ubject_info.subject_type	
	'authorization_ticket'	
	ing subject_attributes['verification key'] (KEY)	
	ing validity_restrictions['region']	
containing		
	ning region_type	
	ating 'circle'	
	ntaining circular_region	
indicating REGION and containing header_fields [1]		
containing type		
indicating 'gen	eration time'	
and containing generation_time		
indicating CURRENT_TIME		
and containing header_fields [2]		
containing type		
	eration_location'	
	eneration_location	
	tion inside the REGION	
and containing header_fields[3]		
containing type		
indicating 'its_aid'		
and containing its		
indicating 'AID		
	any other header_fields	
and containing payload_fields		
containing type		
indicating 'sign		
and containing da		
indicating length $> 0$		
and containing DENM payload		
and containing trailer_fields		
containing single instance of type TrailerField		
containing type		
indicating 'signature' and containing signature		
verifiable us		
then	055200	
the IUT accepts the m		
	efined in this test purpose is used in the subsequent test purposes with the snippet name	
	V_DENM_B'. Only differences to this snippet are mentioned in subsequent test purposes.	

TP ld	TP_SEC_ITSS_RCV_DENM_01_03_BV		
	Check that IUT accepts a well-formed Secured DENM signed with the certificate with a		
Summary	rectangular region validity restriction		
Reference	ETSI TS 103 097 [1], clause 7.2		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT being in the 'author			
	inside the time validity period of CERT_TS_C_AT n is inside the region validity period of CERT_TS_C_AT		
ensure that	TIS Inside the region validity period of CERT_TS_C_AT		
when			
the IUT is receiving a Se	curedMessage		
containing protocol_ve			
indicating value '2'			
and containing header	_fields[0]		
containing type			
indicating 'signer			
and containing sign	er		
containing type	ficatel		
indicating 'certi	ificate ertificate (CERT_TS_C_AT)		
	ject_info.subject_type		
	uthorization_ticket'		
	subject_attributes['verification key'] (KEY)		
	validity_restrictions['region']		
containing re			
	g region_type		
	ng 'rectangle'		
and containing rectangular_regions			
	ng REGIONS		
and containing header	_fields [1]		
containing type			
indicating 'generation_time'			
	and containing generation_time indicating CURRENT_TIME		
and containing header			
containing type			
indicating 'genera	ition location'		
and containing gene			
indicating position	n inside the REGION		
and containing header_fields[3]			
containing type			
indicating 'its_aid			
and containing its_a indicating 'AID_D			
and not containing any			
and containing payloa			
containing type			
indicating 'signed	,		
	and containing data		
indicating length > 0			
and containing DENM payload			
and containing trailer_fields			
	stance of type TrailerField		
containing type	aturo'		
indicating 'sign	aluit anatura		
and containing signature verifiable using KEY			
then			
the IUT accepts the mes	sage		
	ed in this test purpose is used in the subsequent test purposes with the snippet name		
	DENM_C'. Only differences to this snippet are mentioned in subsequent test purposes.		

TP ld	TP_SEC_ITSS_RCV_DENM_01_04_BV	
Check that IUT accepts a well-formed Secured DENM signed with the certificate with a		
Summary	polygonal region validity restriction	
Reference	ETSI TS 103 097 [1], clause 7.2	
PICS Selection	PICS_GN_SECURITY	
14	Expected behaviour	
with		
the IUT being in the 'au	e is inside the time validity period of CERT_TS_D_AT	
	ation is inside the region validity period of CERT_TS_D_AT	
ensure that		
when		
the IUT is receiving a	a SecuredMessage	
containing protoco		
indicating value		
and containing hea	ader_fields[0]	
containing type		
indicating 'sig		
and containing s		
containing typ indicating		
	ig certificate (CERT_TS_D_AT)	
	subject_info.subject_type	
	g 'authorization_ticket'	
	ning subject_attributes['verification key'] (KEY)	
	ning validity_restrictions['region']	
	ng region	
	ining region_type	
	icating 'polygon'	
	ontaining polygonal_region	
and containing hea	icating REGION	
containing type		
	neration_time'	
	generation_time	
and containing hea	ader_fields [2]	
containing type		
	neration_location	
	generation_location	
indicating position inside the REGION		
and containing hea containing type	ader_tields[3]	
indicating 'its	aid'	
and containing i		
indicating 'All		
	any other header_fields	
and containing pay	yload_field	
containing type		
indicating 'sig		
and containing of		
indicating len		
and containing trai	ig DENM payload	
	e instance of type TrailerField	
containing sing		
indicating		
and containin		
verifiable u		
then		
the IUT accepts the r		
	defined in this test purpose is used in the subsequent test purposes with the snippet name	
'MSG_SEC_RO	CV_DENM_D'. Only differences to this snippet are mentioned in subsequent test purposes.	

TP ld	TP_SEC_ITSS_RCV_DENM_01_05_BV		
_	Check that IUT accepts a well-formed Secured DENM signed with the certificate with a		
Summary	identified region validity restriction		
Reference	ETSI TS 103 097 [1], clause 7.2		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT being in the 'auth			
	is inside the time validity period of CERT_TS_E_AT tion is inside the region validity period of CERT_TS_E_AT		
ensure that	ion is inside the region validity period of CERT_TS_E_AT		
when			
the IUT is receiving a	SecuredMessage		
containing protocol_			
indicating value '2			
and containing head	der_fields[0]		
containing type			
indicating 'sign			
and containing sig			
containing type			
indicating 'ce	ertificate certificate (CERT_TS_E_AT)		
	ubject_info.subject_type		
	'authorization_ticket'		
	ng subject_attributes['verification key'] (KEY)		
	ng validity_restrictions['region']		
containing			
contain	ing region_type		
	ating 'id_region'		
	ntaining identified_region		
	ating REGION		
and containing head	der_fields [1]		
containing type	aration time!		
	indicating 'generation_time' and containing generation_time		
indicating CUR			
and containing head			
containing type			
	eration_location'		
	eneration_location		
indicating position inside the REGION			
and containing header_fields[3]			
containing type	- : .0		
indicating 'its_a			
and containing its indicating 'AID			
	any other header_fields		
and containing payle			
containing type			
indicating 'sign	ed'		
and containing da	ata		
indicating lengt			
	DENM payload		
and containing traile			
	instance of type TrailerField		
containing type			
indicating 'si and containing			
verifiable us			
then			
the IUT accepts the m	essage		
	fined in this test purpose is used in the subsequent test purposes with the snippet name		
	V_DENM_E'. Only differences to this snippet are mentioned in subsequent test purposes.		

#### 5.3.3.2 Check the message protocol version

TP ld	TP_SEC_ITSS_RCV_DENM_02_01_BO
Summary	Check that IUT discards a Secured DENM containing protocol version set to a value less
	than 2
Reference	ETSI TS 103 097 [1], clause 5.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	authorized' state
and the IUT current	t time is inside the time validity period of CERT TS A AT
ensure that	
when	
the IUT is receivi	ng a SecuredMessage (MSG_SEC_RCV_DENM_A)
containing pro	
indicating 1	
then	
the IUT discards	a SecuredMessage

#### триа

TP ld	TP_SEC_ITSS_RCV_DENM_02_02_BO	
0	Check that IUT discards a Secured DENM containing protocol version set to a value greater	
Summary	than 2	
Reference	ETSI TS 103 097 [1], clause 5.1	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	e 'authorized' state	
and the IUT current	t time is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
the IUT is received	ing a SecuredMessage (MSG_SEC_RCV_DENM_A)	
containing protocol_version		
indicating 3		
then		
the IUT discards a SecuredMessage		

#### 5.3.3.3 Check header fields

TP ld	TP SEC ITSS RCV DENM 04 01 BO	
Summary	Check that IUT discards a secured DENM if the message contains more than one header	
	field of type 'signer_info'	
Reference ETSI TS 103 097 [1], clause 7.2		
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	'authorized' state	
and the IUT current	time is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
	ng a SecuredMessage (MSG_SEC_RCV_DENM_A)	
	der_fields[0].type	
indicating 'si		
	header_fields[1].type	
indicating 'si		
	header_fields[2].type	
	eneration_time'	
	header_fields[3].type	
	eneration_location'	
and containing header_fields[4].type		
indicating 'its_aid'		
	ning other header fields	
then		
the IUT discards t	the SecuredMessage	

TP ld	TP_SEC_ITSS_RCV_DENM_04_02_BO	
Summary		
	Check that IUT discards a secured DENM if the message does not contain the header field	
-	of type 'signer_info'	
Reference	ETSI TS 103 097 [1], clause 7.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'a	nuthorized' state	
and the IUT current til	me is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
the IUT is receiving	a SecuredMessage (MSG_SEC_RCV_DENM_A)	
containing head		
indicating 'gen		
	eader_fields[1].type	
indicating 'generation_location'		
and containing header_fields[2].type		
indicating 'its_aid'		
and not containing other header fields		
then		
	SourcedMoscogo	
the IUT discards a	Securedinessage	

TP ld	TP_SEC_ITSS_RCV_DENM_04_03_BO
Summary	Check that IUT discards the Secured DENM if the signer_info header field is not encoded first
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
ensure that when the IUT is receivin containing head indicating 'ge and containing indicating 'ge and containing indicating 'its and containing indicating 'sig	ime is inside the time validity period of CERT_TS_A_AT g a SecuredMessage (MSG_SEC_RCV_DENM_A) ler_fields[0].type neration_time' header_fields[1].type neration_location' header_fields[2].type _aid' header_fields[3].type
then	
the IUT discards t	he SecuredMessage

TP ld	TP_SEC_ITSS_RCV_DENM_04_04_BO		
Summary	Check that IUT discards a secured DENM if the message contains more than one header		
Summary	field of type 'generation_time'		
Reference	ETSI TS 103 097 [1], clause 7.2		
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 S	SecuredMessage (MSG_SEC_RCV_DENM_A)		
containing header_fields[0].type			
indicating 'signer_info'			
containing header_fi	ields[1].type		
	indicating 'generation_time'		
and containing header_fields[2].type			
indicating 'generation_time'			
and containing header_fields[3].type			
indicating 'generation_location'			
and containing header_fields[4].type			
indicating 'its_aid'			
and not containing other header fields			
then			
the IUT discards a Sec	uredMessage		

t	he IUT	discards a	Secured	lessage
		aloourao a	Coouroan	loobugo

TP ld	TP_SEC_ITSS_RCV_DENM_04_05_BO		
Summary	Check that IUT discards a secured DENM if the message does not contain the header field		
	of type 'generation_time'		
Reference			
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT being in the '	authorized' state		
and the IUT current ti	ime is inside the time validity period of CERT_TS_A_AT		
ensure that			
when			
the IUT is receiving	g a SecuredMessage (MSG_SEC_RCV_DENM_A)		
containing head	er_fields[0].type		
indicating 'sig	ner info'		
containing head	er_fields[1].type		
	neration_location'		
	neader_fields[2].type		
indicating 'its_aid'			
and not containing other header fields			
then	5		
	SecuredMessage		

TP ld	TP_SEC_ITSS_RCV_DENM_04_06_BO	
	Check that IUT discards a secured DENM if the message contains more than one header	
Summary	field of type 'its_aid'	
Reference	ETSI TS 103 097 [1], clause 7.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'au	ithorized' state	
and the IUT current tim	e is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
the IUT is receiving a	a SecuredMessage (MSG_SEC_RCV_DENM_A)	
containing header		
indicating 'signe		
	ader_fields[1].type	
indicating 'gene		
	ader_fields[2].type	
indicating 'gene		
and containing he		
containing type		
indicating 'its		
containing its_a		
indicating 'Al		
and containing header_fields[4]		
containing type indicating 'its_aid'		
containing its_a		
indicating 'Al		
	g other header fields	
then		
the IUT discards a S	ecuredMessage	

TP ld	TP_SEC_ITSS_RCV_DENM_04_06a_BO
Summary	Check that IUT discards a secured DENM if the message does not contain the header field
	of type 'its_aid'
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'aut	norized' 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	SecuredMessage (MSG_SEC_RCV_DENM_A)
containing header_	
indicating 'signer	
and containing hea	
indicating 'genera	
and containing hea	
indicating 'genera	
and not containing	other header fields
then	
the IUT discards a Se	curedMessage

TP ld	TP_SEC_ITSS_RCV_DENM_04_07_BO
Summary	Check that IUT discards a secured DENM if the message contains more than one header
	field of type 'generation_location'
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
	ng a SecuredMessage (MSG_SEC_RCV_DENM_A)
containing hea	der_fields[0].type
indicating 'si	gner_info'
and containing	header_fields[1].type
	eneration_time'
	header_fields[2]
containing ty	
	'generation_location'
	ng generation_location
	X_LOCATION
	header_fields[3]
containing ty	
	'generation_location'
	ng generation_location
	X_LOCATION
	header_fields[4].type
indicating 'its	
	ning other header fields
then	
the IUT discards	a SecuredMessage

TP ld	TP_SEC_ITSS_RCV_DENM_04_08_BO
	Check that IUT discards a secured DENM if the message does not contain the header field
Summary	•
	of type 'generation_location'
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'a	uthorized' state
and the IUT current tir	ne is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receiving	a SecuredMessage (MSG_SEC_RCV_DENM_A)
containing heade	<b>o</b> ( <b>i</b> = <b>i</b> = <b>i</b> = <b>j</b>
indicating 'sigr	
containing heade	
indicating 'gen	
	eader_fields[2].type
indicating 'its_	
	ng other header fields
then	
the IUT discards a	SecuredMessage

TP ld	TP_SEC_ITSS_RCV_DENM_04_09_BO
Summary	Check that IUT discards a Secured DENM if the header fields are not in the ascending order
	according to the numbering of the enumeration.
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivir	ng a SecuredMessage (MSG_SEC_RCV_DENM_A)
containing hea	der_fields[0].type
indicating 'si	gner_info'
and containing	header_fields[1].type
indicating 'its	s_aid'
and containing	header_fields[2].type
indicating 'ge	eneration_time'
and containing	header_fields[3].type
indicating 'ge	eneration_location'
then	
the IUT discards t	he SecuredMessage

TP ld	TP_SEC_ITSS_RCV_DENM_04_10_BO
Summary	Check that IUT discards a Secured DENM containing header field of type
	'generation_time_standard_deviation'
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
and the IUT curren	t time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
	ing a SecuredMessage (MSG_SEC_RCV_DENM_A)
	ader_fields[0].type
indicating 's	• =
	g header_fields[1].type
	jeneration_time'
	g header_fields[2]
containing	
	g 'generation_time_standard_deviation'
containir	ing generation_time_with_standard_deviation
	ing CURRENT_TIME
	aining log_std_dev
	ing 255
	g header_fields[3].type
	jeneration_location
	g header_fields[4].type
indicating 'i	
then	
	a SecuredMessage

TP ld	TP_SEC_ITSS_RCV_DENM_04_11_BO
Summary	Check that IUT discards the Secured DENM containing the header fields of type
Summary	'expiry_time'
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the '	authorized' state
and the IUT current ti	me is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
	g a SecuredMessage (MSG_SEC_RCV_DENM_A)
containing head	
indicating 'sig	
and containing h	••
containing typ	
	generation_time'
containing ge	
0	
and containing h	••
containing typ	
indicating '	
and containin	CURRENT_TIME + 1 h
	neader_fields[3].type
	neration_location
	neader_fields[4].type
indicating 'its	
<b>U</b> -	ng other header fields
then	
	e SecuredMessage

TP ld	TP_SEC_ITSS_RCV_DENM_04_12_BV
Summary	Check that IUT accepts the Secured DENM containing additional non-standard HeaderField
Reference	ETSI TS 103 097 [1], clause 7.2
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	
the IUT is receiving a S	SecuredMessage (MSG_SEC_RCV_DENM_A)
containing header_fi	
indicating 'signer_	
and containing head	
indicating 'generat	
and containing head	
indicating 'generat	
and containing head	er_fields[3].type
indicating 'its_aid'	
and containing head	er_fields[4]
containing type	the dead has dead in the (4000)
	standard header field type (1000)
and containing oth	
indicating non-e	
and not containing o	
	ourodMossaga
the IUT accepts the Se	Cureumessaye

TP ld	TP_SEC_ITSS_RCV_DENM_04_13_BO
	Check that IUT discards the Secured CAM containing the header field
Summary	encryption_parameter' and 'recipient_info'
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
	thorized' state with CERT_IUT_A_AT
and the IUT current time	e is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
	<pre>securedMessage (MSG_SEC_RCV_DENM_A)</pre>
containing header	
indicating 'signe	
and containing hea	
indicating 'gener	
and containing hea	
indicating 'gene	
and containing hea	
indicating 'its_ai	
and containing hea	ader_fields[4]
containing type	
	cryption_parameters'
and containing e	
	mm_algorithm
	aes_128_ccm'
and containin	
and containing hea	ader_tields[5]
containing type	ining info
indicating 'rec	
and containing r	
containing rec	
containing	
	ing to CERT_IUT_A_AT
	ning pk_encryption g 'ecies_nistp256'
	ning enc_key
	other header fields
then	
the IUT discards the	SecuredMessage

TP ld	TP_SEC_ITSS_RCV_DENM_04_14_BO
	Check that IUT discards the Secured DENM containing the header fields of type
	'request_unrecognized_certificate'
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'auth	orized' state with X_IUT_AT_CERT
and the IUT current time	is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
	SecuredMessage (MSG_SEC_RCV_DENM_A)
containing header_f	
indicating 'signer_	
and containing head	ler_fields[1]
containing type	
indicating 'gene	
containing genera	
indicating CUR	—
and containing head	ier_neids[2]
containing type	est upressentiated sertificate
•	est_unrecognized_certificate'
and containing dig	igest of X_IUT_AT_CERT
and containing head	
indicating 'genera	
and containing head	
indicating 'its_aid'	
and not containing c	
then	
the IUT discards the S	ecuredMessage
	T - Any valid AT certificate has been used to authorize IUT.

# 5.3.3.4 Check signer info

TP ld	TP_SEC_ITSS_RCV_DENM_05_01_BO
Summary	Check that IUT discards a Secured DENM if the header_fields contains a signer of type 'self'
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
ensure that when	is inside the time validity period of CERT_TS_A_AT SecuredMessage (MSG_SEC_RCV_DENM_A) ields['signer_info'] type

TP ld	TP SEC ITSS RCV DENM 05 02 BO
	Check that IUT discards a Secured DENM if the header_fields contains a signer of type
	'certificate_digest_with_other_algorithm'
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'a	uthorized' state
and the IUT current tir	ne is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receiving	a SecuredMessage (MSG_SEC_RCV_DENM_A)
containing heade	r_fields['signer_info']
containing sigr	ner.type
indicating 'c	ertificate_digest_with_other_algorithm'
then	
the IUT discards a S	SecuredMessage

TP ld	TP_SEC_ITSS_RCV_DENM_05_03_BO
Summary	Check that IUT discards a Secured DENM if the header_fields contains a signer of type
Summary	certificate_chain
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in t	the 'authorized' state
and the IUT curre	ent time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is rece	iving a SecuredMessage (MSG_SEC_RCV_DENM_A)

containing header\_fields['signer\_info'] containing signer.type indicating 'certificate\_chain' then the IUT discards a SecuredMessage

TP ld	TP_SEC_ITSS_RCV_DENM_05_04_BO
Summany	Check that IUT discards a secured DENM if the header_fields contains a signer info of unknown
Summary	or reserved type
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in t	he 'authorized' state
and the IUT curre	ent time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is rece	iving a SecuredMessage (MSG_SEC_RCV_DENM_A)
containing h	eader_fields['signer_info']
containing	g signer.type
indicati	ng X_UNKNOWN_SIGNERINFO_TYPE
then	-
the IUT discard	ds a SecuredMessage
NOTE: Values to	be used as X_UNKNOWN_SIGNERINFO_TYPE are 5, 239, 240 and 255.

