# ETSITS 103 525-2 V1.2.1 (2022-01)



Intelligent Transport Systems (ITS); Testing;

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

# Reference RTS/ITS-005208 Keywords ITS, security, testing, TSS&TP

#### **ETSI**

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

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

Siret N° 348 623 562 00017 - APE 7112B Association à but non lucratif enregistrée à la Sous-Préfecture de Grasse (06) N° w061004871

#### Important notice

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

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

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

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

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

#### Notice of disclaimer & limitation of liability

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

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

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

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

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

#### Copyright Notification

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

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

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

© ETSI 2022. All rights reserved.

# Contents

Intelle	ectual Property Rights	5
Forew	vord	5
Moda	l verbs terminology	5
1	Scope	6
2	References	6
2.1	Normative references	
2.2	Informative references.	
3	Definition of terms, symbols and abbreviations	7
3.1	Terms	
3.2	Symbols	7
3.3	Abbreviations	7
4	Test Suite Structure (TSS)	8
4.1	Structure for Security tests	
4.2	Test entities and states	
4.2.1	ITS-S states	
4.2.2	EA states	
4.2.3	AA states	
4.2.4	RootCA states	
4.2.5	TLM states	
4.3	Test configurations	
4.3.1	Overview	
4.3.2	Enrolment	10
4.3.2.1	Configuration CFG_ENR_ITSS	10
4.3.2.2	· · · · · · · · · · · · · · · · · · ·	
4.3.3	Authorization	
4.3.3.1	Configuration CFG_AUTH_ITSS	10
4.3.3.2	Configuration CFG_AUTH_AA	11
4.3.4	Authorization Validation	
4.3.4.1		
4.3.4.2	<i>b</i> = =	
4.3.5	CA certificate generation	
4.3.5.1		
4.3.5.2		
4.3.5.3	- · · · · · · · · · · · · · · · · · · ·	
4.3.6	ECTL generation	
4.3.6.1		12
4.3.6.2		
4.3.7	Root CTL generation	
4.3.7.1	6 = =	
4.3.8	CRL generation	
4.3.8.1 4.3.9	ITS-S CRL/CTL handling	
4.3.9 4.3.9.1		
5	Test Purposes (TP)	
5.1	Introduction	
5.1.1	TP definition conventions	
5.1.2	TP Identifier naming conventions	
5.1.3	Rules for the behaviour description	
5.1.4	Sources of TP definitions	
5.1.5	Mnemonics for PICS reference	
5.1.6	Certificates content	
5.2	ITS-S behaviour	
5.2.0	Overview	
5.2.1	Manufacturing	15

5.2.2	Enrolment	15
5.2.2.0	Overview	15
5.2.2.1	Enrolment request	16
5.2.2.2	Enrolment response handling	21
5.2.2.3	Enrolment request repetition	22
5.2.3	Authorization	
5.2.3.0	Overview	24
5.2.3.1	Authorization request	24
5.2.3.2	Authorization response handling	33
5.2.3.3	Authorization request repetition	33
5.2.4	CTL handling	35
5.2.5	CTL distribution	36
5.2.6	CRL handling	42
5.2.7	CRL distribution	44
5.3	Common CA behaviour	47
5.3.0	Overview	47
5.3.1	Certificate validation	48
5.3.1.1	Basic certificate content	48
5.3.1.2	Check certificate region validity restriction	51
5.3.1.3	Check ECC point type of the certificate signature	55
5.3.1.4	Check ECC point type of the certificate public keys	55
5.3.1.5	Verify certificate signatures	56
5.3.1.6	Verify certificate permissions	
5.3.1.7	Check time validity restriction in the chain	60
5.4	EA behaviour	60
5.4.0	Overview	60
5.4.1	Enrolment request handling	60
5.4.2	Enrolment response	66
5.4.3	Authorization validation request handling	
5.4.4	Authorization validation response	72
5.4.5	CA Certificate Request	
5.5	AA behaviour	
5.5.0	Overview	
5.5.1	Authorization request handling	81
5.5.2	Authorization validation request	
5.5.3	Authorization validation response handling	
5.5.4	Authorization response	
5.5.5	CA Certificate Request	
5.6	RootCA behaviour	
5.6.0	Overview	
5.6.1	CTL generation	
5.6.2	CRL generation	
5.6.3	CA certificate generation	
5.7	DC behaviour	
5.8	TLM behaviour	
5.8.1	CTL generation	
5.9	CPOC behaviour	128
History		120

# Intellectual Property Rights

#### **Essential patents**

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

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

#### **Trademarks**

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

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

# **Foreword**

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

The present document is part 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 [4].