TP ld	TP_SEC_ITSS_RCV_DENM_06_01_BO
Summary	Check that IUT discards a Secured DENM containing generation_time before the certificate
	validity period
Reference	ETSI TS 103 097 [1], clauses 5.4 and 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	a 'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivi	ng a SecuredMessage (MSG_SEC_RCV_DENM_A)
	ider_fields['signer_info']
containing	g certificate (CERT_TS_MSG_06_01_BO_AT)
contair	ning validity_restrictions['time_start_and_end']
	aining start_validity
	dicating START_VALIDITY_AT
	containing end_validity
	dicating END_VALIDITY_AT
	header_fields ['generation_time']
	jeneration_time
•	GEN_TIME < START_VALIDITY_AT
then	
the IUT discards	the message

5.3.3.5	Check generation time	e
---------	-----------------------	---

TP ld	TP_SEC_ITSS_RCV_DENM_06_02_BO
Summary	Check that IUT discards a Secured DENM containing generation_time after the certificate
	validity period
Reference	ETSI TS 103 097 [1], clauses 5.4 and 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
	ng a SecuredMessage (MSG_SEC_RCV_DENM_A)
	der_fields['signer_info']
	g certificate (CERT_TS_MSG_06_02_BO_AT)
	ing validity_restrictions['time_start_and_end']
	aining start_validity
	dicating START_VALIDITY_AT
	containing end_validity
	dicating END_VALIDITY_AT
	header_fields ['generation_time']
then	GEN_TIME > END_VALIDITY_AT
the IUT discards	ure message

#### 5.3.3.6 Check its\_aid

TP ld	TP_SEC_ITSS_RCV_DENM_07_01_BO
Summary	Check that IUT discards a Secured DENM when its_aid value is not AID_DENM
Reference	ETSI TS 103 097 [1], clause 7.2
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 S	SecuredMessage (MSG_SEC_RCV_DENM_A)
containing header_f	ields['its_aid']
indicating 'AID_C	AM'
and containing paylo	pad_field
containing type	
indicating 'signe	
and containing da	
containing DEN	IM payload
then	
the IUT discards the D	ENM message
TP ld	TP_SEC_ITSS_RCV_DENM_07_02_BO
Summary	Check that IUT discards a Secured DENM when its_aid value is undefined

Summary	mmary Check that IUT discards a Secured DENM when its_aid value is undefined	
Reference	eference ETSI TS 103 097 [1], clause 7.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	e 'authorized' state	
and the IUT current	t time is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
the IUT is received	ing a SecuredMessage (MSG_SEC_RCV_DENM_A)	
containing hea	ader_fields['its_aid']	
indicating 'A	AID_UNDEFINED'	
and containing	g payload_field	
containing t	уре	
indicating	j 'signed'	
and contain	ing data	
containin	g DENM payload	
then		
the IUT discards	the message	

TP ld	TP_SEC_ITSS_RCV_DENM_08_01_BO
Summony	Check that IUT discards Secured DENM if the HeaderField generation_location is outside of
Summary	the circular validity region of the signing certificate
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION
	Expected behaviour
with	
the IUT being in the	authorized' state
ensure that	
when	
	ng a SecuredMessage
	header_fields ['signer_info'].type
indicating ce	
	header_fields ['signer_info'].certificate (CERT_TS_AT_B)
•	alidity_restrictions ['region']
containing	
	ning region_type ating 'circle'
	ntaining circular_region
	rating REGION
	header_fields ['generation_location']
	leneration_location
	value outside of the REGION
	header_fields['its_aid']
indicating 'A	
then	
the IUT discards	the message

# 5.3.3.7 Check generation location

TP ld	TP_SEC_ITSS_RCV_DENM_08_02_BO
	Check that IUT discards Secured DENM if the HeaderField generation_location is outside of
Summary	the rectangular validity region of the signing certificate
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY AND PICS_USE_RECTANGULAR_REGION
	Expected behaviour
with	
the IUT being in the 'aut	horized' state
ensure that	
when	
the IUT is receiving a	8
5	fields ['signer_info'].type
indicating certific	
	der_fields ['signer_info'].certificate (CERT_TS_AT_C)
	ty_restrictions ['region']
containing reg	
containing r	
	y 'rectangle'
	ing rectangular_regions
	g REGION der_fields ['generation_location']
containing gener	
	ie outside of the REGION
and containing hea	
indicating 'AID_E	
then	
the IUT discards the r	nessage
	······································

TP ld	TP_SEC_ITSS_RCV_DENM_08_03_BO
	Check that IUT discards Secured DENM if the HeaderField generation_location is outside of
Summary	the polygonal validity region of the signing certificate
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION
	Expected behaviour
with	
the IUT being in the 'a	uthorized' state
ensure that	
when	
	a SecuredMessage
5	er_fields ['signer_info'].type
indicating cert	
•	eader_fields ['signer_info'].certificate (CERT_TS_AT_D)
	dity_restrictions ['region']
containing I	
	g region_type
	ing 'polygon'
	aining polygonal_region
	ing REGION
	eader_fields ['generation_location']
	neration_location
	alue outside of the REGION eader_fields['its_aid']
indicating 'AID	
then	
the IUT discards th	e message

TP ld	TP_SEC_ITSS_RCV_DENM_08_04_BO
Cummon.	Check that IUT discards Secured DENM if the HeaderField generation_location is outside o
Summary	the identified validity region of the signing certificate
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION
	Expected behaviour
with	
the IUT being in the	authorized' state
ensure that	
when	
	g a SecuredMessage
	ler_fields ['signer_info'].type
indicating ce	
	header_fields ['signer_info'].certificate (CERT_TS_AT_E)
	lidity_restrictions ['region']
containing	
	ng region_type
	ting 'id_region' containing identified_region
	ting REGION
	header_fields ['generation_location']
	eneration_location
	value outside of the REGION
	header_fields['its_aid']
indicating 'Al	
then	
the IUT discards t	ne message

### 5.3.3.8 Check Payload

TP ld	TP_SEC_ITSS_RCV_DENM_09_02_BO
Summary	Check that IUT discards the Secured DENM containing empty payload of type 'signed'
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
	ng a SecuredMessage (MSG_SEC_RCV_DENM_A)
containing pay	oad_field
containing ty	pe
indicating	'signed'
and containi	ng data
indicating	length 0
then	
the IUT discards	

TP ld	TP_SEC_ITSS_RCV_DENM_09_03_BO
Summary	Check that IUT discards the Secured DENM containing payload of type 'unsecured'
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivi	ng a SecuredMessage (MSG_SEC_RCV_DENM_A)
containing pay	
containing t	
indicating	'unsecured'
and contain	ing data
	length > 0
then	<b>.</b>
the IUT discards	the message

TP ld	TP_SEC_ITSS_RCV_DENM_09_04_BO
Summary	Check that IUT discards the Secured DENM containing payload of type 'encrypted'
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'a	authorized' state
and the IUT current ti	me is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receiving	g a SecuredMessage (MSG_SEC_RCV_DENM_A)
containing paylo	ad_field
containing type	
indicating 'encrypted'	
and containing data	
indicating length > 0	
then	
the IUT discards the message	

TP ld	TP_SEC_ITSS_RCV_DENM_09_05_BO		
Summary	Check that IUT discards the Secured DENM containing payload of type 'signed_external'		
Reference	ETSI TS 103 097 [1], clause 7.2		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT being in the 'auth	norized' 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 S	SecuredMessage (MSG_SEC_RCV_DENM_A)		
containing payload_	containing payload_field		
containing type			
indicating signed_external			
and containing data			
indicating length $> 0$			
then			
the IUT discards the m	nessage		

TP ld	TP_SEC_ITSS_RCV_DENM_09_06_BO	
6	Check that IUT discards the Secured DENM containing exactly one non-empty payload of	
Summary	type 'signed_and_encrypted'	
Reference	ETSI TS 103 097 [1], clause 7.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	'authorized' state	
and the IUT current	time is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
	ng a SecuredMessage (MSG_SEC_RCV_DENM_A)	
containing payload_field		
containing type		
indicating 'signed_and_encrypted'		
and containing data		
indicating length > 0		
then		
the IUT discards the message		

#### 5.3.3.9 Check presence of trailer field

TP ld	TP_SEC_ITSS_RCV_DENM_10_01_BO
Summers/	Check that IUT discards the Secured DENM if the message does not contain the trailer field
Summary	of type signature
Reference	ETSI TS 103 097 [1], clause 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
ensure that when the IUT is receiving a containing trailer_f not containing tr	e is inside the time validity period of CERT_TS_A_AT SecuredMessage (MSG_SEC_RCV_DENM_A)
then the IUT discards the message	

TP Id	TP_SEC_ITSS_RCV_DENM_10_02_BO	
Summers/	Check that IUT discards the Secured DENM containing more than one instance of	
Summary	TrailerField of type 'signature'	
Reference	ETSI TS 103 097 [1], clause 7.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'autl	horized' 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 SecuredMessage (MSG_SEC_RCV_DENM_A)		
containing trailer_fi		
containing type	••	
indicating 'signature'		
and containing trailer_fields[1]		
containing type		
indicating 'signature'		
then		
the IUT discards the n	nessage	

### 5.3.3.10 Check signature

TP ld	TP_SEC_ITSS_RCV_DENM_11_01_BO	
Summary	Check that the IUT discards Secured DENM containing signature that is not verified using	
	the verification key from the certificate contained in the message's signer info	
Reference	ETSI TS 103 097 [1], clauses 4.2.2 and 7.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with	·	
the IUT being in the	authorized' state	
	ime is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
the IUT is receivin	g a SecuredMessage (MSG_SEC_RCV_DENM_A)	
containing head	er_fields ['signer_info']	
containing sig	gner	
containing	certificate (CERT_TS_A_AT)	
	ng subject_attributes['verification key']	
conta	ining key (KEY)	
and containing	rrailer_fields[0]	
containing type		
indicating 'signature'		
containing signature		
NOT verifiable using KEY		
then		
the IUT discards the message		

TP ld	TP_SEC_ITSS_RCV_DENM_11_02_BO
Summary	Check that IUT discards the Secured DENM if the message contains trailer field of type
	'signature' with reserved public key algorythms
Reference	ETSI TS 103 097 [1], clauses 4.2.2 and 7.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	a 'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivi	ng a SecuredMessage (MSG_SEC_RCV_DENM_A)
containing trai	ler_fields
containing a	in instance of type TrailerField
containin	
indicat	ing 'signature'
and conta	aining signature.algorithm
indicat	ing X_RESERVED_PK_ALGORYTHM
then	
the IUT discards	the message
NOTE: Values to b	e provided as X_RESERVED_PK_ALGORYTHM are: 240, 255.

# 5.3.3.11 Check signing certificate type

TP ld	TP_SEC_ITSS_RCV_DENM_12_01_BO	
Summary	Check that IUT discards a Secured DENM if the signer certificate of the message contains	
	the subject type 'enrolment_credential'	
Reference	ETSI TS 103 097 [1], clause 6.3	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	'authorized' state	
ensure that		
when		
the IUT is receivir	ng a SecuredMessage	
containing header_fields ['signer_info']		
containing signer.type		
indicating 'certificate'		
containing signer.certificate (CERT_TS_EA_A)		
containing subject_info.subject_type		
indicating 'enrolment_credentials'		
containing header_fields['its_aid']		
indicating 'AID_DENM'		
then		
the IUT discards t	he message	

TP ld	TP_SEC_ITSS_RCV_DENM_12_02_BO	
Summony	Check that IUT discards a Secured DENM if the signer certificate of the message contains	
Summary	the subject type "authorization_authority"	
Reference	ETSI TS 103 097 [1], clause 6.3	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'auth	orized' state	
ensure that		
when		
the IUT is receiving a SecuredMessage		
containing header_fields ['signer_info']		
containing signer.type		
indicating 'certificate'		
containing signer.certificate (CERT_TS_AA_A)		
containing subject_info.subject_type		
indicating 'authorization_authority'		
containing header_fields['its_aid']		
indicating 'AID_DENM'		
then		
the IUT discards the message		

TP ld	TP SEC ITSS RCV DENM 12 03 BO	
Summary	Check that IUT discards a Secured DENM if the signer certificate of the message contains the subject type 'enrolment_authority'	
Reference	ETSI TS 103 097 [1], clause 6.3	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with the IUT being in the	'authorized' state	
0	time is inside the time validity period of CERT_TS_A_AT	
when		
the IUT is receivi	ng a SecuredMessage (MSG_SEC_RCV_DENM_A)	
containing hea	ider_fields ['signer_info']	
containing s	igner	
containing type		
indicating 'certificate'		
containing certificate (CERT_TS_A_EA)		
containing subject_info.subject_type		
indicating 'enrolment_authority'		
then		
the IUT discards the message		

TP ld	TP_SEC_ITSS_RCV_DENM_12_04_BO	
Summary	Check that IUT discards a Secured DENM if the signer certificate of the message contains	
Summary	the subject type 'root_ca'	
Reference	ETSI TS 103 097 [1], clause 6.3	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'auth	norized' 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 SecuredMessage (MSG_SEC_RCV_DENM_A)	
containing header_f		
containing signer		
containing type		
indicating 'certificate'		
containing certificate (CERT_TS_ROOT)		
containing subject_info.subject_type		
indicating 'root_ca'		
then		
the IUT discards the m	nessage	

# 5.3.3.12 Check certificate validity

TP ld	TP_SEC_ITSS_RCV_DENM_13_01_BO
Summary	Check that IUT discards secured DENM signed with the not yet valid certificate
Reference	ETSI TS 103 097 [1], clause 6.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'aut	horized' state
and the IUT current time	e is before the time validity period of CERT_TS_MSG_13_01_BO_AT
ensure that	
when	
	SecuredMessage (MSG_SEC_RCV_DENM_A)
containing header_	fields['signer_info'].signer
containing certifi	cate (CERT_TS_MSG_13_01_BO_AT)
containing val	idity_restrictions['time_start_and_end']
containing s	start_validity
indicating	g START_VALIDITY_AT > CURRENT_TIME
and contain	ing end_validity
indicating	g END_VALIDITY_AT > START_VALIDITY_AT
then	
the IUT discards the r	nessage

TP ld	TP_SEC_ITSS_RCV_DENM_13_02_BO
Summary	Check that IUT discards secured DENM signed with the expired certificate
Reference	ETSI TS 103 097 [1], clause 6.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	
and the IUT current	time is before the time validity period of CERT_TS_MSG_13_02_BO_AT
ensure that	
when	
	ng a SecuredMessage (MSG_SEC_RCV_DENM_A)
	der_fields['signer_info'].signer
	ertificate (CERT_TS_MSG_13_02_BO_AT)
	g validity_restrictions['time_start_and_end']
	ing start_validity
	ating START_VALIDITY_AT < CURRENT_TIME ntaining end_validity
	ating END_VALIDITY_AT < CURRENT_TIME
then	
the IUT discards	the message
TP ld	TP_SEC_ITSS_RCV_DENM_13_03_BO
Summory	Check that IUT discards secured DENM when IUT location is outside the circular validity
Summary	restriction of the signing certificate
Reference	ETSI TS 103 097 [1], clause 6.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	
	time is inside the validity period of CERT_TS_MSG_13_03_BO_AT
	location is set to CURRENT_IUT_LOCATION
ensure that	
when	
	ng a SecuredMessage (MSG_SEC_RCV_DENM_B)
	der_fields['signer_info'].signer ertificate (CERT_TS_MSG_13_03_BO_AT)

- containing certificate (CERT\_TS\_MSG\_13\_03\_BO\_AT) containing validity\_restrictions['region'] containing region

indicating REGION

- containing region\_type indicating 'circle' and containing circular\_region
- not containing the CURRENT\_IUT\_LOCATION then

the IUT discards the message

TP ld	TP_SEC_ITSS_RCV_DENM_13_04_BO
Summary	Check that IUT discards secured DENM when IUT location is outside the rectangular validity
	restriction of the signing certificate
Reference	ETSI TS 103 097 [1], clause 6.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
and the IUT current	time is inside the validity period of CERT_TS_MSG_13_04_BO_AT
and the IUT current	location is set to CURRENT_IUT_LOCATION
ensure that	
when	
the IUT is receivi	ng a SecuredMessage (MSG_SEC_RCV_DENM_C)
containing hea	ider_fields['signer_info'].signer
	ertificate (CERT_TS_MSG_13_04_BO_AT)
containing	g validity_restrictions['region']
contair	ing region
cont	aining region_type
in	dicating 'rectangle'
and	containing rectangular_regions
in	dicating REGION
	not containing the CURRENT_IUT_LOCATION
then	
the IUT discards	the message
TP ld	TP_SEC_ITSS_RCV_DENM_13_05_BO
	Check that IUT discards secured DENM when IUT location is outside the polygonal validity

I P Id	IP_SEC_IISS_RCV_DENM_13_05_BO
Summary	Check that IUT discards secured DENM when IUT location is outside the polygonal validity
	restriction of the signing certificate
Reference	ETSI TS 103 097 [1], clause 6.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'au	thorized' state
and the IUT current time	e is inside the validity period of CERT_TS_MSG_13_05_BO_AT
and the IUT current loca	ation is set to CURRENT_IUT_LOCATION
ensure that	
when	
the IUT is receiving a	I SecuredMessage (MSG_SEC_RCV_DENM_D)
	_fields['signer_info'].signer
containing certif	icate (CERT_TS_MSG_13_05_BO_AT)
6	lidity_restrictions['region']
containing	5
	ng region_type
	ting 'polygon'
	taining polygonal_region
	ting REGION
	containing the CURRENT_IUT_LOCATION
then	
the IUT discards the	message

TP ld	TO SEC ITSS DOV DENM 12 06 DO
Summary	TP_SEC_ITSS_RCV_DENM_13_06_BO
	Check that IUT discards secured DENM when IUT location is outside the identified validity
-	restriction of the signing certificate
Reference	ETSI TS 103 097 [1], clause 6.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current f	time is inside the validity period of CERT_TS_MSG_13_06_BO_AT
and the IUT current I	location is set to CURRENT_IUT_LOCATION
ensure that	
when	
the IUT is receivin	ig a SecuredMessage (MSG_SEC_RCV_DENM_E)
	Jer_fields['signer_info'].signer
containing ce	ertificate (CERT_TS_MSG_13_06_BO_AT)
	validity_restrictions['region']
	ng region
	ining region_type
ind	licating 'id'
	containing id_region
	licating REGION
	not containing the CURRENT_IUT_LOCATION
then	<b>v</b>
the IUT discards the	he message

# 5.3.4 Generic Signed Message Profile

#### 5.3.4.1 Check that IUT accepts well-formed GN Beacon message

Check that IUT accepts a well-formed Secured GN Beacon signed with the certificate without region validity restriction           Reference         ETSI TS 103 097 [1], clause 7.3           PICS Selection         PICS_GN_SECURITY           Expected behaviour           vith         the IUT being in the 'authorized' state and the IUT current time is inside the time validity period of CERT_TS_A_AT	TP ld	TP_SEC_ITSS_RCV_GENMSG_01_01_BV
Minimary         without region validity restriction         -           IdS Selection         PICS_GN_SECURITY         -           IdS Selection         PICS_GN_SECURITY         -           ith         the UT being in the 'authorized' state         -           and the UT current time is inside the time validity period of CERT_TS_A_AT         -           nsure that         when         -           the UT is receiving a SecuredMessage         -         -           containing topool         version         -           indicating value '2'         -         -           and containing type         -         -           indicating certificate (CERT_TS_A_AT)         -         -           and containing upper timolating value '2'         -         -         -           and containing upper timolating value '2'         -         -         -           indicating Certificate'         -         -         -         -           and containing upper timoles (VERT_TS_A_AT)         -	_	
Efference         ETSITE 103 097 [1], clause 7.3           ICS Selection         PICS_GN_SECURITY           Expected behaviour           ith         Expected behaviour           ith         Expected behaviour           ith         IUT being in the 'authorized' state           and the IUT current time is inside the time validity period of CERT_TS_A_AT           insure that         when           the IUT is receiving a SecuredMessage         containing protocol_version           indicating signer_info'         and containing peader_fields[0]           containing type         indicating signer           containing signer         containing signer           containing subject_info.subject_type         indicating 'signer_info'           and containing subject_info.subject_type         indicating 'signer'           indicating 'signer'         containing subject_info.subject_type           indicating 'signer'         and containin	Summary	
ICS Selection         PICS_GN_SECURITY           ith         Expected behaviour           ith         the UT being in the 'authorized' state           and the UT current time is inside the time validity period of CERT_TS_A_AT           issue that         when           the IUT is receiving a SecuredMessage         containing protocol_version           indicating value '2'         and containing period           and containing signer_info'         and containing signer           containing type         indicating 'certificate'           and containing subject_info.subject_type         indicating 'certificate'           and containing select_info.subject_type         indicating 'certificate'           and containing select_info.subject_type         indicating 'certificate'           and containing select_info.subject_type         indicating 'certificate'	Reference	
Expected behaviour           ith         the IUT being in the 'authorized' state           and the IUT current time is inside the time validity period of CERT_TS_A_AT           nsure that           when           the IUT is receiving a SecuredMessage           containing protocol_version           indicating value '2'           and containing beader_fields[0]           containing type           indicating 'signer_info'           and containing optimicate'           and containing optimicate'           and containing subject_attributes[Verification key] (KEY)           and containing validity_restrictions['time_star_and_end]           indicating generation_time'           and containing validity_restrictions['time_star_and_end]           indicating generation_time'           and containing validity_restrictions['tegion]           indicating validity_res	PICS Selection	
<pre>ith U being in the 'authorized' state and the IUT current time is inside the time validity period of CERT_TS_A_AT nsure that when the IUT is receiving a SecuredMessage containing protocol_version indicating value '2' and containing type indicating 'sortlicate' and containing type indicating 'certificate' and containing type indicating 'certificate' and containing subject_trification (CERT_TS_A_AT) containing subject_trification (icket' and containing subject_trification (key] (KEY) and containing subject_trification (key] indicating 'certificate' and containing subject_trification (key] (KEY) and containing subject_trification (key] indicating 'certificate' and containing subject_trification (key] indicating 'CERT_TS_AT_TIME_VALIDITY and not containing validity_restrictions['region] and containing header_fields [1] containing type indicating 'generation_time' indicating 'generation_time' indicating 'generation_time' indicating 'generation_time indicating 'peneration_location' and containing header_fields [2] containing type indicating 'spectrification' and containing header_fields[3] containing header_fields[3] containing type indicating 'signed' and containing header_fields [3] containing type indicating 'signed' and containing header_fields [3] containing type indicating 'signed' and containing header_fields [3] containing type indicating 'signed' and containing tailer_fields containing type indicating 'signed' and containing said indicating 'signature verifiable using KEY then the IUT accepts the message HOTE: the message delified in this test purpose is used in the subsequent test purposes with the snippet name</pre>		
the IUT being in the 'authorized' state and the IUT current time is inside the time validity period of CERT_TS_A_AT nsure that when the IUT is receiving a SecuredMessage containing protocol_version indicating value "2" and containing header_fields[0] containing type indicating 'signer_info' and containing signer_info' and containing certificate (CERT_TS_A_AT) containing subject_info.subject_type indicating 'authorization ticket and containing subject_attributes[verificationkey] (KEY) and containing subject_attributes[verificationkey] indicating 'authorization' ticket and containing validity_restrictions['time_stat_and_end] indicating 'authorization' ticket and containing validity_restrictions['time_stat_and_end] indicating 'generation_time' and containing validity_restrictions['time_indicating 'authorization' ticket and containing validity_restrictions['time_indicating 'authorization' ticket and containing validity_restrictions['time_indicating 'authorization' time' and containing yalotify_restrictions['time_indicating 'QERT_TS_AT_TIME_VALIDITY and containing generation_time' indicating 'generation_time' indicating 'generation_location' and containing generation_location' and containing generation_	with	
and the IUT current time is inside the time validity period of CERT_TS_A_AT sure that when the IUT is receiving a SecuredMessage containing protocol_version indicating volue '2' and containing type indicating 'signer_into' and containing subject_info: subject_TS_A_AT) containing subject_info: subject_type indicating 'authorization_ticket' and containing subject_info: subject_type indicating 'subject_info: subject_type indicating 'generation_time' and containing header_fields[1] containing type indicating 'generation_time' indicating 'generation_time indicating 'generation_time indicating 'generation_time indicating 'generation_time indicating 'generation_location' and containing header_fields[2] containing type indicating 'generation_location' and containing header_fields[3] containing type indicating 'signed' and containing beEACON' and containing based indicating 'signed' and containing signed' and containing tailet_fields containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message top prove is used in the subsequent test purposes with the snippet name		horized' state
nsure that when the IUT is receiving a SecuredMessage containing protocol_version indicating value '2' and containing signer_into' and containing signer containing signer containing signer containing signer containing subject_info.subject_type indicating 'uthorization ticket' and containing subject_attributes['verification key'] (KEY) and containing subject_into.subject_type indicating 'uthorization ticket' and containing subject_into.subject_type indicating 'uthorization ticket' and containing subject_into.subject_type indicating 'uthorization ticket' and containing subject_into.subject_type indicating 'generation_ticket' and containing subject_into: and containing subject_into: indicating 'generation_time' and containing peacr-fields[1] containing type indicating 'generation_time' and containing peacr-fields[2] containing header_fields[2] containing header_fields[3] containing header_fields[3] containing header_fields[3] containing header_fields[3] containing header_fields[3] containing gayload_field indicating 'signed' and containing gayload_field indicating signed' and containing signature' verifiable using KEY then the IUT accepts the message torpose is used in the subsequent test purposes with the snippet name		
<pre>when the IUT is receiving a SecuredMessage containing protocol_version indicating value '2' and containing type indicating 'igner_info' and containing signer containing type indicating 'certificate' and containing subject_infos.vbiect_type indicating 'authorization_ticket' and containing subject_attributes['verification key'] (KEY) and containing validity_restrictions['time_start_and_end'] indicating 'authorization_ticket' and containing validity_restrictions['time_start_and_end'] indicating 'authorization_ticket' and containing validity_restrictions['time_start_and_end'] indicating 'generation_time' and containing header_fields[1] containing yea indicating 'generation_time' and containing perfect indicating 'generation_time' and containing perfect indicating 'generation_time' and containing generation_time indicating 'generation_time indicating 'generation_time indicating 'generation_time' and containing pader_fields[2] containing type indicating 'generation_location and containing pader_fields[3] containing type indicating 'signed' and containing pader_fields[3] containing type indicating 'signed' and containing pade_field containing taile_fields containing taile_fields containing</pre>	ensure that	
containing protocol_version indicating value '2' and containing header_fields[0] containing type indicating 'signer_info' and containing signer containing type indicating 'certificate' and containing uselect_info.subject_type indicating 'authorization_itcket' and containing subject_info.subject_type indicating 'authorization_itcket' and containing subject_info.subject_type indicating 'authorization_itcket' and containing subject_info.subject_type indicating 'authorization_itcket' and containing subject_info.subject_type indicating CERT_TS_AT_TIME_VALIDITY and not containing header_fields[1] containing type indicating (generation_time indicating (generation_time indicating (generation_time indicating (generation_location) and containing header_fields[2] containing type indicating (section)_costion' and containing header_fields[3] containing header_fields[3] containing header_fields[3] containing type indicating 'ID_BEACON' and containing taile_fields indicating 'Signed' and containing traile_fields containing		
containing protocol_version indicating value '2' and containing header_fields[0] containing type indicating 'signer_info' and containing signer containing type indicating 'certificate' and containing uselect_info.subject_type indicating 'authorization_itcket' and containing subject_info.subject_type indicating 'authorization_itcket' and containing subject_info.subject_type indicating 'authorization_itcket' and containing subject_info.subject_type indicating 'authorization_itcket' and containing subject_info.subject_type indicating CERT_TS_AT_TIME_VALIDITY and not containing header_fields[1] containing type indicating (generation_time indicating (generation_time indicating (generation_time indicating (generation_location) and containing header_fields[2] containing type indicating (section)_costion' and containing header_fields[3] containing header_fields[3] containing header_fields[3] containing type indicating 'ID_BEACON' and containing taile_fields indicating 'Signed' and containing traile_fields containing	the IUT is receiving a	SecuredMessage
indicating value '2' and containing header_fieldS[0] containing type indicating 'signer_info' and containing generificate (CERT_TS_A_AT) containing certificate' and containing certificate (CERT_TS_A_AT) containing value'z' througe 'signer' indicating 'authorization_ticket' and containing subject_attributes['verification key'] (KEY) and containing value'_ity_restrictions['time_start_and_end'] indicating CERT_TS_AT_TIME_VALIDITY and not containing validity_restrictions['region'] and containing generation_time' and containing generation_time indicating 'generation_time indicating 'generation_time' and containing header_fieldS [2] containing header_fieldS [2] containing header_fieldS [2] containing header_fieldS[3] containing generation_location and containing generation_location and containing generation_location and containing trailer_fieldS[3] containing type indicating 'AID_BEACCN' and containing fataid indicating 'signed' and containing fataid indicating type indicating type indicating type indicating type indicating type indicating trailer_fieldS containing trailer_fieldS containing type indicating 'signed' and containing fatai indicating 'signed' and containing fatai indicating 'signature' and containing tailer_fieldS containing type indicating 'signature' and containing signature verifiable using KEY then the UT accepts the message		
and containing header_fields[0] containing type indicating signer_info' and containing signer containing ype indicating 'certificate' and containing subject_info.subject_type indicating 'authorization_licket' and containing subject_atributes[verification key] (KEY) and containing validity_restrictions['time_start_and_end] indicating (CERT_TS_AT_TIME_VALIDITY and not containing validity_restrictions['time] and containing header_fields [1] containing type indicating 'generation_time and containing type antime indicating 'generation_time indicating 'generation_time indicating 'generation_time indicating 'generation_time indicating 'generation_time indicating 'generation_location' and containing header_fields[2] containing type indicating 'is_aid' and containing header_fields[3] containing type indicating 'signed' and containing traied' and containing traied' indicating 'signed' and containing traied' indicating 'signed' and containing traiefields containing traiefields		
<pre>indicating 'signer_info' and containing signer containing type indicating 'certificate' and containing subject_info.subject_type indicating 'certificate' and containing subject_attributes['verification key'] (KEY) and containing subject_attributes['verification key'] (KEY) and containing validity_restrictions['time_star_and_end'] indicating 'CERT_TS_AT_TIME_VALIDITY and not containing header_fields [1] containing type indicating 'generation_time' and containing ender_fields [2] containing header_fields [2] containing header_fields [2] containing header_fields [2] containing header_fields [3] containing header_fields [3] containing header_fields [4] and containing header_fields [4] containing header_fields [4] containing header_fields [5] containing type indicating 'generation_coation' and containing header_fields [4] containing header_fields [5] containing type indicating 'signerd' and containing traite_fields Con</pre>		
and containing signer containing vertificate and containing certificate (CERT_TS_A_AT) containing subject_infocublect_type indicating 'authorization_ticket' and containing subject_attributes[verification key'] (KEY) and containing validity_restrictions[time_start_and_end] indicating CERT_TS_AT_TIME_VALIDITY and not containing validity_restrictions[region] and containing palety_restrictions[region] and containing spectration_time indicating (Suprestrictions[region]) and containing spectration_time indicating (Suprestrictions[region]) and containing spectration_time indicating (Suprestrictions[region]) and containing spectration_time indicating (Suprestrictions] and containing header_fields [2] containing type indicating (Suprestrictions] and containing header_fields[3] containing type indicating (Suprestrictions] and containing header_fields[3] containing type indicating 'is_, aid' and containing type indicating 'is_, aid and containing paload_field containing type indicating 'is_, aid and containing type and containing type and containing type an		
<pre>containing type indicating 'certificate (CERT_TS_A_AT) containing subject_info.subject_type indicating 'authorization_ticket' and containing subject_attributes['verification key'] (KEY) and containing validity_restrictions['time_start_and_end] indicating CERT_TS_AT_TIME_VALIDITY and not containing validity_restrictions['region'] and containing header_fields [1] containing type indicating generation_time' and containing generation_time indicating GurRENT_TIME_VALIDITY and containing peneration_time indicating generation_time indicating generation_time indicating generation_time indicating generation_time indicating generation_tocation and containing header_fields[3] containing header_fields[3] containing header_fields[3] containing theader_fields[3] containing theader_fields[4] and containing header_fields[3] containing theader_fields[4] containing theader_fields[3] containing theader_fields[3] containing theader_fields[3] containing theader_fields[3] containing theader_fields[3] containing theader_fields[3] containing theader_fields indicating 'signed' and containing tailer_fields[0] containing trailer_fields[0] containing trailer_fields[0] containing isignature' and containing signature' and containing signature' and containing signature verifiable using KEY then the IUT accepts the message DOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name</pre>		ier_info'
<pre>indicating 'certificate' and containing certificate (CERT_TS_A_AT) containing subject_info.subject_type indicating 'authorization_ticket' and containing subject_info.subject_type indicating CERT_TS_AT_TIME_VALIDITY and not containing validity_restrictions['time_start_and_end] indicating CERT_TS_AT_TIME_VALIDITY and not containing validity_restrictions['region'] and containing validity_restrictions['time_start_and_end] indicating 'generation_time' and containing generation_time' indicating 'generation_time' indicating 'generation_time indicating 'generation_time indicating 'generation_time indicating 'generation_time indicating 'generation_location' and containing header_fields[2] containing type indicating 'generation_location and containing header_fields[3] containing type indicating 'signed' and containing payload_field containing type indicating 'signed' and containing tailer_fields containing trailer_fields containing signature and containing signature the IUT accepts the message DOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name</pre>	and containing si	gner
and containing subject_info.subject_type indicating 'authorization_ticket' and containing subject_attributes['verification key'] (KEY) and containing validity_restrictions['time_start_and_end'] indicating CERT_TS_AT_TIME_VALIDITY and not containing validity_restrictions['region'] and containing header_fields [1] containing header_fields [2] containing header_fields [2] containing header_fields [2] containing header_fields [2] containing header_fields [3] containing header_fields[3] containing its_aid' and containing its_aid' and containing header_fields[3] containing type indicating 'Signed' and containing header_fields[3] containing type indicating 'signed' and containing header_fields[3] containing header_fields[3] containing type indicating 'signed' and containing header_fields[3] containing type indicating 'signed' and containing header_fields[3] containing type indicating 'signed' and containing header_fields[3] containing type indicating 'signed' and containing theader_fields[3] containing type indicating 'signed' and containing theader_fields[3] containing type indicating 'signed' and containing theader_fields[3] containing type indicating 'signed' and containing trailer_fields[0] containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message MOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name	containing type	e
<pre>containing subject_info.subject_type indicating 'authorization_ticket' and containing validity_restrictions[time_start_and_end'] indicating OERT_TS_AT_TIME_VALIDITY and not containing validity_restrictions[region'] and containing header_fields [1] containing type indicating (URRENT_TIME_VALIDITY and containing generation_time' indicating (URRENT_TIME_VALIDITY and containing header_fields [2] containing type indicating (URRENT_TIME_VALIDITY and containing header_fields [2] containing type indicating (generation_location' and containing generation_location' and containing generation_location' and containing header_fields[3] containing type indicating 'its_aid' and containing its_aid indicating 'ID_BEACON' and containing payload_field containing hype indicating 'signed' and containing type indicating 'signed' and containing type ind</pre>	indicating 'c	ertificate'
indicating 'authorization_ticket' and containing validity_restrictions['time_start_and_end'] indicating CERT_TS_AT_TIME_VALIDITY and not containing validity_restrictions['region'] and containing header_fields [1] containing type indicating generation_time' and containing generation_time indicating CURRENT_TIME inside CERT_TS_AT_TIME_VALIDITY and containing header_fields [2] containing type indicating 'generation_location' and containing header_fields[3] containing type indicating its_aid' and containing theader_fields[3] containing type indicating its_aid and containing type and containing type and containing type and containing type		
and containing subject_attributes['verification key'] (KEY) and containing validity_restrictions['time_start_and_end'] indicating CERT_TS_AT_TIME_VALIDITY and not containing validity_restrictions['region'] and containing type indicating generation_time and containing generation_time indicating CURRENT_TIME_VALIDITY and containing header_fields [2] containing type indicating 'generation_location' and containing generation_location and containing generation_location and containing generation_location and containing its_aid and containing type indicating 'its_aid' and containing type indicating 'generation_location and containing type indicating 'sta_id' and containing tailer_fieldS containing type indicating 'stajenture' and containing tailer_fieldS[0] containing type indicating 'stajenture' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
and containing validity_restrictions['tme_start_and_end'] indicating CERT_TS_AT_TIME_VALIDITY and not containing validity_restrictions['region'] and containing type indicating 'generation_time' and containing generation_time indicating CURRENT_TIME indicating CURRENT_TIME indicating type [ indicating feneration_location' and containing generation_location' and containing generation_location and containing type indicating 'its_aid' and containing paAcCON' and containing paKaCON' and containing type indicating 'signed' and containing data indicating signed' and containing data indicating length > 0 and containing type indicating 'signed' and containing type indicating signed' and containing type indicating signed' and containing tailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message		
indicating CERT_TS_AT_TIME_VALIDITY and not containing validity_restrictions['region'] and containing type indicating 'generation_time indicating OURRENT_TIME inside CERT_TS_AT_TIME_VALIDITY and containing header_fields [2] containing type indicating 'generation_location' and containing generation_location' and containing header_fields[3] containing type indicating 'Its_aid' and containing type indicating 'Its_aid' and containing payload_field containing type indicating 'Jtb_EEACON' and containing type indicating 'Its_aid' and containing type indicating 'signed' and containing type indicating fields[0] containing type indicating 'signet' and containing type indicating 'signet' and containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message		
and not containing validity_restrictions['region'] and containing header_fields [1] containing type indicating 'generation_time' and containing generation_time indicating CURRENT_TIME inside CERT_TS_AT_TIME_VALIDITY and containing header_fields [2] containing type indicating 'generation_location' and containing generation_location and containing header_fields[3] containing type indicating 'its_aid' and containing ts_aid and containing ts_aid indicating 'signed' and containing type indicating 'signed' and containing trailer_fields[0] containing trailer_fields[0] containing type indicating 'signature' and containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message		
and containing header_fields [1] containing type indicating 'generation_time' and containing generation_time indicating CURRENT_TIME inside CERT_TS_AT_TIME_VALIDITY and containing header_fields [2] containing type indicating 'generation_location' and containing generation_location and containing generation_location and containing tis_aid containing type indicating 'its_aid' and containing its_aid indicating 'AID_BEACON' and containing payload_field containing type indicating 'signed' and containing tailer_fields containing trailer_fields containing trailer_fields containing trailer_fields[0] containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
containing type indicating 'generation_time' and containing generation_time indicating CURRENT_TIME inside CERT_TS_AT_TIME_VALIDITY and containing header_fields [2] containing type indicating 'generation_location' and containing generation_location and containing header_fields[3] containing type indicating 'its_aid' and containing its_aid indicating 'AID_BEACON' and containing type indicating 'generation_location' and containing type indicating 'signed' and containing tailer_fields containing trailer_fields containing trailer_fields containing trailer_fields containing trailer_fields containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
indicating 'generation_time' and containing generation_time inside CERT_TS_AT_TIME_ inside CERT_TS_AT_TIME_VALIDITY and containing header_fields [2] containing type indicating 'generation_location' and containing generation_location and containing header_fields[3] containing type indicating 'its_aid' and containing its_aid indicating 'AID_BEACON' and containing type indicating 'signed' and containing tata indicating length > 0 and containing trailer_fields[0] containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message		der_neids [1]
and containing generation_time indicating CURRENT_TIME inside CERT_TS_AT_TIME_VALIDITY and containing header_fields [2] containing type indicating generation_location' and containing header_fields[3] containing header_fields[3] containing type indicating 'its_aid' and containing its_aid indicating 'AID_BEACON' and containing payload_field containing type indicating length > 0 and containing trailer_fields[0] containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		aration time'
indicating CURRENT_TIME inside CERT_TS_AT_TIME_VALIDITY and containing header_fields[2] containing type indicating 'generation_location' and containing generation_location and containing header_fields[3] containing type indicating 'its_aid' and containing its_aid indicating 'AID_BEACON' and containing payload_field containing type indicating 'signed' and containing trailer_fields containing trailer_fields containing trailer_fields containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
inside CERT_TS_AT_TIME_VALIDITY and containing header_fields [2] containing type indicating 'generation_location' and containing generation_location and containing header_fields[3] containing type indicating 'its_aid' and containing its_aid indicating 'AID_BEACON' and containing payload_field containing type indicating 'signed' and containing data indicating length > 0 and containing trailer_fields containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message		
and containing header_fields [2] containing type indicating 'generation_location' and containing generation_location and containing header_fields[3] containing header_fields[3] containing type indicating 'kID_BEACON' and containing payload_field containing type indicating 'signed' and containing data indicating length > 0 and containing trailer_fields[0] containing type indicating 'signature' verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
containing type indicating 'generation_location' and containing generation_location and containing header_fields[3] containing type indicating 'its_aid' and containing its_aid indicating 'AID_BEACON' and containing payload_field containing type indicating 'signed' and containing data indicating length > 0 and containing trailer_fields containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
indicating 'generation_location' and containing generation_location and containing header_fields[3] containing type indicating 'its_aid' and containing its_aid indicating AID_BEACON' and containing payload_field containing type indicating 'signed' and containing data indicating length > 0 and containing trailer_fields containing trailer_fields[0] containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message		
and containing generation_location and containing header_fields[3] containing type indicating 'is_aid' and containing is_aid indicating 'AID_BEACON' and containing payload_field containing type indicating 'signed' and containing data indicating length > 0 and containing trailer_fields containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message		eration location'
and containing header_fields[3] containing type indicating 'its_aid' and containing its_aid indicating 'AID_BEACON' and containing payload_field containing type indicating 'signed' and containing data indicating length > 0 and containing trailer_fields containing trailer_fields[0] containing type indicating 'signature' and containing signature' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
containing type indicating 'its_aid' and containing its_aid indicating 'AID_BEACON' and containing payload_field containing type indicating 'signed' and containing data indicating length > 0 and containing trailer_fields containing trailer_fields[0] containing trailer_fields[0] containing signature' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
indicating 'its_aid' and containing its_aid indicating 'AID_BEACON' and containing payload_field containing type indicating 'signed' and containing data indicating length > 0 and containing trailer_fields containing trailer_fields[0] containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
indicating 'AID_BEACON' and containing payload_field containing type indicating 'signed' and containing data indicating length > 0 and containing trailer_fields containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		aid'
and containing payload_field containing type indicating 'signed' and containing data indicating length > 0 and containing trailer_fields containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name	and containing its	s_aid
containing type indicating 'signed' and containing data indicating length > 0 and containing trailer_fields containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name	indicating 'AID	_BEACON'
indicating 'signed' and containing data indicating length > 0 and containing trailer_fields containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		load_field
and containing data indicating length > 0 and containing trailer_fields containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
indicating length > 0 and containing trailer_fields containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
and containing trailer_fields containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
containing trailer_fields[0] containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
containing type indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
indicating 'signature' and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
and containing signature verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
verifiable using KEY then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
then the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
the IUT accepts the message IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		
IOTE: The message defined in this test purpose is used in the subsequent test purposes with the snippet name		005220L

TP ld	TP_SEC_ITSS_RCV_GENMSG_01_02_BV
Summary	Check that IUT accepts a well-formed Secured GN Beacon signed with the certificate with a
	circular region validity restriction
Reference PICS Selection	ETSI TS 103 097 [1], clause 7.3 PICS_GN_SECURITY
	Expected behaviour
vith	
the IUT being in the 'auth	iorized' state
	is inside the time validity period of CERT_TS_B_AT
	ion is inside the region validity period of CERT_TS_B_AT
ensure that	
when	
the IUT is receiving a S	
containing protocol	
indicating value '2	
and containing heac containing type	
indicating 'sign	er info'
and containing sign	
containing type	
indicating 'ce	
	certificate (CERT_TS_B_AT)
	ubject_info.subject_type
	'authorization_ticket'
	ng subject_attributes['verification key'] (KEY) ng validity_restrictions['time_start_and_end']
	CERT_TS_AT_TIME_VALIDITY
	ng validity_restrictions['region']
containing	
	ing region_type
	ating 'circle'
	ntaining circular_region
	ating REGION
and containing head	Jer_Tields [1]
containing type indicating 'gene	aration time'
and containing ge	
indicating CUR	
and containing head	
containing type	
	eration_location'
	eneration_location
	tion inside the REGION
and containing heac containing type	ายา_แยนร์[ว]
indicating 'its_a	aid'
and containing its	
indicating 'AID	
and containing payle	pad_field
containing type	
indicating 'sign	
and containing da	
indicating lengt and containing traile	
containing trailer	
containing type	
indicating 'si	
and containing	signature
verifiable usi	ing KEY
then	
the IUT accepts the me	
NOTE: The message de	fined in this test purpose is used in the subsequent test purposes with the snippet name /_GENMSG_B'. Only differences to this snippet are mentioned in subsequent test purposes.