# Modal verbs terminology

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

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

# 1 Scope

The present document provides the Test Suite Structure and Test Purposes (TSS & TP) for PKI management as defined in ETSI TS 102 941 [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 102 941 (V1.4.1): "Intelligent Transport Systems (ITS); Security; Trust and Privacy
	Management".

- [2] ETSI TS 103 097 (V1.4.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".
- [3] IEEE Std 1609.2<sup>TM</sup>-2016: "IEEE Standard for Wireless Access in Vehicular Environments Security Services for Applications and Management Messages", as amended by IEEE Std 1609.2a<sup>TM</sup>-2017: "Standard for Wireless Access In Vehicular Environments Security Services for Applications and Management Messages Amendment 1".
- [4] ETSI TS 103 525-1 (V1.2.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 1: Protocol Implementation Conformance Statement (PICS)".
- [5] ETSI TS 103 096-2 (V1.5.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 2: Test Suite Structure and Test Purposes (TSS & TP)".
- [6] ETSI TS 103 601 (V1.1.1): "Intelligent Transport Systems (ITS); Security; Security management messages communication requirements and distribution protocols".

## 2.2 Informative references

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

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

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

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

[i.2]	ETSI TS 102 965 (V1.3.1): "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration".
[i.3]	ISO/IEC 9646-1 (1994): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 1: General concepts".
[i.4]	ISO/IEC 9646-2 (1994): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 2: Abstract Test Suite specification".
[i.5]	ISO/IEC 9646-6 (1994): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 6: Protocol profile test specification".
[i.6]	ISO/IEC 9646-7 (1995): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 7: Implementation Conformance Statements".
[i.7]	ETSI ETS 300 406 (1995): "Methods for testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".
[i.8]	United Nations Statistics Division: "Standard country or area codes for statistical use (M49)".

# 3 Definition of terms, symbols and abbreviations

#### 3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 102 941 [1], ETSI TS 103 097 [2], ETSI TS 103 525-1 [4], ETSI TS 102 965 [i.2], ISO/IEC 9646-6 [i.5], ISO/IEC 9646-7 [i.6] and the following apply:

AID\_CERT\_REQ: "Secured certificate request service" ITS-AID

AID\_CTL: "CTL service" ITS-AID
AID\_CRL: "CRL service" ITS-AID

# 3.2 Symbols

Void.

## 3.3 Abbreviations

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

AA Authorization Authority
AID Application IDentifier

AID\_CAM ITS Application IDentifier for CAM AID\_DENM Application Identifier for DENM

AID\_GN Application Identifier for general GeoNetworking messages

AT Authorization Ticket
ATS Abstract Test Suite
BO exceptional BehaviOur
BV Valid Behaviour
CA Certification Authority

CAM Co-operative Awareness Messages

CERT CERTificate

CRL Certificate Revocation List
CTL Certificate Trust List

DENM Decentralized Environmental Notification Message

EA Enrolment Authority
ECC Elliptic Curve Cryptography

ECTL European Certificate Trust List

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
TS Test System
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 Management** 

Root	Group	Sub-Group	Category
Security Management	ITS-S	Enrolment	Valid
		Authorization	Valid
		CRL handling	Valid
		CTL handling	Valid
	CA	Common Certificate Authority	Valid
	EA	Enrolment	Valid
		Authorization Validation	Valid
		CA certificate generation	Valid
		CRL handling	Valid
		CTL handling	Valid
	AA	Authorization	Valid
		Authorization Validation	Valid
		CA certificate generation	Valid
		CRL handling	Valid
		CTL handling	Valid
	RootCA	CA certificate generation	Valid
		CTL/CRL generation	Valid
	DC	CTL/CRL distribution	Valid
	TLM	ECTL generation	Valid
		TLM certificate generation	Valid
	CPOC	ECTL distribution	Valid

# 4.2 Test entities and states

#### 4.2.1 ITS-S states

- State 'initialized':
  - ITS-S in 'initialized' state is ready to perform the enrolment request.
  - ITS-S in 'initialized' state contains following information elements:
    - permanent canonical identifier (PCI);
    - public/private key pair for cryptographic purposes (canonical key pair);
    - the trust anchor (Root CA) public key certificate and the DC network address;

- contact information for the EA which will issue certificates for the ITS-S:
  - network address;
  - public key certificate.

#### • State 'enrolled':

- ITS-S in 'enrolled' state has successfully performed the enrolment request process.
- ITS-S in 'enrolled' state is ready to perform an authorization request.
- ITS-S in 'enrolled' state contains all information elements of the 'initialized' state and additionally:
  - enrolment credential (EC) with the condition of being neither expired nor revoked;
  - private key corresponding to the EC public encryption key;
  - private key corresponding to the EC public verification key.