108
-----

TP Id	TP_SEC_ITSS_RCV_GENMSG_01_03_BV
Summary	Check that IUT accepts a well-formed Secured GN Beacon signed with the certificate with
Summary	rectangular region validity restriction
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
vith	
the IUT being in the 'auth	is inside the time validity period of CERT_TS_C_AT
	ion is inside the region validity period of CERT_TS_C_AT
ensure that	
when	
the IUT is receiving a S	SecuredMessage
containing protocol_	
indicating value '2	
and containing head	ler_fields[0]
containing type	
indicating 'signe	
and containing sig	
containing type indicating 'ce	
	certificate (CERT_TS_C_AT)
	ubject_info.subject_type
	'authorization_ticket'
	ng subject_attributes['verification key'] (KEY)
	ng validity_restrictions['time_start_and_end']
	CERT_TS_AT_TIME_VALIDITY
	ng validity_restrictions['region']
containing	
	ing region_type
	ating 'rectangle' ntaining rectangular_regions
	ating REGIONS
and containing head	
containing type	
indicating 'gene	eration_time'
and containing ge	
indicating CUR	RENT_TIME
and containing head	ler_fields [2]
containing type	
	eration_location'
and containing ge	
and containing head	ion inside the REGION
containing type	
indicating 'its_a	id'
and containing its	
indicating 'AID_	
and containing paylo	
containing type	
indicating 'signe	
and containing da	
indicating lengt	
and containing traile	
containing trailer_ containing type	
indicating 'sig	
containing sign	
verifiable usi	
then	·······
the IUT accepts the me	essage
	fined in this test purpose is used in the subsequent test purposes with the snippet name

TP ld	TP_SEC_ITSS_RCV_GENMSG_01_04_BV
Summary Check that IUT accepts a well-formed Secured GN Beacon signed with the	
	polygonal region validity restriction
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with the ULT being in the 'out	harizad' atata
the IUT being in the 'aut	a is inside the time validity period of CERT_TS_D_AT
	ition is inside the region validity period of CERT_TS_D_AT
ensure that	auth is inside the region validity period of CERT_TO_D_AT
when	
the IUT is receiving a	SecuredMessage
containing protocol	
indicating value	
and containing hea	
containing type	
indicating sig	ner_info'
and containing s	
containing typ	
indicating 'd	
	g certificate (CERT_TS_D_AT)
	subject_info.subject_type
	g 'authorization_ticket'
	ing subject_attributes['verification key'] (KEY)
	ning validity_restrictions['time_start_and_end'] g CERT_TS_AT_TIME_VALIDITY
	ing validity_restrictions['region']
containin	
	ning region_type
	cating 'polygon'
	ontaining polygonal_region
	cating REGION
and containing hea	
containing type	
indicating 'ger	
and containing g	
	RRENT_TIME
and containing hea	der_fields [2]
containing type	neration location!
	neration_location
	eneration_location ition inside the REGION
and containing hea	
containing type	
indicating 'its_	aid'
and containing it	
indicating 'ĂIE	
and containing pay	load_field
containing type	
indicating 'sig	
and containing d	
indicating leng	
and containing trail	
containing trailer	
containing typ	
indicating 's and containing	
verifiable us	
then	
the IUT accepts the n	lessage
	efined in this test purpose is used in the subsequent test purposes with the snippet name
	V_GENMSG_D'. Only differences to this snippet are mentioned in subsequent test purposes

TP ld	TP_SEC_ITSS_RCV_GENMSG_01_05_BV
Check that IUT accepts a well-formed Secured GN Beacon signed with the certific	
-	an identified region validity restriction
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY
14	Expected behaviour
with	anizadi atata
the IUT being in the 'auth	is inside the time validity period of CERT_TS_E_AT
	tion is inside the region validity period of CERT_TS_E_AT
ensure that	ion is inside the region validity period of OEI(1_10_L_A1
when	
the IUT is receiving a	SecuredMessage
containing protocol	
indicating value '	
and containing head	der_fields[0]
containing type	
indicating 'sign	
and containing si	
containing type	
indicating 'c	
	certificate (CERT_TS_E_AT)
	ubject_info.subject_type 'authorization_ticket'
	ing subject_attributes['verification key'] (KEY)
	ing validity_restrictions['time_start_and_end']
	CERT_TS_AT_TIME_VALIDITY
	ing validity_restrictions['region']
containing	
	ing region_type
	ating 'id_region'
and co	ntaining identified_region
indic	ating REGION
and containing head	der_fields [1]
containing type	
indicating 'gen	
and containing ge	
indicating CUF	
and containing head	
containing type	eration_location'
	eneration_location
	tion inside the REGION
and containing head	
containing type	[1]
indicating 'its_a	aid'
and containing its	s_aid
indicating 'AID	_BEACON'
and containing payl	oad_field
containing type	
indicating 'sign	
and containing da	
indicating leng	
and containing trailer	
containing trailer_ containing type	
indicating 's	
and containing	
verifiable us	
then	
the IUT accepts the m	essage
	ofined in this test purpose is used in the subsequent test purposes with the snippet name
	V_GENMSG_E'. Only differences to this snippet are mentioned in subsequent test purposes

#### 5.3.4.2 Check the message protocol version

TP ld	TP_SEC_ITSS_RCV_GENMSG_02_01_BO
Cummon.	Check that IUT discards a Secured GN Message containing protocol version set to a value
Summary	less than 2
Reference	ETSI TS 103 097 [1], clause 5.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
and the IUT curren	t time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receiv	ing a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
containing pro	tocol_version
indicating 1	
then	
the IUT discards	a SecuredMessage

TP Id	TP SEC ITSS RCV GENMSG 02 02 BO
	Check that IUT discards a Secured GN Message containing protocol version set to a value
Summary	greater than 2
Reference	ETSI TS 103 097 [1], clause 5.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
ensure that when	s inside the time validity period of CERT_TS_A_AT SecuredMessage (MSG_SEC_RCV_GENMSG_A)
the IUT discards a Sec	uredMessage

#### 5.3.4.3 Check header fields

TP ld	TP_SEC_ITSS_RCV_GENMSG_04_01_BO
Summary	Check that IUT discards a secured GN Message if the header_fields contains more than
	one header field of type 'signer_info'
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivin	ng a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
containing head	der_fields[0].type
indicating 'sig	gner_info'
	header_fields[1].type
indicating 'sig	
	header_fields[2].type
	eneration_time'
	header_fields[3].type
	eneration_location'
	header_fields[4].type
indicating 'its	
	ing other header fields
then	
the IUT discards a	a SecuredMessage

TP ld	TP_SEC_ITSS_RCV_GENMSG_04_02_BO	
C	Check that IUT discards a secured GN Message if the header_fields does not contain the	
Summary	header field of type 'signer_info'	
Reference	ETSI TS 103 097 [1], clause 7.3	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	authorized' state	
and the IUT current	time is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
the IUT is receiving	ng a SecuredMessage (MSG_SEC_RCV_GENMSG_A)	
	der_fields[0].type	
	eneration_time'	
	header_fields[1].type	
	eneration_location'	
	header_fields[2].type	
indicating 'its		
and not containing other header fields		
then		

TP Id TP_SEC_ITSS_RCV_GENMSG_04_03_BO		
Summary	Check that IUT is able to receive a secured GN Message if the signer_info header field is	
Summary	not encoded first	
Reference ETSI TS 103 097 [1], clause 7.3		
PICS Selection PICS_GN_SECURITY		
	Expected behaviour	
with		
the IUT being in the 'au	ithorized' state	
and the IUT current tim	e is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
the IUT is receiving a	a SecuredMessage (MSG_SEC_RCV_GENMSG_A)	
containing header		
indicating 'gene	ration_time'	
	ader_fields[1].type	
indicating 'gene	ration_location'	
	ader_fields[2].type	
indicating 'its_a		
	ader_fields[3].type	
indicating 'signe		
-	g other header fields	
then		
the IUT discards the	SecuredMessage	

TP ld	TP_SEC_ITSS_RCV_GENMSG_04_04_BO	
Summary	Check that IUT discards a secured GN Message if the message contains more than one	
Summary	header field of type 'generation_time'	
eference ETSI TS 103 097 [1], clause 7.3		
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		
5	SecuredMessage (MSG_SEC_RCV_GENMSG_A)	
containing header_fi		
indicating 'signer_		
containing header_fi	• • • •	
indicating 'generat		
and containing head		
indicating 'generat		
and containing head		
indicating 'generation		
and containing head	er_fields[4].type	
indicating 'its_aid'	they been devided	
and not containing o	ther neader lields	
then		

the IUT	discards a	SecuredMessage	

TP ld	TP_SEC_ITSS_RCV_GENMSG_04_05_BO	
Summony	Check that IUT discards a secured GN Message if the message does not contain the	
Summary	header field of type 'generation_time'	
Reference	ETSI TS 103 097 [1], clause 7.3	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'a	authorized' state	
	me is inside the time validity period of CERT_TS_A_AT	
ensure that	··· – – – –	
when		
the IUT is receiving	a SecuredMessage (MSG_SEC_RCV_GENMSG_A)	
containing head	<b>, , , , , , , , , ,</b>	
indicating 'sig		
	neader_fields[1].type	
	neration_location'	
	neader_fields[2].type	
indicating 'its_	• • • •	
and not containing other header fields		
then		
the IUT discards a		

TP ld	TP_SEC_ITSS_RCV_GENMSG_04_06_BO
Summary	Check that IUT discards a Secured GN Message if the message contains more than one
Summary	header field of type 'its_aid'
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
and the IUT curren	t time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receive	ing a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
	ader_fields[0].type
indicating 's	
and containing	header_fields[1].type
	jeneration_time'
	a header_fields[2].type
	jeneration_location'
	a header_fields[3]
containing t	ype
indicating	
containing i	
indicating	AID BEACON'
and containing	header_fields[4]
containing t	ype
indicating	its_aid'
containing i	
	AID_BEACON'
	ning other header fields
then	с С
the IUT discards	a SecuredMessage
	¥
rp Id	TP_SEC_ITSS_RCV_GENMSG_04_06a_BO
Summary	Check that IUT discards a secured GN Message if the message does not contain the
-	header field of type 'its_aid'
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour

the IUT being in the 'authorized' state and the IUT current time is inside the time validity period of CERT\_TS\_A\_AT ensure that

when

the IUT is receiving a SecuredMessage (MSG\_SEC\_RCV\_GENMSG\_A) containing header\_fields[0].type indicating 'signer\_info' and containing header\_fields[1].type indicating 'generation\_time' and containing header\_fields[2].type indicating 'generation\_location' and not containing other header fields then

the IUT discards a SecuredMessage

TP ld	TP_SEC_ITSS_RCV_GENMSG_04_07_BO	
Summary	Check that IUT discards a secured GN Message if the message contains more than one	
	header field of type 'generation_location'	
eference ETSI TS 103 097 [1], clause 7.3		
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'aut	horized' state	
and the IUT current time	e is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
the IUT is receiving a	SecuredMessage (MSG_SEC_RCV_GENMSG_A)	
containing header_		
indicating 'signe		
and containing hea		
indicating 'gener		
and containing hea		
indicating 'gener		
and containing hea	• • • •	
indicating 'gener		
and containing header_fields['its_aid']		
indicating 'AID_E		
	other header fields	
then		

the IUT	discards a	a SecuredMessa	age

TP ld	TP_SEC_ITSS_RCV_GENMSG_04_08_BO	
Summory	Check that IUT discards a secured GN Message if the header_fields contains no element o	
Summary	header field of type 'generation_location'	
Reference	ETSI TS 103 097 [1], clause 7.3	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	'authorized' state	
and the IUT current	time is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
the IUT is receivin	g a SecuredMessage (MSG_SEC_RCV_GENMSG_A)	
containing head	Jer_fields[0].type	
indicating 'sig	gner_info'	
	header_fields[1].type	
indicating 'ge	eneration_time'	
	header_fields['its_aid']	
indicating 'AID_BEACON'		
and not containing other header fields		
then		
	a SecuredMessage	

TP ld	TP_SEC_ITSS_RCV_GENMSG_04_09_BO	
Summary	Check that IUT is able to receive a Secured GN Beacon if the header fields are not in the	
	ascending order according to the numbering of the enumeration.	
Reference	ETSI TS 103 097 [1], clause 7.3	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	'authorized' state	
and the IUT current	time is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
	g a SecuredMessage (MSG_SEC_RCV_GENMSG_A)	
	ler_fields[0].type	
indicating 'sig		
	header_fields[1].type	
indicating 'its		
and containing header_fields[2].type		
indicating 'generation_time'		
and containing header_fields[3].type		
•	neration_location'	
then		
the IUT discards t	he SecuredMessage	

TP ld	TP_SEC_ITSS_RCV_GENMSG_04_11_BV
Summary	Check that IUT accepts a GN Secured Message containing optional header field of type
	'expiry_time'
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
	ng a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
	der_fields[0].type
indicating 'si	
containing si	
	certificate
	ng CERT_TS_A_AT
	header_fields[1]
containing ty	
	'generation_time'
	eneration_time
	TIME_1 inside the validity period of CERT_TS_A_AT
	header_fields[2]
containing ty	
•	'expiration'
containing ex	
	TIME_2 (TIME_2 > CURRENT_TIME)
	header_fields[3].type
	eneration_location'
	header_fields['its_aid']
	D_BEACON'
	ing other header fields
then	a Sacurad Massaga
	a SecuredMessage

TP ld	TP_SEC_ITSS_RCV_GENMSG_04_12_BV
Summary	Check that IUT accepts the Secured GN Message containing additional non-standard
	HeaderField
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in th	e 'authorized' state
and the IUT curren	t time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
	ing a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
	ader_fields[0].type
indicating 's	
	g header_fields[1].type
	generation_time'
	g header_fields[2].type
	generation_location'
indicating 'i	g header_fields[3].type
	g header_fields[4]
containing	
•	
indicating non-standard header field type (1000) and containing other_header	
indicating non-empty data	
	ining other header fields
then	<b>U</b>
the IUT accepts	the SecuredMessage

TP ld	TP_SEC_ITSS_RCV_GENMSG_04_13_BV		
	Check that ITS-S accepts a Secured GN Message containing header fields		
Summary	'encryption_parameters' and 'recipient_info'		
Reference	ETSI TS 103 097 [1], clause 7.3		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
	norized' state with CERT_IUT_A_AT		
	is inside the time validity period of CERT_TS_A_AT		
ensure that			
when			
the IUT is receiving a	SecuredMessage (MSG_SEC_RCV_GENMSG_A)		
containing header_f			
indicating 'signer			
and containing head	Jer_fields[1].type		
indicating 'genera			
and containing head	der_fields[2].type		
indicating 'genera			
	and containing header_fields[3].type		
indicating 'its_aid			
and containing header_fields[4]			
	containing type		
	indicating encryption_parameters		
and containing er			
	containing symm_algorithm		
indicating 'aes_128_ccm'			
and containing nonce			
and containing header_fields[5]			
containing type			
indicating 'recipient_info'			
and containing recipients			
containing recipients[0]			
containing cert_id			
referencing to CERT_IUT_A_AT			
and containing pk_encryption indicating 'ecies_nistp256'			
and containing enc_key and not containing other header fields			
then			
the IUT accepts the Se	anessaMharusa		
	scureumessaye		

# 5.3.4.4 Check signer info

TP ld	TP_SEC_ITSS_RCV_GENMSG_05_01_BO	
Summary	Check that IUT discards a secured GN Beacon if the header_fields contains a signer of type	
	'self'	
Reference	ETSI TS 103 097 [1], clause 7.3	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	e 'authorized' state	
and the IUT curren	t time is inside the time validity period of CERT_TS_A_AT	
ensure that	ensure that	
when		
the IUT is receiv	ing a SecuredMessage (MSG_SEC_RCV_GENMSG_A)	
containing hea	ader_fields['signer_info']	
containing signer.type		
indicating 'self'		
then	-	
the IUT discards	the IUT discards a SecuredMessage	

TP ld	TP_SEC_ITSS_RCV_GENMSG_05_02_BO	
Summary	Check that IUT discards a secured GN Beacon if the header_fields contains a signer of type	
Summary	certificate_digest_with_other_algorithm	
Reference	ETSI TS 103 097 [1], clause 7.3	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'a	uthorized' state	
and the IUT current tim	and the IUT current time is inside the time validity period of CERT_TS_A_AT	
ensure that		
when		
•	a SecuredMessage (MSG_SEC_RCV_GENMSG_A)	
	containing header_fields['signer_info']	
containing signer.type		
indicating 'certificate_digest_with_other_algorithm'		
then		
the IUT discards a SecuredMessage		

TP ld	TP_SEC_ITSS_RCV_GENMSG_05_03_BO
Summary	Check that IUT discards a secured GN Beacon if the header_fields contains a signer of type
	'certificate_chain'
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with the IUT being in the and the IUT curren	e 'authorized' state t time is inside the time validity period of CERT_TS_A_AT
ensure that when	
containing hea containing	ing a SecuredMessage (MSG_SEC_RCV_GENMSG_A) ader_fields['signer_info'] signer.type g 'certificate_chain'
then	
the IUT discards	a SecuredMessage

TP Id	TP SEC ITSS RCV GENMSG 05 04 BO
Summary	
	Check that IUT discards a Secured Messageif the header_fields contains a signer info of
	unknown or reserved type
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	authorized' state
and the IUT current	time is inside the time validity period of CERT TS A AT
ensure that	
when	
	ng a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
	der_fields['signer_info']
containing s	
•	X_UNKNOWN_SIGNERINFO_TYPE
then	
the IUT discards	a SecuredMessage
NOTE: Values to b	e used as X_UNKNOWN_SIGNERINFO_TYPE are 5, 239, 240 and 255.

TP ld	TP SEC ITSS RCV GENMSG 06 01 BO
Summary	Check that IUT discards a secured GN Message containing generation_time before the
	message signing certificate validity period
Reference	ETSI TS 103 097 [1], clauses 5.4 and 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivi	ng a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
containing hea	der_fields['signer_info']
containing	g certificate (CERT_TS_MSG_06_01_BO_AT)
contain	ing validity_restrictions['time_start_and_end']
	aining start_validity
	dicating START_VALIDITY_AT
	containing end_validity
	dicating END_VALIDITY_AT
	header_fields ['generation_time']
	eneration_time
•	GEN_TIME < START_VALIDITY_AT
then	
the IUT discards	the message

# 5.3.4.5 Check generation time

TP ld	TP_SEC_ITSS_RCV_GENMSG_06_02_BO
-	Check that IUT discards the secured GN Message containing generation_time after the
Summary	message signing certificate validity period
Reference	ETSI TS 103 097 [1], clauses 5.4 and 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'auth	
and the IUT current time	is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receiving a	SecuredMessage (MSG_SEC_RCV_GENMSG_A)
containing header_f	iields['signer_info']
containing cert	ificate (CERT_TS_MSG_06_02_BO_AT)
containing v	alidity_restrictions['time_start_and_end']
containing	g start_validity
indicati	ng START_VALIDITY_AT
and conta	ining end_validity
indicati	ng END_VALIDITY_AT
and containing head	der_fields ['generation_time']
containing genera	
	I_TIME > END_VALIDITY_AT
then	
the IUT discards the m	nessage

#### 5.3.4.6 Check its\_aid

TP ld	TP SEC ITSS RCV GENMSG 07 01 BO
Summary	Check that IUT discards SecuredMessage when its_aid value is undefined
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
ensure that when the IUT is receivin containing hea indicating 'A	'authorized' state time is inside the time validity period of CERT_TS_A_AT ng a SecuredMessage (MSG_SEC_RCV_GENMSG_A) der_fields['its_aid'] ID_UNDEFINED'
then the IUT discards	the message

121

# 5.3.4.7 Check generation location

TP ld	TP_SEC_ITSS_RCV_GENMSG_08_01_BO
Summary	Check that IUT discards Secured GN Message if the HeaderField generation_location is
	outside of the circular validity region of the signing certificate
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_B_AT
and the IUT current	location is inside the validiti region of CERT_TS_B_AT
ensure that	-
when	
the IUT is receiving	ng a SecuredMessage (MSG_SEC_RCV_GENMSG_B)
containing hea	der_fields ['signer_info']
containing c	ertificate (CERT_TS_B_AT)
containing	validity_restrictions ['region']
contain	ing region
conta	aining region_type
ind	dicating 'circle'
and	containing circular_region
ind	dicating REGION
and containing	header_fields ['generation_location']
indicating lo	cation outside of the REGION
then	
the IUT discards	the message

ETSI

TP ld	TP_SEC_ITSS_RCV_GENMSG_08_02_BO
Summary	Check that IUT discards Secured GN Message if the HeaderField generation_location is
Summary	outside of the rectangular validity region of the signing certificate
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY AND PICS_USE_RECTANGULAR_REGION
	Expected behaviour
with	
the IUT being in the 'author	prized' state
and the IUT current time i	s inside the time validity period of CERT_TS_C_AT
and the IUT current location	on is inside the validiti region of CERT_TS_C_AT
ensure that	
when	
	ecuredMessage (MSG_SEC_RCV_GENMSG_C)
containing header_fi	
•	ate (CERT_TS_C_AT)
	ity_restrictions ['region']
containing re	
	region_type
	g 'rectangle'
	ning rectangular_regions
	g REGION
	er_fields ['generation_location']
	outside of the REGION
then	
the IUT discards the me	essaye

TP ld TP\_SEC\_ITSS\_RCV\_GENMSG\_08\_03\_BO Check that IUT discards Secured GN Message if the optional HeaderField Summary generation\_location is outside of the polygonal validity region of the signing certificate Reference ETSI TS 103 097 [1], clause 7.3 **PICS Selection** PICS\_GN\_SECURITY AND PICS\_USE\_POLYGONAL\_REGION Expected behaviour with the IUT being in the 'authorized' state and the IUT current time is inside the time validity period of CERT\_TS\_D\_AT and the IUT current location is inside the validiti region of CERT\_TS\_D\_AT ensure that when the IUT is receiving a SecuredMessage (MSG\_SEC\_RCV\_GENMSG\_D) containing header\_fields ['signer\_info'] containing certificate (CERT\_TS\_D\_AT) containing validity\_restrictions ['region'] containing region containing region\_type indicating 'polygon' and containing polygonal\_region indicating REGION and containing header\_fields ['generation\_location'] indicating location outside of the REGION then the IUT discards the message

TP ld	TP_SEC_ITSS_RCV_GENMSG_08_04_BO
Summary	Check that IUT discards Secured GN Message if the optional HeaderField
Summary	generation_location is outside of the identified validity region of the signing certificate
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION
	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_E_AT
and the IUT current locat	ion is inside the validiti region of CERT_TS_E_AT
ensure that	
when	
	SecuredMessage (MSG_SEC_RCV_GENMSG_E)
containing header_f	
•	ate (CERT_TS_E_AT)
	lity_restrictions ['region']
containing re	
	region_type
	ng 'id_region'
	ining identified_region
	ng REGION
	ler_fields ['generation_location']
•	outside of the REGION
then	
the IUT discards the m	essage

#### 5.3.4.8 Check Payload

TP ld	TP_SEC_ITSS_RCV_GENMSG_09_02_BO
Summary	Check that IUT discards the Secured GN Message containing empty payload of type signed
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
ensure that when	ime is inside the time validity period of CERT_TS_A_AT g a SecuredMessage (MSG_SEC_RCV_GENMSG_A) bad_field be signed' g data ength 0

TP ld	TP_SEC_ITSS_RCV_GENMSG_09_03_BO
Summary	Check that IUT discards the Secured GN Message containing payload element of type
	'unsecured'
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	a 'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivi	ng a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
containing pay	rload_field
containing t	уре
indicating	, 'unsecured'
and contain	ing data
indicating	length > 0
then	
the IUT discards	the message

TP ld	TP_SEC_ITSS_RCV_GENMSG_09_04_BO
Summary	Check that IUT discards the Secured GN Message containing payload element of type
	'encrypted'
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receiving	ng a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
containing pay	load_field
containing ty	уре
indicating	'encrypted'
and containi	ng data
indicating	length > 0
then	
the IUT discards	the message

TP ld	TP_SEC_ITSS_RCV_GENMSG_09_05_BV
Summers	Check that IUT accepts a well-formed Secured GN Message containing payload of type
Summary	signed_external
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
the IUT being in the and the IUT current ensure that when	e 'authorized' state time is inside the time validity period of CERT_TS_A_AT
containing pay containing ty	
then	-
the IUT accepts t	the message

TP ld	TP_SEC_ITSS_RCV_GENMSG_09_06_BV
Summary	Check that IUT accepts a well-formed Secured GN Message containing payload of type
Summary	signed_and_encrypted
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'aut	horized' 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	SecuredMessage (MSG_SEC_RCV_GENMSG_A)
containing payload	_field
containing type	
indicating 'sigr	ned_and_encrypted'
then	
the IUT accepts the m	nessage

# 5.3.4.9 Check presence of trailer field

TP ld	TP_SEC_ITSS_RCV_GENMSG_10_01_BO
Summary	Check that IUT discards the Secured GN Message if the message does not contain the
	trailer field of type 'signature'
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
and the IUT curren	t time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receiv	ing a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
containing tra	ler_fields
not contain	ing trailer_fields['signature']
then	
the IUT discards	the message

TP ld	TP_SEC_ITSS_RCV_GENMSG_10_02_BO
Summary	Check that IUT discards the Secured GN Message containing more than one instance of
Summary	TrailerField of type 'signature'
Reference	ETSI TS 103 097 [1], clause 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'auth	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 S	SecuredMessage (MSG_SEC_RCV_DENM_A)
containing trailer_fie	lds[0]
containing type	
indicating signa	ature'
and containing traile	
containing type	
indicating signa	ature'
then	
the IUT discards the m	essage

# 5.3.4.10 Check signature

TP ld	TP_SEC_ITSS_RCV_GENMSG_11_01_BO
	Check that the IUT discards Secured GN Message containing signature that is not verified
Summary	using the verification key from the certificate contained in the message's signer info
Reference	ETSI TS 103 097 [1], clauses 4.2.2 and 7.3
PICS Selection	PICS GN SECURITY
	Expected behaviour
with	
the IUT being in the 'auth	orized' state
J	is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receiving a S	SecuredMessage (MSG_SEC_RCV_GENMSG_A)
containing header_f	
containing signer	
	ificate (CERT_TS_A_AT)
	ubject_attributes['verification key']
	y key (KEY)
and containing traile	r_fields[0]
containing type	
indicating 'sign	
containing signate	
NOT verifiable	using KE f
the IUT discards the m	0052300
	essaye
TP ld	TP_SEC_ITSS_RCV_GENMSG_11_02_BO
Summany	Check that IUT discards the Secured Message if the message contains trailer field of type
Summary	'signature' with reserved public key algorythms
Reference	ETSI TS 103 097 [1], clauses 4.2.2 and 7.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'auth	orized' state
	is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
	SecuredMessage (MSG_SEC_RCV_GENMSG_A)
containing trailer_fie	
	ance of type TrailerField
containing type	
indicating 'si	
-	
8 -	RESERVED_PK_ALGORYTHM
then	
	000000
the IUT discards the m NOTE: Values to be prov	iessage vided as X_RESERVED_PK_ALGORYTHM are: 240, 255.

TP ld	TP SEC ITSS RCV GENMSG 12 01 BO
Summary	Check that IUT discards a Secured GN Message if the signer certificate of the message
	contains the subject type 'enrolment_credential'
Reference	ETSI TS 103 097 [1], clause 6.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'a	uthorized' state
and the IUT current tim	ne is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receiving	a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
containing heade	r_fields ['signer_info']
containing sign	er
containing ty	/pe
indicating	'certificate'
5	ertificate (CERT_TS_A_EC)
	subject_info.subject_type
	ng 'enrolment_credentials'
then	
the IUT discards the	message

# 5.3.4.11 Check signing certificate type

P ld	TP SEC ITSS RCV GENMSG 12 02 BO
	Check that IUT discards a Secured GN Message if the signer certificate of the message
Summary	
	contains the subject type 'authorization_authority'
Reference	ETSI TS 103 097 [1], clause 6.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
vith	
the IUT being in the 'auth	norized' state
Ū	is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
	SecuredMessage (MSG_SEC_RCV_GENMSG_A)
containing header_f	<b>o</b> ( ,
•	
containing signer	
containing type	
indicating 'ce	
containing cert	ificate (CERT_TS_A_AA)
containing s	ubject_info.subject_type
indicating	'authorization_authority'
then	•
the IUT discards the m	0000000

TP ld	TP_SEC_ITSS_RCV_GENMSG_12_03_BO
6	Check that IUT discards a Secured GN Message if the signer certificate of the message
Summary	contains the subject type 'enrolment_authority'
Reference	ETSI TS 103 097 [1], clause 6.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivir	ng a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
containing hea	der_fields ['signer_info']
containing si	gner
containing	I type
indicati	ng 'certificate'
containing	certificate (CERT_TS_A_EA)
contain	ing subject_info.subject_type
indic	ating 'enrolment_authority'
then	
the IUT discards	he message

TP ld	TP_SEC_ITSS_RCV_GENMSG_12_04_BO
6	Check that IUT discards a Secured GN Message if the signer certificate of the message
Summary	contains the subject type 'root_ca'
Reference	ETSI TS 103 097 [1], clause 6.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_A_AT
ensure that	
when	
the IUT is receivi	ng a SecuredMessage (MSG_SEC_RCV_GENMSG_A)
containing hea	ider_fields ['signer_info']
containing s	igner
containing	j type
indicati	ing 'certificate'
containing	g certificate (CERT_TS_ROOT)
contain	ing subject_info.subject_type
indic	ating 'root_ca'
then	
the IUT discards	the message

TP ld	TP_SEC_ITSS_RCV_GENMSG_13_01_BO
Summary	Check that IUT discards secured message signed with the not yet valid certificate
Reference	ETSI TS 103 097 [1], clause 6.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'auth	orized' state
and the IUT current time	is before the time validity period of CERT_TS_MSG_13_01_BO_AT
ensure that	
when	
the IUT is receiving a S	SecuredMessage (MSG_SEC_RCV_GENMSG_A)
	ields['signer_info'].signer
containing certific	ate (CERT_TS_MSG_13_01_BO_AT)
containing valid	dity_restrictions['time_start_and_end']
containing st	
	START_VALIDITY_AT > CURRENT_TIME
	ng end_validity
indicating	END_VALIDITY_AT > START_VALIDITY_AT
then	
the IUT discards the m	essage

# 5.3.4.12 Check certificate validity

TP ld	TP_SEC_ITSS_RCV_GENMSG_13_02_BO
Summary	Check that IUT discards secured message signed with the expired certificate
Reference	ETSI TS 103 097 [1], clause 6.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'auth	orized' state
and the IUT current time i	is before the time validity period of CERT_TS_MSG_13_02_BO_AT
ensure that	
when	
the IUT is receiving a S	SecuredMessage (MSG_SEC_RCV_GENMSG_A)
containing header_fi	ields['signer_info'].signer
containing certifica	ate (CERT_TS_MSG_13_02_BO_AT)
containing valid	lity_restrictions['time_start_and_end']
containing st	art_validity
indicating	START_VALIDITY_AT < CURRENT_TIME
and containin	ng end_validity
indicating	END_VALIDITY_AT < CURRENT_TIME
then	
the IUT discards the m	essage

TP ld	TP_SEC_ITSS_RCV_GENMSG_13_03_BO
Summary	Check that IUT discards secured message when IUT location is outside the circular validity
	restriction of the signing certificate
Reference	ETSI TS 103 097 [1], clause 6.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
and the IUT current	time is inside the validity period of CERT_TS_MSG_13_03_BO_AT
and the IUT current	location is set to CURRENT_IUT_LOCATION
ensure that	
when	
	ng a SecuredMessage (MSG_SEC_RCV_GENMSG_B)
	ider_fields['signer_info'].signer
	vertificate (CERT_TS_MSG_13_03_BO_AT)
	g validity_restrictions['region']
	ning region
	aining region_type
	dicating 'circle'
	containing circular_region
in	
	not containing the CURRENT_IUT_LOCATION
then	
the IUT discards	ine message

TP ld	TP_SEC_ITSS_RCV_GENMSG_13_04_BO
Summary	Check that IUT discards secured message when IUT location is outside the rectangular
	validity restriction of the signing certificate
Reference	ETSI TS 103 097 [1], clause 6.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the validity period of CERT_TS_MSG_13_04_BO_AT
and the IUT current	location is set to CURRENT_IUT_LOCATION
ensure that	
when	
	ng a SecuredMessage (MSG_SEC_RCV_GENMSG_C)
	der_fields['signer_info'].signer
•	ertificate (CERT_TS_MSG_13_04_BO_AT)
	y validity_restrictions['region']
	ing region
	aining region_type
	dicating 'rectangle'
	containing rectangular_regions
IN	dicating REGION
then	not containing the CURRENT_IUT_LOCATION
then	the measure
the IUT discards	ne message

TP ld	TP_SEC_ITSS_RCV_GENMSG_13_05_BO
Cummon or a	Check that IUT discards secured message when IUT location is outside the polygonal
Summary	validity restriction of the signing certificate
Reference	ETSI TS 103 097 [1], clause 6.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
and the IUT curren	t time is inside the validity period of CERT_TS_MSG_13_05_BO_AT
and the IUT curren	t location is set to CURRENT_IUT_LOCATION
ensure that	
when	
	ring a SecuredMessage (MSG_SEC_RCV_GENMSG_D)
	ader_fields['signer_info'].signer
	certificate (CERT_TS_MSG_13_05_BO_AT)
	ng validity_restrictions['region']
	ning region
	taining region_type
	ndicating 'polygon'
	l containing polygonal_region
ir	ndicating REGION
	not containing the CURRENT_IUT_LOCATION
then	
the IUT discards	s the message
TP ld	TP_SEC_ITSS_RCV_GENMSG_13_06_BO
Summariy	Check that IUT discards secured message when IUT location is outside the identified
Summary	validity restriction of the signing certificate
Reference	ETSI TS 103 097 [1], clause 6.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
and the IUT curren	t time is inside the validity period of CERT_TS_MSG_13_06_BO_AT
	t location is set to CURRENT_IUT_LOCATION
ensure that	
when	
the IUT is receiv	ring a SecuredMessage (MSG_SEC_RCV_GENMSG_E)
containing has	ader fieldel'signer info'l signer

ensure that
when
the IUT is receiving a SecuredMessage (MSG_SEC_RCV_GENMSG_E)
containing header_fields['signer_info'].signer
containing certificate (CERT_TS_MSG_13_06_BO_AT)
containing validity_restrictions['region']
containing region
containing region_type
indicating 'id'
and containing id_region
indicating REGION
not containing the CURRENT_IUT_LOCATION
then
the IUT discards the message

#### 5.3.5 Profiles for certificates

#### Check that certificate version is 2 5.3.5.1

TP ld	TP_SEC_ITSS_RCV_CERT_01_01_BO
Summary	Check that IUT discards the AT certificate with version 3
Reference	ETSI TS 103 097 [1], clauses 6.1 and 7.4.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'auth	
	is inside the time validity period of CERT_TS_01_01_BO_AT
ensure that	• · · · ·
when the IUT is receiving	
containing header_fiel	ds ['signer_info']
containing signer	
containing type	ficatel
indicating 'certi	
containing vers	ertificate (CERT_TS_01_01_BO_AT)
indicating '3'	
then	
the IUT discards the m	ancesed
TP ld	TP_SEC_ITSS_RCV_CERT_01_02_BO
Summary	Check that IUT discards the AT certificate with version 1
Reference	ETSI TS 103 097 [1], clauses 6.1 and 7.4.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'auth	iorized' state
and the IUT current time	is inside the time validity period of CERT_TS_01_02_BO_AT
ensure that	
when the IUT is receiving	
containing header_fiel	ds ['signer_info']
containing signer	
containing type	
indicating 'certi	
	ertificate (CERT_TS_01_02_BO_AT)
containing vers	
indicating '1'	

then

the IUT discards the message

	-	
TP ld	TP_SEC_ITSS_RCV_CERT_01_03_BO	
Summary	Check that IUT discards the AA certificate with version 3	
Reference	ETSI TS 103 097 [1], clauses 6.1 and 7.4.1	
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_01_03_BO_AT	
ensure that		
when the IUT is receiving		
containing header_field	ds ['signer_info']	
containing signer		
containing type	<b>.</b>	
indicating 'certit		
	rtificates[0] (CERT_TS_01_03_BO_AA)	
containing vers		
indicating '3'		
and containing certificates[1] (CERT_TS_01_03_BO_AT)		
containing signer_info.type		
indicating 'certificate_digest_with_sha256'		
and containing signer_info.digest		
	o CERT_TS_01_03_BO_AA	
then		
the IUT discards the m	essage	

TP ld	TP_SEC_ITSS_RCV_CERT_01_04_BO
Summary	Check that IUT discards the AA certificate with version 1
Reference	ETSI TS 103 097 [1], clauses 6.1 and 7.4.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
ensure that when the IUT is receiving containing header_field containing signer containing type indicating 'certif containing certifica containing versi indicating '1' and containing cer	is inside the time validity period of CERT_TS_01_04_BO_AT a SecuredMessage ds ['signer_info'] ficate_chain' ates[0] (CERT_TS_01_04_BO_AA) ion rtificates[1] (CERT_TS_01_04_BO_AT) er_info.digest o CERT_TS_01_04_BO_AA

5.3.5.2	Check that enrolment certificate is not used for sign other certificates
---------	--

ERT_02_01_BO
a SecuredMessage if the issuer certificate of the authorization
s the subject type 'enrolment_credential'
ause 6.3
pected behaviour
period of CERT_TS_02_01_BO_AT
D1_BO_AT)
/
a256'
A_EC)
be
ERT_02_02_BO
a SecuredMessage if the issuer certificate of the authorization
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential'
a SecuredMessage if the issuer certificate of the authorization
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential' ause 6.3
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential'
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential' ause 6.3
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential' ause 6.3 pected behaviour
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential' ause 6.3
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential' ause 6.3 pected behaviour
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential' ause 6.3 pected behaviour
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential' ause 6.3 pected behaviour
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential' ause 6.3 pected behaviour
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential' ause 6.3 pected behaviour
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential' ause 6.3 pected behaviour period of CERT_TS_02_02_BO_AT
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential' ause 6.3 pected behaviour
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential' ause 6.3 pected behaviour period of CERT_TS_02_02_BO_AT
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential' ause 6.3 pected behaviour period of CERT_TS_02_02_BO_AT D2_02_BO_AA)
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential' ause 6.3 pected behaviour period of CERT_TS_02_02_BO_AT D2_02_BO_AA) A_EC
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential' ause 6.3 pected behaviour period of CERT_TS_02_02_BO_AT D2_02_BO_AA) A_EC De
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential' ause 6.3 pected behaviour period of CERT_TS_02_02_BO_AT D2_02_BO_AA) A_EC D2_02_BO_AT)
a SecuredMessage if the issuer certificate of the authorization ains the subject type 'enrolment_credential' ause 6.3 pected behaviour period of CERT_TS_02_02_BO_AT D2_02_BO_AA) A_EC pe

then the IUT discards the message

TP ld	TP_SEC_ITSS_RCV_CERT_02_03_BO
Summary	Check that IUT discards a SecuredMessage if the issuer certificate of the authorization
	ticket certificate contains the subject type 'enrolment_authority'
Reference	ETSI TS 103 097 [1], clause 6.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current t	time is inside the time validity period of CERT_TS_02_03_BO_AT
ensure that	
when the IUT is rece	iving a SecuredMessage
containing header	_fields ['signer_info']
containing signe	٦٤
containing ty	pe
indicating '	certificate'
	ng certificate (CERT_TS_02_03_BO_AT)
containing	signer_info.type
	ng 'certificate_digest_with_sha256'
and contai	ning signer_info.digest
	sing to certificate (CERT_TS_A_EA)
	ining subject_info.subject_type
ind	icating 'enrolment_authority'
then	
the IUT discards the	ne message

TP ld	TP_SEC_ITSS_RCV_CERT_02_04_BO
Summary	Check that IUT discards a SecuredMessage if the issuer certificate of the authorization
	authority certificate contains the subject type 'enrolment_authority'
Reference	ETSI TS 103 097 [1], clause 6.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_02_04_BO_AT
ensure that	
when the IUT is rec	eiving a SecuredMessage
containing heade	r_fields ['signer_info']
containing sigr	ier
containing t	уре
	'certificate_chain'
	ing certificates[0] (CERT_TS_02_04_BO_AA)
	g signer_info.digest
	cing to certificate CERT_TS_A_EA
	aining subject_info.subject_type
	dicating 'enrolment_authority'
	ing certificates[1] (CERT_TS_02_04_BO_AT)
	g signer_info.digest
	cing to CERT_TS_02_04_BO_AA
then	
the IUT discards	the message

TP ld	TP_SEC_ITSS_RCV_CERT_03_01_BO
Summary	Check that IUT discards a SecuredMessage if the issuer certificate of the authorization
	ticket certificate contains the subject type 'authorization_ticket'
Reference	ETSI TS 103 097 [1], clause 6.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_03_01_BO_AT
ensure that	
when the IUT is rec	eiving a SecuredMessage
	r_fields ['signer_info'].signer
containing cer	tificate (CERT_TS_03_01_BO_AT)
containing s	igner_info.digest
referencir	ng to CERT_TS_03_BO_CA
contair	ning subject_info.subject_type
indic	cating 'authorization_ticket'
then	
the IUT discards	the message

TP ld	TP_SEC_ITSS_RCV_CERT_03_02_BO
Summary	Check that IUT discards a SecuredMessage if the issuer certificate of the authorization
	authority certificate contains the subject type 'authorization_ticket'
Reference	ETSI TS 103 097 [1], clause 6.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_03_02_BO_AT
ensure that	
when the IUT is rec	eiving a SecuredMessage
containing heade	r_fields ['signer_info']
containing sigr	ner
containing t	уре
indicating	'certificate_chain'
	ng certificates[0] (CERT_TS_03_02_BO_AA)
	g signer_info.digest
	cing to CERT_TS_03_BO_CA
	aining subject_info.subject_type
in	dicating 'authorization_ticket'
and contain	ng certificates[1] (CERT_TS_03_02_BO_AT)
	g signer_info.digest
referencir	ng to CERT_TS_03_02_BO_AA
then	
the IUT discards	the message

onois in onois indiate orginal with other recontinuate to not according	5.3.5.4	Check that AA certificate signed with other AA certificate is not accepted
---	---------	--

TP ld	TP_SEC_ITSS_RCV_CERT_04_01_BO
Summary	Check that IUT discards a SecuredMessage if the issuer certificate of the AA certificate
	contains the subject type 'authorization_authority'
Reference	ETSI TS 103 097 [1], clause 6.3
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'a	authorized' state
and the IUT current til	me is inside the time validity period of CERT_TS_04_01_BO_AT
ensure that	
when the IUT is received	ving a SecuredMessage
containing header_	fields ['signer_info']
containing signe	r
containing typ	e
indicating 'c	certificate_chain'
and containing	g certificates[0] (CERT_TS_04_01_BO_AA)
containing signer_info.digest	
referencing to CERT_TS_A_AA	
and containing certificates[1] (CERT_TS_04_01_BO_AT)	
containing	signer_info.digest
	ng to CERT_TS_04_01_BO_AA
then	•
the IUT discards th	e message