#### • State 'authorized':

- ITS-S in 'authorized' state has successfully performed the authorization request process.
- ITS-S in 'authorized' state contains all information elements of the 'enrolled' state and additionally:
  - one or more authorization tickets (AT):
    - being not expired;
    - of which at least one is currently valid;
  - all private keys corresponding to the AT public verification keys;
  - if applicable: all private keys corresponding to the AT public encryption keys.

#### 4.2.2 EA states

- State 'initial':
  - EA contains following information elements:
    - the trust anchor (Root CA) public key certificate and the DC network address.
- State 'operational':
  - EA is ready to receive enrolment requests from ITS-S.
  - In addition to information elements enumerated in the 'initial' state, EA in the 'operational' state contains following information elements:
    - public/private key pairs and EA certificate permitting issuing of enrolment certificates.

#### 4.2.3 AA states

- State 'initial':
  - AA in initial state contains following information elements:
    - the trust anchor (Root CA) public key certificate and the DC network address;
- State 'operational':
  - public/private key pairs and AA certificate permitting issuing of authorization tickets (AT certificates);
  - root CTL containing trusted EA certificates;

the EA access point URL.

#### 4.2.4 RootCA states

- State 'operational':
  - RootCA is offline, but can generate CRL, CTL, AA, EA, RCA, etc. certificates by manual request.

#### 4.2.5 TLM states

- State 'operational':
  - TLM is offline, but can generate ECTL by manual request.

# 4.3 Test configurations

#### 4.3.1 Overview

#### 4.3.2 Enrolment

#### 4.3.2.1 Configuration CFG\_ENR\_ITSS

IUT: ITS-S in the state 'initialized':

- Following information elements shall be provided by IUT for the EA emulated by the TS:
  - Permanent Canonical Identifier (PCI);
  - public key of canonical key pair;
  - profile information.

TS: EA is emulated by TS.

#### 4.3.2.2 Configuration CFG\_ENR\_EA

IUT: EA is in the state 'operational', ready to handle enrolment requests and contains following information about ITS-S emulated by the TS:

- the permanent canonical identifier of the emulated ITS-S;
- the profile information for the emulated ITS-S;
- the public key from the canonical key pair belonging to the emulated ITS-S.

TS: ITS-S is emulated by the TS.

#### 4.3.3 Authorization

#### 4.3.3.1 Configuration CFG\_AUTH\_ITSS

IUT: ITS-S in the state 'enrolled' and containing following information:

- the AA certificate of the emulated AA;
- the EA certificate of the emulated EA:
- the EC certificate issued by the emulated EA.

The URL of the emulated AATS: AA is emulated by the TS.

#### 4.3.3.2 Configuration CFG\_AUTH\_AA

IUT: AA in the operational state and containing following information:

• The profile information for the emulated ITS-S.

TS: ITS-S is emulated by the TS:

• EA is emulated by the TS and validates all incoming requests.

#### 4.3.4 Authorization Validation

#### 4.3.4.1 Configuration CFG\_AVALID\_AA

IUT: AA in the operational state and containing following information:

- the certificate of the emulated EA;
- the URL of the emulated EA.

TS: EA is emulated by the TS and ready to receive authorization validation requests:

• ITS-S is emulated by TS to trigger the authorization process.

## 4.3.4.2 Configuration CFG\_AVALID\_EA

IUT: EA is in the operational state, ready to handle authorization validation requests and contains following information about AA and ITS-S emulated by the TS:

- the permanent canonical identifier of the emulated ITS-S;
- the profile information for the emulated ITS-S;
- the public key from the key pair belonging to the emulated ITS-S.

TS: AA and ITS-S are emulated by the TS and contain following information elements:

- EC certificate issued by IUT;
- EA certificate of IUT;
- the URL of the EA.

# 4.3.5 CA certificate generation

#### 4.3.5.1 Configuration CFG\_CAGEN\_INIT

IUT: CA (EA or AA) in the initial state.

TS: TS checks generated certificate requests and does not emulate any ITS entity.

#### 4.3.5.2 Configuration CFG\_CAGEN\_REKEY

IUT: CA (EA or AA) in the operational state.

TS: TS checks generated certificate requests and does not emulate any ITS entity.

#### 4.3.5.3 Configuration CFG\_CAGEN\_RCA

IUT: Offline RootCA in operational state, generating EA, AA or RCA certificate.

TS: TS checks generated certificate and does not emulate any ITS entity.

#### 4.3.6 ECTL generation

#### 4.3.6.1 Configuration CFG\_CTLGEN\_TLM

IUT: TLM in the operational state.