# 5.3.5.5 Check the certificate signature

TP ld	TP_SEC_ITSS_RCV_CERT_05_01_BO
	Check that IUT discards the message when signing AT certificate has an invalid signature
Summary	
Reference	ETSI TS 103 097 [1], clauses 6.1 and 7.4.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'auth	norized' 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 SecuredMessage	
containing header_fields ['signer_info']	
containing signer	
containing type	
indicating 'certificate'	
and containing certificate (CERT_TS_A_AT)	
containing signer_info.digest	
referencing to a CERT_TS_A_AA	
and containing signature	
NOT verifiable with CERT_TS_A_AA.subject_attributes['verification_key'].key	
then	
the IUT discards the m	nessage

TP ld	TP_SEC_ITSS_RCV_CERT_05_02_BO	
Summary	Check that IUT discards the message when the issuing AA certificate of the signing AT	
Summary	certificate has an invalid signature	
Reference	ETSI TS 103 097 [1], clauses 6.1 and 7.4.1	
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 SecuredMessage	
containing header_field	ds ['signer_info']	
containing signer		
containing type		
indicating 'certil	ficate_chain'	
and containing certificates[0] (CERT_TS_A_AA)		
containing signer_info.digest		
referencing to a CERT_ROOT		
	and containing signature	
NOT verifiable with CERT_ROOT.subject_attributes['verification_key'].key		
and containing certificates[1] (CERT_TS_A_AT)		
containing signer_info.digest		
•	o a CERT_TS_A_AA	
then		
the IUT discards the m	essage	

#### 5.3.5.6 Check circular region of subordinate certificate

TP ld	TP_SEC_ITSS_RCV_CERT_06_01_BV
Summary	Check that the IUT accepts a message when the signing certificate of this message contains
	the same circular region validity restriction as its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_06_01_BV_AT
and the IUT current	location is inside the CURCULAR_REGION_AA
ensure that	
	eiving a SecuredMessage
	r_fields ['signer_info']
containing sigr	
containing t	
	'certificate'
	ertificate (CERT_TS_06_01_BV_AT)
	g validity_restrictions['region']
	ing region_type
	ating 'circle'
	ing circular_region
	ating CURCULAR_REGION_AA
	g signer_info.digest
	cing to a CERT_TS_B_AA
	aining validity_restrictions['region']
CC	intaining region_type
-	indicating 'circle'
ar	nd containing circular_region
then	indicating CURCULAR_REGION_AA
	ha massaga
the IUT accepts t	ne nessaye

TP ld	TP_SEC_ITSS_RCV_CERT_06_02_BV
	Check that the IUT accepts a message when the signing certificate of this message contains
Summary	the circular region validity restriction which is fully inside in the circular region validity
	restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION
	Expected behaviour
with	
the IUT being in the	
	time is inside the time validity period of CERT_TS_06_02_BV_AT
	location is inside the CURCULAR_REGION_AT
ensure that	
	eiving a SecuredMessage
	er_fields ['signer_info']
containing sig	
containing t	
	'certificate'
	ing certificate (CERT_TS_06_02_BV_AT)
	g validity_restrictions['region']
	ning region_type cating 'circle'
	ntaining circular_region
	cating CURCULAR_REGION_AT
	aining signer_info.digest
	icing to a certificate CERT_TS_B_AA
	aining validity_restrictions['region']
	ontaining region_type
	indicating 'circle'
a	nd containing circular_region
-	indicating CURCULAR_REGION_AA
	fully covering CURCULAR_REGION_AT
then	
the IUT accepts	the message

TP ld	TP_SEC_ITSS_RCV_CERT_06_03_BV
	Check that the IUT accepts a message when the signing certificate of this message contains
Summary	the circular region validity restriction which is fully inside in the rectangular region validity
	restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION
	Expected behaviour
with	
the IUT being in the	
	time is inside the time validity period of CERT_TS_06_03_BV_AT
	location is inside the CURCULAR_REGION_AT
ensure that	
	eiving a SecuredMessage
	r_fields ['signer_info']
containing sigr	
containing ty	/pe 'certificate'
	ng certificate (CERT_TS_06_03_BV_AT)
	g validity_restrictions['region']
	ing region_type
	ating 'circle'
	ntaining circular_region
	ating CURCULAR_REGION_AT
	ining signer_info.digest
referen	cing to a certificate CERT_TS_C_AA
cont	aining validity_restrictions['region']
CC	ntaining region_type
	indicating 'rectangular'
ar	nd containing rectangular_region[0]
	indicating RECT_REGION_AA
the ene	fully covering CURCULAR_REGION_AT
then	
the IUT accepts t	ne message

TP ld	TP_SEC_ITSS_RCV_CERT_06_04_BV
	Check that the IUT accepts a message when the signing certificate of this message contains
Summary	the circular region validity restriction which is fully inside in the polygonal region validity
	restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION
	Expected behaviour
with	
the IUT being in the	
	time is inside the time validity period of CERT_TS_06_04_BV_AT
	location is inside the CURCULAR_REGION_AT
ensure that	
	eiving a SecuredMessage
	er_fields ['signer_info']
containing sig	
containing t	
	'certificate'
	ing certificate (CERT_TS_06_04_BV_AT)
	g validity_restrictions['region']
	ning region_type
	cating 'circle'
	ntaining circular_region ating CURCULAR_REGION_AT
	aining signer_info.digest
	incing to a certificate CERT_TS_D_AA
	aining validity_restrictions['region']
	ontaining region_type
	indicating 'polygon'
a	nd containing polygonal_region
	indicating POLYGON_REGION_AA
	fully covering CURCULAR_REGION_AT
then	
the IUT accepts	the message

TP ld	TP_SEC_ITSS_RCV_CERT_06_05_BV
	Check that the IUT accepts a message when the signing certificate of this message contains
Summary	the circular region validity restriction which is fully inside in the identified region validity
Summary	restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION
PICS Selection	PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION Expected behaviour
with	
the IUT being in the	'authorized' state
	time is inside the time validity period of CERT_TS_06_05_BV_AT
	location is inside the CURCULAR_REGION_AT
ensure that	
	eiving a SecuredMessage
	r_fields ['signer_info']
containing sign	
containing ty	
	'certificate'
	ertificate (CERT_TS_06_05_BV_AT)
	y validity_restrictions['region']
contain	ing region_type
indic	ating 'circle'
and cor	ntaining circular_region
	ating CURCULAR_REGION_AT
	ining signer_info.digest
	cing to a certificate CERT_TS_E_AA
containing validity_restrictions['region']	
	d containing region_type
indicating 'id'	
and containing id_region	
containing region_dictionary	
indicating 'iso_3166_1'	
and containing local_region	
	indicating 0
	and containing region_identifier
	indicating ID_REGION_AT fully covering CURCULAR_REGION_AT
then	
the IUT accepts the	he message

TP ld	TP_SEC_ITSS_RCV_CERT_06_06_BO
	Check that the IUT discards a message when the signing certificate of this message does
Summary	not contain the region validity restriction but its issuing certificate contains the circular region
	validity restriction
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_06_06_BO_AT
and the IUT current	location is inside the CURCULAR_REGION_AT
ensure that	
when the IUT is rec	eiving a SecuredMessage
containing heade	r_fields ['signer_info']
containing sign	
containing ty	ире
indicating	'certificate'
	ng certificate (CERT_TS_06_06_BO_AT)
	ining validity_restrictions['region']
	ining signer_info.digest
	cing to a CERT_TS_B_AA
	aining validity_restrictions['region']
CC	ntaining region_type
	indicating 'circle'
ar	nd containing circular_region
	indicating CURCULAR_REGION_AT
then	
the IUT discards	the message
TP ld	TP_SEC_ITSS_RCV_CERT_06_07_BO
	Check that the IUT discards a message when the signing certificate of this message
Summary	contains circular region validity restriction which is outside of the circular region validity
	restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION
	Expected behaviour
with	•
the IUT being in the	'authorized' state
	time is inside the time validity period of CERT_TS_06_07_BO_AT
	location is inside the CURCULAR_REGION_AT
ensure that	
when the IUT is rec	eiving a SecuredMessage
	r_fields ['signer_info']
containing sign	
containing ty	
	'certificate'
	ng certificate (CERT_TS_06_07_BO_AT)
	g validity_restrictions['region']
	ing region_type
	ating 'circle'
	ntaining circular_region
indicating CI BCI II AR REGION AT	

indicating CURCULAR\_REGION\_AT

and containing signer\_info.digest referencing to a CERT\_TS\_06\_07\_BO\_AA containing validity\_restrictions['region'] containing region\_type indicating 'circle' and containing circular\_region indicating CURCULAR\_REGION\_AA\_OUTSIDE not including CURCULAR\_REGION\_AT

then the IUT discards the message

TP ld	TP_SEC_ITSS_RCV_CERT_06_08_BO
	Check that the IUT discards a message when the signing certificate of this message
Summary	contains circular region validity restriction which is not fully covered by the the circular region
	validity restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_CIRCULAR_REGION
	Expected behaviour
with	
the IUT being in the	
and the IUT current	time is inside the time validity period of CERT_TS_06_08_BO_AT
	location is inside the CURCULAR_REGION_AT
ensure that	
	eiving a SecuredMessage
	r_fields ['signer_info']
containing sigr	
containing ty	
	'certificate'
	ing certificate (CERT_TS_06_08_BO_AT)
	g validity_restrictions['region']
	aining region_type
	dicating 'circle'
	containing circular_region
	dicating CURCULAR_REGION_AT
	aining signer_info.digest
	cing to a CERT_TS_06_08_BO_AA
	aining validity_restrictions['region']
CC	indianting region_type
	indicating 'circle'
ar	nd containing circular_region indicating CURCULAR_REGION_AA_INTERSECT
	including partially CURCULAR_REGION_AA
then	Including partially CORCOLAR_REGION_AT
the IUT discards	the message
	ano mododago

TP ld	TP_SEC_ITSS_RCV_CERT_07_01_BV
Summary	Check that the IUT accepts a message when the signing certificate of this message contains
	the same rectangular region validity restriction as its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_RECTANGULAR_REGION
	Expected behaviour
with	
the IUT being in the 'aut	horized' state
and the IUT current time	e is inside the time validity period of CERT_TS_07_01_BV_AT
and the IUT current loca	ition is inside the RECT_REGION_AA
ensure that	
when the IUT is receivin	g a SecuredMessage
containing header_fie	lds ['signer_info']
containing signer	
containing type	
indicating 'cer	
	ertificate (CERT_TS_07_01_BV_AT)
	idity_restrictions['region']
containing r	
	g 'rectangle'
	ning rectangular_region[0]
	g RECT_REGION_AA
	g signer_info.digest
	to a CERT_TS_C_AA
	g validity_restrictions['region']
	ning region_type
	cating 'rectangular'
	ontaining rectangular_region[0]
then	cating RECT_REGION_AA
	2000200
the IUT accepts the m	iessaye

# 5.3.5.7 Check rectangular region of subordinate certificate

TP ld	TP_SEC_ITSS_RCV_CERT_07_03_BV
	Check that the IUT accepts a message when the signing certificate of this message contains
Summary	the validity restriction with rectangular region which is fully inside in the rectangular region
-	validity restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_RECTANGULAR_REGION
	Expected behaviour
with	
the IUT being in the	
	time is inside the time validity period of CERT_TS_07_03_BV_AT
	location is inside the RECT_REGION_AT
ensure that	
	eiving a SecuredMessage
	r_fields ['signer_info']
containing sigr	
containing ty	
5	'certificate'
	ng certificate (CERT_TS_07_03_BV_AT) g validity_restrictions['region']
	ing region_type
	ating 'rectangle'
	ntaining rectangular_region[0]
	ating RECT_REGION_AT
	ining signer_info.digest
	cing to a certificate CERT_TS_C_AA
cont	aining validity_restrictions['region']
CC	ntaining region_type
	indicating 'rectangular'
ar	nd containing rectangular_region[0]
	indicating RECT_REGION_AA
4	fully covering RECT_REGION_AT
then	
the IUT accepts t	ne message

TP ld	TP_SEC_ITSS_RCV_CERT_07_04_BV
	Check that the IUT accepts a message when the signing certificate of this message contains
Summary	the rectangular region validity restriction which is fully inside in the polygonal region validity
<b>,</b>	restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_RECTANGULAR_REGION
	Expected behaviour
with	
the IUT being in the '	authorized' state
	me is inside the time validity period of CERT_TS_07_04_BV_AT
	ocation is inside the RECT_REGION_AT
ensure that	
	ving a SecuredMessage
	_fields ['signer_info']
containing signe	
containing typ	
indicating '	
	rtificate (CERT_TS_07_04_BV_AT) validity_restrictions['region']
	ig region_type
	ting 'rectangle'
	ig rectangular_region[0]
	ting RECT_REGION_AT
	signer_info.digest
	ng to a certificate CERT_TS_D_AA
	ning validity_restrictions['region']
	taining region_type
ir	ndicating 'polygon'
	taining polygonal_region
ir	ndicating POLYGON_REGION_AA
	fully covering RECT_REGION_AT
then	
the IUT accepts the	e message

TP ld	TP_SEC_ITSS_RCV_CERT_07_05_BV
	Check that the IUT accepts a message when the signing certificate of this message contain
Summary	the rectangular region validity restriction which is fully inside in the identified region validity
	restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_RECTANGULAR_REGION
	Expected behaviour
with	
the IUT being in the	'authorized' state
	time is inside the time validity period of CERT_TS_07_05_BV_AT
and the IUT current	location is inside the RECT_REGION_AT
ensure that	
when the IUT is rece	iving a SecuredMessage
	_fields ['signer_info']
containing sign	er
containing ty	
indicating	'certificate'
	ng certificate (CERT_TS_07_05_BV_AT)
	validity_restrictions['region']
	ng region_type
	ating 'rectangle'
	taining rectangular_region[0]
	ating RECT_REGION_AT
	ning signer_info.digest
	cing to a certificate CERT_TS_E_AA
	ining validity_restrictions['region']
	ntaining region_type
	indicating 'id'
	d containing id_region
	containing region_dictionary
	indicating 'iso_3166_1' (0)
	and containing local_region
	indicating 0
i	and containing region_identifier
	indicating ID_REGION_AT
46.5.5	fully covering RECT_REGION_AT
then	no magaza
the IUT accepts the	ie message
TP ld	
	TP_SEC_ITSS_RCV_CERT_07_06_BO

TP ld	TP_SEC_ITSS_RCV_CERT_07_06_BO
Summary	Check that the IUT discards a message when the signing certificate of this message does not contain the region validity restriction but its issuing certificate contains the rectangular region validity restriction
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_RECTANGULAR_REGION
	Expected behaviour
with	
the IUT being in the 'autl	horized' state
and the IUT current time	is inside the time validity period of CERT_TS_07_06_BO_AT
and the IUT current loca	tion is inside the RECT_REGION_AT
ensure that	
when the IUT is receiving	g a SecuredMessage
containing header_fie	lds ['signer_info']
containing signer	
containing type	
indicating 'cert	
	cate (CERT_TS_07_06_BO_AT)
	validity_restrictions['region']
	g signer_info.digest
	to a CERT_TS_C_AA
	g validity_restrictions['region']
	ning region_type
	cating 'rectangular'
then	
the IUT discards the n	nessage

TP ld	TP_SEC_ITSS_RCV_CERT_07_07_BO
	Check that the IUT discards a message when the signing certificate of this message
Summary	contains rectangular region validity restriction which is outside of the rectangular region
	validity restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_RECTANGULAR_REGION
	Expected behaviour
with	
the IUT being in the	
	time is inside the time validity period of CERT_TS_07_07_BO_AT
	location is inside the RECT_REGION_AT
ensure that	
	eiving a SecuredMessage
	r_fields ['signer_info']
containing sigr	
containing ty	
	'certificate'
	ing certificate (CERT_TS_07_07_BO_AT)
	g validity_restrictions['region']
	ning region_type
	ating 'rectangle'
	ntaining rectangular_region[0]
	ating RECT_REGION_AT
	aining signer_info.digest
	icing to a CERT_TS_07_07_BO_AA
	aining validity_restrictions['region']
CC	indiating region_type
~	indicating 'rectangle'
ar	nd containing rectangular_region[0] indicating RECT_REGION_AA_OUTSIDE
	not including RECT_REGION_AT
then	
the IUT discards	the message

TP ld	TP_SEC_ITSS_RCV_CERT_07_08_BO
	Check that the IUT discards a message when the signing certificate of this message
Summary	contains rectangular region validity restriction which is not fully covered by the the
	rectangular region validity restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_RECTANGULAR_REGION
	Expected behaviour
with	
the IUT being in the	a 'authorized' state
	time is inside the time validity period of CERT_TS_07_08_BO_AT
	location is inside the RECT_REGION_AT
ensure that	
	eiving a SecuredMessage
•	er_fields ['signer_info']
containing sigr	
containing ty	
	'certificate'
	ing certificate (CERT_TS_07_08_BO_AT)
	g validity_restrictions['region']
	ning region_type
	cating 'rectangle'
	ntaining rectangular_region[0] cating RECT_REGION_AT
	aining signer_info.digest
	ncing to a CERT_TS_07_08_BO_AA
	aining validity_restrictions['region']
	ontaining region_type
	indicating 'rectangle'
ar	nd containing rectangular_region[0]
	indicating RECT_REGION_AA_INTERSECT
1	including partialy RECT_REGION_AT
then	
the IUT discards	the message

TP ld	TP_SEC_ITSS_RCV_CERT_08_01_BV
Summary	Check that the IUT accepts a message when the signing certificate of this message contain
	the same polygonal region validity restriction as its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION
	Expected behaviour
with	
the IUT being in the	a 'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_08_01_BV_AT
and the IUT current	location is inside the POLYGON REGION AA
ensure that	
when the IUT is rec	eiving a SecuredMessage
containing heade	er_fields ['signer_info']
containing sigr	ner
containing t	
indicating	'certificate'
and contain	ing certificate (CERT_TS_08_01_BV_AT)
containing	g validity_restrictions['region']
contair	ning region_type
indic	cating 'polygon'
	ntaining polygonal_region
	cating POLYGON_REGION_AA
	aining signer_info.digest
referer	ncing to a CERT_TS_D_AA
cont	aining validity_restrictions['region']
CC	ontaining region_type
	indicating 'polygon'
ar	nd containing polygonal_region
	indicating POLYGON_REGION_AA
then	
the IUT accepts t	he message

# 5.3.5.8 Check polygonal region of subordinate certificate

TP ld	TP_SEC_ITSS_RCV_CERT_08_02_BV
	Check that the IUT accepts a message when the signing certificate of this message contains
Summary	the polygonal region validity restriction which is fully inside in the circular region validity
	restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION
	Expected behaviour
with	
the IUT being in the	
	time is inside the time validity period of CERT_TS_08_02_BV_AT
	location is inside the POLYGON_REGION_AT
ensure that	
	eiving a SecuredMessage
	r_fields ['signer_info']
containing sigr	
containing ty	
0	'certificate'
	ng certificate (CERT_TS_08_02_BV_AT)
	y validity_restrictions['region']
	ing region_type
	ating 'polygon'
	ntaining polygonal_region ating POLYGON_REGION_AT
	ining signer_info.digest
	cing to a certificate CERT_TS_B_AA
	aining validity_restrictions['region']
	intaining region_type
	indicating 'circle'
ar	nd containing circular_region
u	indicating CURCULAR_REGION_AA
	fully including POLYGON_REGION_AT
then	.,
the IUT accepts t	he message

TP ld	TP_SEC_ITSS_RCV_CERT_08_03_BV
	Check that the IUT accepts a message when the signing certificate of this message contains
Summary	the polygonal region validity restriction which is fully inside in the rectangular region validity
-	restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION
	Expected behaviour
with	
the IUT being in the	
	time is inside the time validity period of CERT_TS_08_03_BV_AT
	location is inside the POLYGON_REGION_AT
ensure that	
	eiving a SecuredMessage
	r_fields ['signer_info']
containing sign	
containing t	
	'certificate' ing certificate (CERT_TS_08_03_BV_AT)
	g validity_restrictions['region']
	ing region_type
	ating 'polygon'
	ntaining polygonal_region
	ating POLYGON_REGION_AT
	aining signer_info.digest
referer	cing to a certificate CERT_TS_C_AA
cont	aining validity_restrictions['region']
CC	ontaining region_type
	indicating 'rectangular'
ar	nd containing rectangular_region[0]
	indicating RECT_REGION_AA
44	fully covering POLYGON_REGION_AT
then	
the IUT accepts t	ne message

TP ld	TP_SEC_ITSS_RCV_CERT_08_04_BV
	Check that the IUT accepts a message when the signing certificate of this message contains
Summary	the polygonal region validity restriction which is fully inside in the polygonal region validity
	restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION
	Expected behaviour
with	
the IUT being in the 'a	
	me is inside the time validity period of CERT_TS_08_04_BV_AT
	cation is inside the POLYGON_REGION_AA
ensure that	
	ving a SecuredMessage
	fields ['signer_info']
containing signe	
containing typ	
indicating 'c	
	g certificate (CERT_TS_08_04_BV_AT)
	/alidity_restrictions['region']
	g region_type
	ing 'polygon' aining polygonal_region
	ing POLYGON_REGION_AT
	ing signer_info.digest
	ng to a CERT_TS_D_AA
	ning validity_restrictions['region']
	aining region_type
	dicating 'polygon'
	containing polygonal_region
	dicating POLYGON_REGION_AA
	fully including POLYGON_REGION_AT
then	
the IUT accepts the	e message

TP ld	TP_SEC_ITSS_RCV_CERT_08_05_BV
	Check that the IUT accepts a message when the signing certificate of this message contains
Summary	the polygonal region validity restriction which is fully inside in the identified region validity
•	restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION
	Expected behaviour
with	
the IUT being in the	
	ime is inside the time validity period of CERT_TS_08_04_BV_AT
	ocation is inside the POLYGON_REGION_AT
ensure that	
	iving a SecuredMessage
	_fields ['signer_info']
containing signe containing typ	
indicating '	
	g certificate (CERT_TS_08_05_BV_AT)
	validity_restrictions['region']
	ng region_type
	ting 'polygon'
	taining polygonal_region
	Iting POLYGON_REGION_AT
	ning signer_info.digest
	ing to a certificate CERT_TS_E_AA
	ining validity_restrictions['region']
	ntaining region_type
	ndicating 'id'
	d containing id_region containing region_dictionary
(	indicating 'iso_3166_1' (0)
2	and containing local_region
· · · · ·	indicating 0
â	and containing region_identifier
·	indicating ID_REGION_AT
	fully including POLYGON_REGION_AT
then	
the IUT accepts th	e message

TP ld	TP_SEC_ITSS_RCV_CERT_08_06_BO
Summary	Check that the IUT discards a message when the signing certificate of this message does not contain the region validity restriction but its issuing certificate contains the polygonal
	region validity restriction
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current time is inside the time validity period of CERT_TS_08_06_BO_AT	
ensure that	
when the IUT is rec	eiving a SecuredMessage
	r_fields ['signer_info']
containing sigr	
containing ty	
0	'certificate'
	ng certificate (CERT_TS_08_06_BO_AT)
	ining validity_restrictions['region']
	ining signer_info.digest
	cing to a CERT_TS_D_AA
	aining validity_restrictions['region']
containing region_type	
indicating 'polygon'	
then	
the IUT discards	the message

<b>TD</b> 1 1		
TP ld	TP_SEC_ITSS_RCV_CERT_08_07_BO	
Summary	Check that the IUT discards a message when the signing certificate of this message	
	contains polygonal region validity restriction containing less than 3 points	
Reference ETSI TS 103 097 [1], clause 7.4.1		
PICS Selection	ICS Selection PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION	
	Expected behaviour	
with		
the IUT being in the 'auth		
and the IUT current time	is inside the time validity period of CERT_TS_08_07_BO_AT	
and the IUT current locat	ion is inside the POLYGON_REGION_AT	
ensure that		
when the IUT is receiving		
containing header_fiel	ds ['signer_info']	
containing signer		
containing type		
indicating 'certi		
	ertificate (CERT_TS_08_07_BO_AT)	
	dity_restrictions['region']	
containing re		
indicating		
and containing polygonal_region (POLYGON_REGION_08_04_BO)		
indicating length = $2$		
and containing signer_info.digest		
referencing to a CERT_TS_D_AA		
containing validity_restrictions['region']		
containing region_type		
indicating 'polygon' and containing polygonal_region		
indicating POLYGON_REGION_AA		
fully covering all points of POLYGON_REGION_08_04_BO		
then		
	the IUT discards the message	

156

TP ld	TP_SEC_ITSS_RCV_CERT_08_08_BO
	Check that the IUT discards a message when the signing certificate of this message
Summary	contains polygonal region validity restriction which is outside of the polygonal region validit
Summary	restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION
	Expected behaviour
with	
the IUT being in the 'a	authorized' state
	me is inside the time validity period of CERT_TS_08_08_BO_AT
	bocation is inside the POLYGON_REGION_AT
ensure that	
	ving a SecuredMessage
	_fields ['signer_info']
containing signe	
containing typ	
indicating 'o	
	g certificate (CERT_TS_08_08_BO_AT)
	validity_restrictions['region']
containir	ng region_type
	ting 'polygon'
	aining polygonal_region
	ting POLYGON_REGION_AT
	ning signer_info.digest
	ing to a CERT_TS_08_08_BO_AA
	ning validity_restrictions['region']
	taining region_type
	ndicating 'polygon'
	containing polygonal_region
ır	
then	not including POLYGON_REGION_AT
then the IUT discards th	n maaaaa
	le message
TP ld	TP_SEC_ITSS_RCV_CERT_08_09_BO
	Check that the IUT discards a message when the signing certificate of this message
Summary	contains polygonal region validity restriction which is not fully covered by the the polygonal
	region validity restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_POLYGONAL_REGION
	Expected behaviour
with	
the IUT being in the 'a	
	me is inside the time validity period of CERT_TS_08_09_BO_AT
	ocation is inside the POLYGON_REGION_AT
ensure that	
	ving a SecuredMessage
	_fields ['signer_info']
containing signe	
containing typ	
indicating 'd	g certificate (CERT_TS_08_09_BO_AT)

then the IUT discards the message

containing validity\_restrictions['region']

and containing polygonal\_region indicating POLYGON\_REGION\_AT

> containing region\_type indicating 'polygon' and containing polygonal\_region

referencing to a CERT\_TS\_08\_09\_BO\_AA containing validity\_restrictions['region']

indicating POLYGON\_REGION\_AA\_INTERSECT including partialy POLYGON\_REGION\_AT

and containing signer\_info.digest

containing region\_type indicating 'polygon'

TP ld	TP_SEC_ITSS_RCV_CERT_09_01_BV
	Check that the IUT accepts a message when its signing certificate contains the identified
Summary	region validity restriction with the same identified region as the issuing certificate and without
	local area definition
Reference	ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION
	Expected behaviour
with	· · · · · · · · · · · · · · · · · · ·
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_09_01_BV_AT
and the IUT current	location is inside the ID_REGION_AT
ensure that	
when the IUT is rece	eiving a SecuredMessage
	_fields ['signer_info']
containing sign	er
containing ty	pe
indicating	certificate'
and containing	ng certificate (CERT_TS_09_01_BV_AT)
containing	validity_restrictions['region']
contain	ng region_type
indica	ating 'id'
and cor	taining id_region
	ining region_dictionary
	licating 'iso_3166_1'
	containing region_identifier
inc	licating ID_REGION_AT
and	containing local_region
	licating 0
	signer_info.digest
	cing to a certificate CERT_TS_E_AA
	iining region_type
	licating 'id'
	containing id_region
	ntaining region_dictionary
	indicating 'iso_3166_1'
	d containing region_identifier
	indicating ID_REGION_AT
	d containing local_region
	indicating 0
then	
the IUT accepts the	ne message

# 5.3.5.9 Check identified region of subordinate certificate

	TP_SEC_ITSS_RCV_CERT_09_02_BV
	Check that the IUT accepts a message when its signing certificate contains the identified
Summary	region validity restriction with the same identified region as the issuing certificate and with
	local area definition
Reference	ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION
	Expected behaviour
with	
the IUT being in the 'auth	
	is inside the time validity period of CERT_TS_09_02_BV_AT
	on is inside the ID_REGION_AT
ensure that	
when the IUT is receiving	
containing header_field	ds ['signer_info']
containing signer	
containing type	
indicating 'certificate'	
	rtificate (CERT_TS_09_02_BV_AT)
	lity_restrictions['region']
containing re	
indicating 'id'	
and containing id_region	
	region_dictionary
	ng 'iso_3166_1'
	ining region_identifier
indicating ID_REGION_AT	
and containing local_region	
indicating ID_LOCAL_REGION_1	
containing signer_info.digest referencing to a certificate CERT_TS_E_AA	
indicatir	region_type
	ining id_region
containing region_dictionary indicating 'iso_3166_1'	
and containing region_identifier	
	ating ID_REGION_AT
and containing local_region	
	ating 0
then	
the IUT accepts the me	essade

TP ld	TP_SEC_ITSS_RCV_CERT_09_03_BV	
	Check that the IUT accepts a message when its signing certificate contains the identified	
Summary	region validity restriction fully containing in the circular validity restriction of its issuing	
-	certificate	
Reference	ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the	'authorized' state	
	time is inside the time validity period of CERT_TS_09_03_BV_AT	
	location is inside the ID_REGION_AT	
ensure that		
	eiving a SecuredMessage	
	r_fields ['signer_info']	
containing sign		
containing ty		
	'certificate'	
	ng certificate (CERT_TS_09_03_BV_AT) g validity_restrictions['region']	
	ing region_type	
	ating 'id'	
	ntaining id_region	
	aining region_dictionary	
	dicating 'iso_3166_1'	
	containing region_identifier	
	dicating IĎ_RĚGION_AT	
	containing local_region	
inc	dicating 0	
	ining signer_info.digest	
	cing to a certificate CERT_TS_09_03_BV_AA	
	aining validity_restrictions['region']	
	ntaining region_type	
	indicating 'circle'	
	nd containing circular_region	
	fully covering ID_REGION_AT	
then		
the IUT accepts the	ne message	

TP ld	TP SEC ITSS RCV CERT 09 04 BV
	Check that the IUT accepts a message when the signing certificate of this message contains
Summary	the polygonal region validity restriction which is fully inside in the rectangular region validity
,	restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION
	Expected behaviour
with	
the IUT being in the	
	t time is inside the time validity period of CERT_TS_09_03_BV_AT
	t location is inside the ID_REGION_AT
ensure that	
	ceiving a SecuredMessage
	er_fields ['signer_info']
containing sig	
containing t	ype g 'certificate'
	ing certificate (CERT_TS_09_04_BV_AT)
	g validity_restrictions['region']
	ning region_type
	cating 'id'
	ntaining id_region
	aining region_dictionary
in	dicating 'iso_3166_1'
	containing region_identifier
	dicating ID_REGION_AT
	containing local_region
	dicating 0
	aining signer_info.digest
	ncing to a certificate CERT_TS_09_04_BV_AA
	taining validity_restrictions['region'] ontaining region_type
	indicating 'rectangular'
C	ontaining rectangular_region[0]
	fully covering ID_REGION_AT
then	
the IUT accepts	the message

TP ld	TP_SEC_ITSS_RCV_CERT_09_05_BV
	Check that the IUT accepts a message when the signing certificate of this message contains
Summary	the polygonal region validity restriction which is fully inside in the polygonal region validity
	restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION
	Expected behaviour
with	
the IUT being in the	
	time is inside the time validity period of CERT_TS_09_05_BV_AT
	location is inside the ID_REGION_AT
ensure that	
	eiving a SecuredMessage
	r_fields ['signer_info']
containing sign	
containing ty	'certificate'
	ing certificate (CERT_TS_09_05_BV_AT)
	g validity_restrictions['region']
	ling region_type
	ating 'id'
and co	ntaining id_region
	aining region_dictionary
	dicating 'iso_3166_1'
	containing region_identifier
	dicating ID_REGION_AT
	containing local_region
	dicating 0
	aining signer_info.digest
	cing to a certificate CERT_TS_09_05_BV_AA aining validity_restrictions['region']
	ontaining region_type
	indicating 'polygon'
ar	nd containing polygonal_region
u.	fully covering ID_REGION_AT
then	
the IUT accepts t	he message

TP ld	TP_SEC_ITSS_RCV_CERT_09_06_BV
	Check that the IUT accepts a message when the signing certificate of the message contain
Summary	the identified region validity restriction with the identified region which is fully covered by the
2	identified region of the validity restriction of its issuing certificate
Reference	ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION
	Expected behaviour
with	
the IUT being in the	authorized' state
	ime is inside the time validity period of CERT_TS_09_06_BV_AT
	ocation is inside the ID_REGION_AT
ensure that	
	iving a SecuredMessage
	_fields ['signer_info']
containing signe	
containing typ	
indicating '	
	ig certificate (CERT_TS_09_06_BV_AT)
	validity_restrictions['region']
	ng region_type
	ting 'id'
	taining id_region
	ining region_dictionary
	icating 'un_stats'
	ontaining region_identifier
	icating ID_REGION_AT
	ontaining local_region
	icating 0
	ning signer_info.digest
	ing to a CERT_TS_09_06_BV_AA
	ining validity_restrictions['region']
	ntaining region_type
	ndicating 'id'
	d containing id_region
	containing region_dictionary
	indicating 'un_stats'
é	and containing region_identifier
	indicating ID_REGION_AA_UNSTATS
	which includes ID_REGION_AT
2	and containing local_region
	indicating 0
then	Ŭ,
the IUT accepts th	e message

TP ld	TP_SEC_ITSS_RCV_CERT_09_07_BO		
	Check that the IUT discards a message when the signing certificate of this message does		
Summary	not contain the region validity restriction but its issuing certificate contains the identified		
	region validity restriction		
Reference	ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1		
PICS Selection	PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION		
	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_09_07_BO_AT		
ensure that			
when the IUT is receiving			
containing header_fields ['signer_info']			
containing signer			
containing type			
indicating 'certificate'			
and containing certificate (CERT_TS_09_07_BO_AT)			
	not containing validity_restrictions['region']		
and containing signer_info.digest			
referencing to the certificate CERT_TS_E_AA			
containing validity_restrictions['region']			
containing region_type			
indicating 'id'			
then			
the IUT discards the m	the IUT discards the message		

TP ld	TP_SEC_ITSS_RCV_CERT_09_08_BO
	Check that the IUT discards a message when the signing certificate and its issuing
Summary	certificate are both containing the identified region validity restrictions with the same region
-	id but different local regions
Reference	ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION
	Expected behaviour
with	
the IUT being in the 'a	uthorized' state
and the IUT current tin	ne is inside the time validity period of CERT_TS_09_08_BO_AT
and the IUT current lo	cation is inside the ID_REGION_AA, local region 1
ensure that	
	ing a SecuredMessage
containing header_f	ields ['signer_info']
containing signer	
containing type	)
indicating 'ce	
	certificate (CERT_TS_09_08_BO_AT)
	alidity_restrictions['region']
containing region_type	
indicating 'id'	
	ining id_region
containing region_dictionary	
	ating 'iso_3166_1'
containing region_identifier	
	ating ID_REGION_AA
containing local_region	
indicating ID_LOCAL_REGION_1	
containing signer_info.digest	
referencing to a CERT_TS_09_08_BO_AA	
containing validity_restrictions['region']	
containing region_type	
indicating 'id'	
containing id_region	
containing region_dictionary	
indicating 'iso_3166_1'	
containing region_identifier	
indicating ID_REGION_AA	
CC	ntaining local_region
indicating ID_LOCAL_REGION_2	
then	not equal to ID_LOCAL_REGION_1
	90622290
the IUT discards the message	

TP ld	TP_SEC_ITSS_RCV_CERT_09_09_BO
	Check that the IUT discards a message when the identified region of the validity restriction
Summary	of its signing certificate is different and not fully covered by the one in the issuing certificate
Reference	ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION
	Expected behaviour
with	
the IUT being in the 'auth	norized' state
	is inside the time validity period of CERT_TS_09_09_BO_AT
and the IUT current locat	ion is inside the ID_REGION_AT
ensure that	
when the IUT is receiving	
containing header_fiel	ds ['signer_info']
containing signer	
containing type	
indicating 'certi	
	ertificate (CERT_TS_09_09_BO_AT)
	dity_restrictions['region']
containing re	
indicating	
and containi	g region_dictionary
	ng 'iso_3166_1'
	ining region_identifier
	ng ID_REGION_AT
	ining local_region
indicati	
containing sign	
referencing t	to a CERT_TS_09_09_BO_AA
	y validity_restrictions['region']
	ing region_type
	ating 'id'
	ntaining id_region
	aining region_dictionary
	dicating 'iso_3166_1'
	containing region_identifier
Inc	dicating ID_REGION_AA_OTHER other than ID_REGION_AT
and	containing local_region
	dicating 0
then	
the IUT discards the m	nessage

166

TP ld	TP_SEC_ITSS_RCV_CERT_09_10_BO
Summary	Check that the IUT discards a message when the identified region validity restriction of its
	signing certificate contains unknown area code
Reference ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1	
PICS Selection	PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
and the IUT curren	t time is inside the time validity period of CERT_TS_09_10_BO_AT
and the IUT curren	t location is inside the ID_REGION_AT
ensure that	
when the IUT is rea	ceiving a SecuredMessage
containing head	er_fields ['signer_info']
containing sig	ner
containing t	
	g 'certificate'
	ing certificate (CERT_TS_09_10_BO_AT)
	g validity_restrictions['region']
	ning region_type
	cating 'id'
	ontaining id_region
	taining region_dictionary
	ndicating 'iso_3166_1'
	containing region_identifier
ır	Idicating ID_REGION_UNKNOWN
	not existing in ISO 3166-1 [4]
	containing local_region
	ndicating 0
	aining signer_info.digest
	ncing to a CERT_TS_A_AA
	containing validity_restrictions [4]
then	the measure
the IUT discards	ine message

TP ld	TP_SEC_ITSS_RCV_CERT_09_11_BO
	Check that the IUT discards a message when the validity restriction of its signing certificate
Summary	contains the identified region of type iso-3166-1 but region code is from the UN-Stats
	dictionary
Reference	ETSI TS 103 097 [1], clauses 4.2.26 and 7.4.1
PICS Selection	PICS_GN_SECURITY AND PICS_USE_IDENTIFIED_REGION
	Expected behaviour
with	
the IUT being in the	
	time is inside the time validity period of CERT_TS_09_11_BO_AT
	location is inside the ID_REGION_AA_UNSTATS
ensure that	
	eiving a SecuredMessage
	r_fields ['signer_info']
containing sigr	
containing t	
	'certificate'
	ing certificate (CERT_TS_09_11_BO_AT) g validity_restrictions['region']
	ing region_type
	ating 'id'
	ntaining id_region
	aining region_dictionary
	dicating 'iso_3166_1'
	containing region_identifier
	dicating ID_REGION_AA_UNSTATS
and	containing local_region
in	dicating 0
	aining signer_info.digest
	cing to a CERT_TS_A_AA
	containing validity_restrictions['region']
then	
the IUT discards	the message

#### 5.3.5.10 Check time validity restrictions

#### 5.3.5.10.1 Check time validity restriction presence

TP ld	TP_SEC_ITSS_RCV_CERT_10_01_BO
Summany.	Check that the IUT discards a message when its signing certificate does not contain the
Summary	time validity restriction
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
ensure that	
when the IUT is rec	ceiving a SecuredMessage
containing heade	er_fields ['signer_info']
containing sig	ner
containing t	
	g 'certificate'
	certificate (CERT_TS_10_01_BO_AT)
	ining validity_restrictions['time_start_and_end']
	containing validity_restrictions['time_end']
and not c	containing validity_restrictions['time_start_and_duration']
then	
the IUT discards	the message

TP ld	TP_SEC_ITSS_RCV_CERT_10_02_BO		
Summary	Check that the IUT discards a message when the issuing certificate of the message signing		
	certificate does not contain the time validity restriction		
Reference ETSI TS 103 097 [1], clause 7.4.1			
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT being in the	'authorized' state		
ensure that			
when the IUT is reco	eiving a SecuredMessage		
containing heade	r_fields ['signer_info'].signer		
containing type			
indicating 'ce	ertificate'		
	ificate (CERT_TS_10_02_BO_AT)		
	igner_info.digest		
	g to CERT_TS_10_02_BO_AA		
	taining validity_restrictions['time_start_and_end']		
	containing validity_restrictions['time_end']		
and not	containing validity_restrictions['time_start_and_duration']		
than			
then			
the IUT discards	lie liessaye		

169

#### 5.3.5.10.2 Check AT certificate time validity restriction presence

TP ld	TP_SEC_ITSS_RCV_CERT_10_03_BO		
Summary	Check that the IUT discards a message when its signing certificate contains 'time_end'		
Summary	validity restriction		
Reference	ETSI TS 103 097 [1], clauses 7.4.2 and 7.4.4		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT being in the 'au	thorized' state		
and the IUT current time	e is less then time_end validity restricyion of CERT_TS_10_03_BO_AT		
ensure that			
when the IUT is receivir	ng a SecuredMessage		
containing header_fie	elds ['signer_info']		
containing signer			
containing type			
indicating 'cer	'tificate'		
containing certif	icate (CERT_TS_10_03_BO_AT)		
containing va	lidity_restrictions['time_end']		
then			
the IUT discards the	message		

TP ld	TP_SEC_ITSS_RCV_CERT_10_04_BO	
Summary	Check that the IUT discards a message when its signing certificate contains	
Summary	'time_start_and_duration' validity restriction	
Reference ETSI TS 103 097 [1], clauses 7.4.2 and 7.4.4		
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'auth	norized' state	
and the IUT current time	is inside the time validity period of CERT_TS_10_04_BO_AT	
ensure that		
when the IUT is receivi	ng a SecuredMessage	
containing header_fiel	ds ['signer_info']	
containing signer		
containing type		
indicating 'cert	ificate'	
containing certific	cate (CERT_TS_10_04_BO_AT)	
	dity_restrictions['time_start_and_duration']	
then		
the IUT discards the m	nessage	

TP ld	TP_SEC_ITSS_RCV_CERT_10_05_BO
Summary	Check that the IUT discards a message when the issuing certificate of the message signing
	certificate contains 'time_end' validity restriction
Reference	ETSI TS 103 097 [1], clauses 7.4.2 and 7.4.4
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is less then time_end validity restricyion of CERT_TS_10_05_BO_AT
ensure that	
when the IUT is rec	eiving a SecuredMessage
containing heade	r_fields ['signer_info'].signer
containing type	
indicating 'co	
containing cert	ificate (CERT_TS_10_05_BO_AT)
	igner_info.digest
referencir	ng to CERT_TS_10_05_BO_AA
contain	ing validity_restrictions['time_end']
then	
the IUT discards	the message