TS: TS checks generated CTL and does not emulate any ITS entity.

#### 4.3.6.2 Configuration CFG\_CTLGEN\_CPOC

IUT: CPOC in the operational state.

TS: TS checks generated CTL emulating http client of CPOC.

# 4.3.7 Root CTL generation

#### 4.3.7.1 Configuration CFG\_CTLGEN\_RCA

IUT: RCA in the operational state.

TS: TS checks generated CTL and does not emulate any ITS entity.

## 4.3.8 CRL generation

#### 4.3.8.1 Configuration CFG\_CRLGEN\_RCA

IUT: RCA in the operational state.

TS: TS checks generated CRL and does not emulate any ITS entity.

# 4.3.9 ITS-S CRL/CTL handling

#### 4.3.9.1 Configuration CFG\_CXL\_P2P

IUT: ITS-S in the state 'authorized' and containing following information:

- the RCA certificate of the emulated RCA;
- the AT certificate issued by the emulated AA;
- the AA certificate of the emulated AA;
- the EA certificate of the emulated EA;
- the EC certificate issued by the emulated EA;
- the URL of the emulated DC.

Neighbour ITS-S: is emulated by the TS.

RCA: is emulated by the TS.

DC: is emulated by the TS.

# 5 Test Purposes (TP)

#### 5.1 Introduction

#### 5.1.1 TP definition conventions

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

# 5.1.2 TP Identifier naming conventions

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

**Table 2: TP naming convention** 

Identifier	TP_ <root>_<tgt>_<gr>_<sn>_<x></x></sn></gr></tgt></root>		
	<root> = root</root>	SECPKI	
	<tgt> = target</tgt>	ITSS	ITS-Station
		CA	Common Certificate Authority
		AA	Authorization Authority
		EA	Enrolment Authority
		RCA	Root Certification Authority
		DC	Distribution Center
		CPOC	C-ITS Point of Contact
	<gr> = group</gr>	ENR	Enrolment
		AUTH	Authorization
		AUTHVAL	Authorization Validation
		CRL	CRL handling
		CTL	CTL handling
		CERTGEN	Certificate generation
		CTLGEN	CTL generation
		ECTLGEN	ECTL generation
		CRLGEN	CRL generation
		LISTDIST	CTL/CRL/ECTL distribution
		TLMCERTGEN	TLM certificate generation
	<sgr>=sub-group</sgr>	SND	Sending behaviour
		RCV	Receiving behaviour
		REP	Repetition behaviour
·	<sn> = test purpose sequential number</sn>		01 to 99
	<x> = category</x>	BV	Valid Behaviour tests
		BI	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 102 941 [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 102 941 [1] which shall be followed as specified in the clauses below.

# 5.1.5 Mnemonics for PICS reference

To avoid an update of all TPs when the PICS document is changed, Table 3 introduces mnemonics name and the correspondence with the real PICS item number. The 'PICS item' as defined in tables provided in clause A.6 of ETSI TS 103 525-1 [4] and in IEEE 1609.2 [3] shall be used to determine the test applicability.

**Table 3: Mnemonics for PICS reference** 

Mnemonic	PICS item
PICS_SECPKI_IUT_ITSS	[4] A.3.1
PICS_SECPKI_IUT_EA	[4] A.4.2
PICS_SECPKI_IUT_AA	[4] A.4.3
PICS_SECPKI_IUT_RCA	[4] A.4.4
PICS_SECPKI_IUT_DC	[4] A.4.5
PICS_SECPKI_IUT_TLM	[4] A.4.6
PICS_SECPKI_IUT_CPOC	[4] A.4.7
PICS_SECPKI_ENROLMENT	[4] A.3.2 or A.5.1
PICS_SECPKI_ENROLMENT_RETRY	[4] A.3.2.2 or A.5.4
PICS_SECPKI_REENROLMENT	[4] A.3.2.1 or A.5.2
PICS_SECPKI_AUTHORIZATION	[4] A.3.3 or A.6.1
PICS_SECPKI_ AUTHORIZATION _RETRY	[4] A.3.3.3 or A.6.5
PICS_SECPKI_AUTH_PRIVACY	[4] A.3.3.1 or A.6.3
PICS_SECPKI_AUTH_POP	[4] A.3.3.2 or A.6.2
PICS_SECPKI_AUTH_VALIDATION	[4] A.5.3
PICS_SECPKI_CRL	[4] A.9.5 or A.7.1
PICS_SECPKI_CRL_DOWNLOAD	[4] A.9.6
PICS_SECPKI_CRL_BROADCAST	[4] A.9.9
PICS_SECPKI_CTL	[4] A.9.3 or A.7.2
PICS_SECPKI_CTL_DELTA	[4] A.9.3.1 or A.7.2.1 or A.7.4.1
PICS_SECPKI_CTL_DOWNLOAD	[4] A.9.4
PICS_SECPKI_CTL_BROADCAST	[4] A.9.8
PICS_SECPKI_ECTL	[4] A.9.1 or A.8.1
PICS_SECPKI_ECTL_DELTA	[4] A.9.1.1 or A.8.1.1 or A.8.2.1
PICS_SECPKI_ECTL_DOWNLOAD	[4] A.9.2 or A.8.3
PICS_SECPKI_ECTL_BROADCAST	[4] A.9.7
PICS_SEC_SHA256	[3] S1.2.2.1.1 or S1.3.2.1.1
PICS_SEC_SHA384	[3] S1.2.2.1.2 or S1.3.2.1.2
PICS_SEC_BRAINPOOL_P256R1	[3] S1.2.2.4.1.2 or S1.3.2.4.1.2
PICS_SEC_BRAINPOOL_P384R1	[3] S1.2.2.4.2 or S1.3.2.4.2
PICS_SEC_IMPLICIT_CERTIFICATES	[3] S1.2.2.8, S1.3.2.7 and S1.3.2.9
PICS_SEC_EXPLICIT_CERTIFICATES	[3] S1.2.2.7, S1.3.2.6 and S1.3.2.8