TP ld	TP_SEC_ITSS_RCV_CERT_10_06_BO
	Check that the IUT discards a message when its signing certificate contains
Summary	'time_start_and_duration' validity restriction
Reference	ETSI TS 103 097 [1], clauses 7.4.2 and 7.4.4
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the '	authorized' state
and the IUT current t	me is less then time_end validity restricyion of CERT_TS_10_06_BO_AT
ensure that	
when the IUT is rece	iving a SecuredMessage
containing header	_fields ['signer_info'].signer
containing type	
indicating 'ce	tificate'
containing certif	icate (CERT_TS_10_06_BO_AT)
-	iner info.digest
referencing	to CERT_TS_10_06_BO_AA
	ng validity_restrictions['time_start_and_duration']
then	· · · · · · · · · · · · · · · · · · ·
the IUT discards th	ne message

5.3.5.11	Check time validity	restriction conforming	g to the i	ssuing certificate

TP ld	TP_SEC_ITSS_RCV_CERT_11_01_BO
Summary	Check that the IUT discards a message when the validity period of the signing certificate
	ends after the validity period of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is greater than START_VALIDITY_AA and less than END_VALIDITY_AA
ensure that	
when	
	ng a SecuredMessage
	der_fields ['signer_info'].signer.certificate (CERT_TS_11_01_BO_AT)
	gner_info.digest
	g to CERT_TS_A_AA
	ing validity_restrictions['time_start_and_end']
	aining start_validity
	dicating START_VALIDITY_AA
	aining end_validity
	licating END_VALIDITY_AA
	alidity_restrictions['time_start_and_end']
	ng START_VALIDITY_AA
	yend_validity
then	ng END_VALIDITY_AA + 1d
the IUT discards	he message
	ine inessaye

TP ld	TP_SEC_ITSS_RCV_CERT_11_02_BO
Summary	Check that the IUT discards a message when the validity period of its signing certificate
	starts before the validity period of the issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'auth	orized' state
and the IUT current time	is greater than START_VALIDITY_AA and less than END_VALIDITY_AA
ensure that	
when the IUT is receiving	
	ds ['signer_info'].signer.certificate (CERT_TS_11_02_BO_AT)
containing signer_in	
referencing to CE	
•	lity_restrictions['time_start_and_end']
containing st	
indicating START_VALIDITY_AA	
and containing end_validity	
	END_VALIDITY_AA
and containing validity_restrictions['time_start_and_end']	
containing start_validity	
indicating START_VALIDITY_AA - 1d and containing end_validity	
indicating END VALIDITY AA	
then	
the IUT discards the m	essage

TP Id	TP_SEC_ITSS_RCV_CERT_11_03_BO
Summary	Check that the IUT discards a message when the issuing certificate of signing certificate is
	expired but the signing certificate is not expired yet
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	
	time is greater than START_VALIDITY_AA and less than END_VALIDITY_AA
ensure that	
	eiving a SecuredMessage
	er_fields ['signer_info'].signer.certificate (CERT_TS_11_03_BO_AT)
	ner_info.digest
	to CERT_TS_11_03_BO_AA
	g validity_restrictions['time_start_and_end']
contair	ning start_validity
	cating START_VALIDITY_AA - 365d
	ntaining end_validity
	cating START_VALIDITY_AA - 1d
	y validity_restrictions['time_start_and_end']
containing s	
	START_VALIDITY_AA - 365d
	ing end_validity   END_VALIDITY_AA
	I END_VALIDIT T_AA
then	
the IUT discards	lile lilessage
TP ld	TP_SEC_ITSS_RCV_CERT_11_04_BO
	Check that the IUT discards a message when the validity period of the signing certificate is
Summary	after the validity period of its issuing certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	a louthorized atoto
	time is greater than START_VALIDITY_AA and less than END_VALIDITY_AA
ensure that	time is greater than START_VALIDITT_AA and less than END_VALIDITT_AA
	eiving a SecuredMessage
	er_fields ['signer_info'].signer.certificate (CERT_TS_11_04_BO_AT)
	ner_info.digest
roforoncing	to CERT_TS_11_04_BO_AA
	g validity_restrictions['time_start_and_end']
	ning start_validity
	cating END_VALIDITY_AA
	ntaining end_validity
	cating END_VALIDITY_AA + 365d
	y validity_restrictions['time_start_and_end']
containing s	
indicating START_VALIDITY_AA	
and containing and validity	

and containing end\_validity indicating END\_VALIDITY\_AA +365d then

the IUT discards the message

TP ld	TP_SEC_ITSS_RCV_CERT_12_01_BO
Summary	Check that the IUT discards a message when its signing certificate does not contain the
	SSP-AID subject attribute
Reference	ETSI TS 103 097 [1], clause 7.4.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
and the IUT current	t time is inside the time validity period of CERT_TS_12_01_BO_AT
ensure that	
when the IUT is rec	eiving a SecuredMessage
containing heade	er_fields ['signer_info']
containing sig	ner
containing t	
indicating 'certificate'	
and containing certificate (CERT_TS_12_01_BO_AT)	
not conta	ining subject_attributes['its_aid_ssp_list']
then	
the IUT discards the message	

TP ld	TP_SEC_ITSS_RCV_CERT_12_02_BO
Summary	Check that the IUT discards a Secured CAM when its signing certificate does not contain a
	record with AID_CAM in the its_aid_ssp_list subject attribute
Reference	ETSI TS 103 097 [1], clause 7.4.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_12_02_BO_AT
ensure that	
when the IUT is rec	eiving a Secured CAM (MSG_SEC_RCV_CAM_01)
containing heade	r_fields ['its_aid']
containing its_	
indicating 'A	
	eader_fields ['signer_info']
containing sigr	
containing ty	
	'certificate'
	ng certificate (CERT_TS_12_02_BO_AT)
	g subject_attributes['its_aid_ssp_list']
	taining an item
	aining its_aid
	dicating 'AID_CAM'
then	
the IUT discards	the message

TP ld	TP_SEC_ITSS_RCV_CERT_12_03_BO
Summary	Check that the IUT discards a Secured DENM when its signing certificate does not contain a
	record with AID_DENM in the its_aid_ssp_list subject attribute
Reference	ETSI TS 103 097 [1], clause 7.4.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'a	authorized' state
and the IUT current ti	me is inside the time validity period of CERT_TS_12_03_BO_AT
ensure that	
when the IUT is recei	ving a Secured DENM (MSG_SEC_RCV_DENM_A)
containing header_	
containing its_ai	
indicating 'AIE	
5	der_fields ['signer_info']
containing signe	
containing typ	
indicating 'd	
	g certificate (CERT_TS_12_03_BO_AT)
	subject_attributes['its_aid_ssp_list']
	iining an item
	ning its_aid
	cating 'AID_DENM'
then	

the IUT discards the message

TP ld	TP_SEC_ITSS_RCV_CERT_12_04_BO
Summary	Check that the IUT discards a Secured CAM when its signing certificate contains two
	records with AID_CAM in the its_aid_ssp_list subject attribute
Reference	ETSI TS 103 097 [1], clause 7.4.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	·
the IUT being in the	authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_12_04_BO_AT
ensure that	
when the IUT is rec	eiving a Secured CAM (MSG_SEC_RCV_CAM_01)
containing heade	r_fields ['its_aid']
containing its_	aid
indicating 'A	ID_CAM'
and containing he	eader_fields ['signer_info']
containing sigr	
containing ty	/pe
indicating	'certificate'
	ing certificate (CERT_TS_12_04_BO_AT)
	g subject_attributes['its_aid_ssp_list']
contain	ing item [0].its_aid
indic	ating 'AID_CAM'
	ntaining item [1].its_aid
indic	ating 'AID_CAM'
then	
the IUT discards	the message

#### 5.3.5.13 Check AID-SSP subject attribute value conforming to the issuing certificate

TP ld	TP_SEC_ITSS_RCV_CERT_13_01_BO
	Check that the IUT discards a message when the signing AT certificate contains a CAM
Summary	AID-SSP record whereas the issuing AA certificate does not contain the record with
Cannaly	AID_CAM
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'a	uthorized' state
and the IUT current tin	ne is inside the time validity period of CERT_TS_13_01_BO_AT
ensure that	
when the IUT is receiv	ing a Secured CAM (MSG_SEC_RCV_CAM_01)
containing header_f	ields ['signer_info'].signer.certificate (CERT_TS_13_01_BO_AT)
containing signer	_info.digest
referencing to	CERT_TS_13_01_BO_AA
	ubject_attributes['its_aid_list']
not contai	ning 'AID_CAM'
and containing subject_attributes['its_aid_ssp_list']	
containing a re	
containing its	s_aid
indicating	'AID_CAM'
then	
the IUT discards the	e message
TP ld	TP_SEC_ITSS_RCV_CERT_13_02_BO
	Check that the IUT discards a message when the signing AT certificate contains a DENM

	IF_3EC_II33_KCV_CERI_I3_02_DO
	Check that the IUT discards a message when the signing AT certificate contains a DENM
Summary	AID-SSP record whereas the issuing AA certificate does not contain the AID record with
	AID_DENM
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	e 'authorized' state
and the IUT current	t time is inside the time validity period of CERT_TS_13_02_BO_AT
ensure that	
when the IUT is rec	eiving a Secured DENM (MSG_SEC_RCV_DENM_A)
containing heade	er_fields ['signer_info'].signer.certificate (CERT_TS_13_02_BO_AT)
containing sigr	ner_info.digest
referencing	to CERT_TS_13_02_BO_AA
containin	g subject_attributes['its_aid_list']
not cor	ntaining 'AID_DENM'
and containing	g subject_attributes['its_aid_ssp_list']
containing a record	
containing its_aid	
indicat	ing 'AID_DENM'
then	
the IUT discards	

TP ld	TP_SEC_ITSS_RCV_CERT_13_03_BO
Summony	Check that IUT discards a SecuredMessage if the AA certificate does not contain a
Summary	subject_attribute of type its_aid_list
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY
Expected behaviour	
with	
the IUT being in the 'authorized' state	
and the IUT current time is inside the time validity period of CERT_TS_13_03_BO_AT	
ensure that	
when the IUT is receiving a Secured CAM (MSG_SEC_RCV_CAM_01)	
containing header_fields ['signer_info'].signer.certificate (CERT_TS_13_03_BO_AT)	
containing signer_info.digest	
referencing to CERT_TS_13_03_BO_AA	
not containing subject_attributes['its_aid_list']	
then	
the IUT discards the message	

# 5.3.5.14 Check the authorization ticket certificate signer info

TP ld	TP_SEC_ITSS_RCV_CERT_14_01_BO
Summary	Check that IUT discards the AT certificate with signer info of type 'certificate'
Reference	ETSI TS 103 097 [1], clause 7.4.2
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the 'auth	norized' state
and the IUT current time	is inside the time validity period of CERT_TS_14_01_BO_AT
ensure that	
when the IUT is receiving	0
containing header_fields ['signer_info']	
containing signer	
containing type	
indicating 'certi	
	ertificate (CERT_TS_14_01_BO_AT)
containing sign	
containing type	
indicating 'certificate'	
and containing certificate	
	CERT_TS_AA_A
then	
the IUT discards the m	lessage

TP ld	TP_SEC_ITSS_RCV_CERT_14_02_BO	
Summary	Check that IUT discards the AT certificate with signer info of type 'certificate_chain'	
Reference	ETSI TS 103 097 [1], clause 7.4.2	
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_14_02_BO_AT	
ensure that		
when the IUT is receiving a SecuredMessage		
containing header_fields ['signer_info']		
containing signer		
containing type		
indicating 'certificate'		
and containing certificate (CERT_TS_14_02_BO_AT)		
containing signer_info		
containing type		
indicating 'certificate_chain'		
and containing certificates[0]		
indicating certificate (CERT_TEST_ROOT)		
and containing certificates[1]		
	indicating certificate (CERT_TS_AA_A)	
the IUT discards the m	essage	

TP ld	TP_SEC_ITSS_RCV_CERT_14_03_BO		
_	Check that IUT discards the AT certificate with signer info of type		
Summary	'certificate_digest_with_other_algorithm'		
Reference	ETSI TS 103 097 [1], clause 7.4.2		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the IUT being in the 'author	prized' state		
and the IUT current time i	and the IUT current time is inside the time validity period of CERT_TS_14_03_BO_AT		
ensure that			
when the IUT is receiving a SecuredMessage			
containing header_fields ['signer_info']			
containing signer			
containing type			
indicating 'certif			
and containing certificate (CERT_TS_14_03_BO_AT)			
containing signer_info			
containing type			
indicating 'certificate_digest_with_other_algorithm'			
and containing digest			
referencing CERT_TS_AA_A			
then			
the IUT discards the message			

TP ld	TP_SEC_ITSS_RCV_CERT_15_01_BO	
Summary	Check that IUT discards the AA certificate with signer info of type 'certificate'	
Reference	ETSI TS 103 097 [1], clause 7.4.4	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'auth	norized' state	
	is inside the time validity period of CERT_TS_15_01_BO_AT	
ensure that		
when the IUT is receiving	g a SecuredMessage	
containing header_fiel	ds ['signer_info']	
containing signer		
containing type		
indicating 'certi		
	ertificate (CERT_TS_15_01_BO_AT)	
containing sign		
	to certificate (CERT_TS_15_01_BO_AA)	
	g signer_info	
	ning type ating 'certificate'	
	ntaining certificate	
	tating CERT_TEST_ROOT	
then		
the IUT discards the m	nessage	
	5	
TP ld	TP_SEC_ITSS_RCV_CERT_15_02_BO	
Summary	Check that IUT discards the AA certificate with signer info of type 'certificate_chain'	
Reference	ETSI TS 103 097 [1], clause 7.4.4	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'auth		
	is inside the time validity period of CERT_TS_15_02_BO_AT	
ensure that		
when the IUT is receiving a SecuredMessage		
containing header_fields ['signer_info'] containing signer		
containing signer		
indicating 'certificate'		
and containing certificate (CERT_TS_15_02_BO_AT)		
containing signer info.digest		
referencing to certificate (CERT_TS_15_02_BO_AA)		
containing signer_info		
containing type		
indicating 'certificate_chain'		
and containing certificates[0]		
indicating certificate (CERT_ROOT)		
and containing certificates[1]		
indicating certificate (CERT_TS_15_02_BO_CA)		
	containing signer_info	
	containing type	
	indicating 'certificate_digest_with_sha256'	
and containing digest		
then	referencing to CERT_TEST_ROOT	
then the IUT discards the m	referencing to CERT_TEST_ROOT	

#### 5.3.5.15 Check the authorization authority certificate signer info

TP ld	TP_SEC_ITSS_RCV_CERT_15_03_BO
Summary	Check that IUT discards the AA certificate with signer info of type
	certificate_digest_with_other_algorithm
Reference	ETSI TS 103 097 [1], clause 7.4.4
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_15_03_BO_AT
ensure that	
when the IUT is receiving	a SecuredMessage
containing header_field	ds ['signer_info']
containing signer	
containing type	
indicating 'certil	ficate'
and containing ce	rtificate (CERT_TS_15_03_BO_AT)
containing signer_info.digest	
referencing to certificate (CERT_TS_15_03_BO_AA)	
containing signer_info	
containing type	
indicating 'certificate_digest_with_other_algorithm'	
and containing digest	
referencing CERT_TEST_ROOT	
then	
the IUT discards the m	essage

#### 5.3.5.16 Check the subject\_name of the AT certificate

TP ld	TP_SEC_ITSS_RCV_CERT_16_01_BO	
Summary	Check that IUT discards a SecuredMessage if the subject_name of the AT certificate is not	
	an empty name field	
Reference	ETSI TS 103 097 [1], clause 7.4.2	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the 'au	thorized' state	
and the IUT current tim	and the IUT current time is inside the time validity period of CERT_TS_16_01_BO_AT	
ensure that		
when the IUT is receiving a SecuredMessage		
containing header_fields ['signer_info']		
containing signer		
containing type	containing type	
indicating 'certificate'		
and containing certificate (CERT_TS_14_01_BO_AT)		
containing subject_info.subject_name		
indicating non-empty string ('Invalid name')		
then		
the IUT discards the	message	

TP ld	TP_SEC_ITSS_RCV_CERT_17_01_BO
Summers	Check that IUT discards a SecuredMessage if the subject attribute of type assurance_level
Summary	is missing in the AT certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	· · · · · · · · · · · · · · · · · · ·
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_17_01_BO_AT
ensure that	
when the IUT is rec	eiving a Secured CAM (MSG_SEC_RCV_CAM_1)
	r_fields ['signer_info'].signer
containing type	
indicating 'c	ertificate'
and containing	certificate (CERT_TS_17_01_BO_AT)
	ng subject attributes['assurance level']
then	• • • • • • • •
the IUT discards	the message

TP ld	TP_SEC_ITSS_RCV_CERT_17_02_BO	
Summary	Check that IUT discards a SecuredMessage if the subject attribute of type assurance_level	
	is missing in the AA certificate	
Reference	ETSI TS 103 097 [1], clause 7.4.1	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	e 'authorized' state	
and the IUT current time is inside the time validity period of CERT_TS_17_02_BO_AT		
ensure that		
when the IUT is rec	when the IUT is receiving a Secured CAM (MSG_SEC_RCV_CAM_1)	
containing heade	containing header_fields ['signer_info'].signer	
containing type		
indicating 'c	ertificate'	
and containing certificate (CERT_TS_17_02_BO_AT)		
containing signer_info.digest		
referencing to certificate (CERT_TS_17_02_BO_AA)		
not containing subject_attributes['assurance_level']		
then		
the IUT discards	the message	

TP ld	TP_SEC_ITSS_RCV_CERT_17_03_BO
	Check that IUT discards a SecuredMessage if the assurance level of issuing certificate is
Summary	less then assurance level of subordinate certificate
Deference	
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	
and the IUT current	time is inside the time validity period of CERT_TS_17_03_BO_AT
ensure that	
when the IUT is rec	eiving a Secured CAM (MSG_SEC_RCV_CAM_1)
containing heade	r_fields ['signer_info'].signer
containing type	
indicating 'c	
and containing	certificate (CERT_TS_17_03_BO_AT)
containing s	ubject_attributes['assurance_level']
containing	g assurance_level
	ng 0x80 (assurance level=4, confidence=0)
and contain	ng signer_info.digest
referencir	ng to certificate (CERT_TS_A_AA)
containing subject_attributes['assurance_level']	
containing assurance_level	
in	dicating 0x60 (assurance level=3, confidence=0)
then	
the IUT discards	the message

TP ld	TP_SEC_ITSS_RCV_CERT_17_04_BO
	Check that IUT discards a SecuredMessage if the assurance level of issuing certificate is
Summary	equal to the assurance level of the subordinate certificate but the confidence of subject
	assurance of issuing certificate is less then the confidence of the subordinate certificate
Reference	ETSI TS 103 097 [1], clause 7.4.1
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the IUT being in the	'authorized' state
and the IUT current	time is inside the time validity period of CERT_TS_17_04_BO_AT
ensure that	
	eiving a Secured CAM (MSG_SEC_RCV_CAM_1)
	_fields ['signer_info'].signer
containing type	
indicating 'ce	
	certificate (CERT_TS_17_04_BO_AT)
	ubject_attributes['assurance_level']
	assurance_level
	ng 0x61 (assurance level=3, confidence=1)
	ng signer_info.digest
	g to certificate (CERT_TS_A_AA)
	ng subject_attributes['assurance_level']
	ining assurance_level
	licating 0x60 (assurance level=3, confidence=0)
then	
the IUT discards t	he message

TP ld	TP_SEC_ITSS_RCV_CERT_18_01_BO	
Summary	Check that IUT discards a SecuredMessage if the subject attribute of type verification_key is	
	missing in the AT certificate	
Reference	ETSI TS 103 097 [1], clause 7.4.1	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the IUT being in the	e 'authorized' state	
and the IUT curren	t time is inside the time validity period of CERT_TS_18_01_BO_AT	
ensure that		
when the IUT is rea	ceiving a Secured CAM (MSG_SEC_RCV_CAM_1)	
containing head	er_fields ['signer_info'].signer	
containing typ	e	
indicating 'c	certificate'	
and containing certificate (CERT_TS_18_01_BO_AT)		
not contain	ng subject_attributes['verification_key']	
then		
the IUT discards	the message	

#### Check certificate verification key presence 5.3.5.18

TP ld	TP_SEC_ITSS_RCV_CERT_18_02_BO		
Summary	Check that IUT discards a SecuredMessage if the subject attribute of type verification_key is		
	missing in the AA certificate		
Reference	ETSI TS 103 097 [1], clause 7.4.1		
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_18_02_BO_AT		
ensure that	ensure that		
	a Secured CAM (MSG_SEC_RCV_CAM_1)		
containing header_field	ds ['signer_info'].signer		
0,11	containing type		
	indicating 'certificate'		
	icate (CERT_TS_18_02_BO_AT)		
containing signer_info.digest			
referencing to certificate (CERT_TS_18_02_BO_AA)			
	g subject_attributes['verification_key']		
then			
the IUT discards the message			

#### Check invalid region type in validity restriction of certificates 5.3.5.19

TP ld	TP_SEC_ITSS_RCV_CERT_19_01_BO		
Summary	Check that IUT discards a SecuredMessage if the reserved region type has been used in region validity restriction of the AT certificate		
Reference	ETSI TS 103 097 [1], clause 4.2.21		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
containing hea containing v	ng a SecuredMessage der_fields ['signer_info'].signer.certificate (CERT_TS_19_01_BO_AT) alidity_restrictions['region'] g region_type		
the IUT discards	the message		

• 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".

183

# History

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