# 5.1.6 Certificates content

The certificates, defined in ETSI TS 103 096-2 [5], clause 6.1.1 is applicable for the present document. Additional certificates used in the test purposes are defined in the Table 4.

**Table 4: Certificates content** 

AA certificate	Content	To be installed on
AA certificate  CERT_IUT_A_AA	Signer digest of the CERT_IUT_A_CA     application permissions:         CRT_REQ with SSP 0x0132;     certificate issuing permissions (SSP value/mask):         CAM with all possible SPP (0x01FFFC / 0xFF0003);         DENM with all possible SSP (0x01FFFFF / 0xFF000000);         SPATEM with all possible SSP (0x01E0 / 0xFF1F);         MAPEM with all possible SSP (0x01C0 / 0xFF3F);         IVIM with all possible SSP (0x01000000FF8 / 0xFF000000007);         SREM with all possible SSP (0x01FFFFE0 / 0xFF00001F);         SSEM with all possible SSP (0x01 / 0xFF);         GPC with all possible SSP (0x01 / 0xFF);	To be installed on the IUT  Yes
	<ul> <li>GN-MGMT without SSP;</li> <li>validation time for 3 years;</li> <li>no region restriction;</li> <li>assurance level 4;</li> <li>verification key of type compressed with NIST P256R curve;</li> <li>encryption key of type compressed with NIST P256R curve;</li> </ul>	
CERT_IUT_A_CA	<ul> <li>valid signature of type x-only with NIST P256R curve;</li> <li>same as CERT_IUT_A_AA;</li> </ul>	Yes
CERT_IUT_I_CA	<ul> <li>same as CERT_IUT_A_CA;</li> <li>type implicit;</li> <li>not containing signature;</li> <li>not containing verification key;</li> <li>containing reconstruction value.</li> </ul>	Yes

# 5.2 ITS-S behaviour

#### 5.2.0 Overview

All test purposes in the present clause may be included in the test sequence if following PICS items are set:

PICS\_SECPKI\_IUT\_ITSS = TRUE

# 5.2.1 Manufacturing

The manufacturing procedure defined in ETSI TS 102 941 [1] is out of scope of the present document.

# 5.2.2 Enrolment

#### 5.2.2.0 Overview

All test purposes in clause 5.2.2 may be included in the test sequence if following PICS items are set:

 $PICS\_SECPKI\_ENROLMENT = TRUE$ 

# 5.2.2.1 Enrolment request

TP Id	SECPKI_ITSS_ENR_01_BV	
Summary	Check that IUT sends an enrolment request when triggered	
Reference	ETSI TS 102 941 [1], clause 6.1.3	
Configuration	CFG_ENR_ITSS	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the 'initi	alized' state	
ensure that		
when		
the IUT is triggered to requested a new Enrolment Certificate (EC)		
then		
the IUT sends to FA an EnrolmentRequestMessage		

TP Id SECPKI_ITSS_ENR_02_BV		
Summary	If the enrolment request of the IUT is an initial enrolment request, the itsld (contained in the InnerECRequest) shall be set to the canonical identifier, the signer (contained in the outer EtsiTs1030971Data-Signed) shall be set to self and the outer signature shall be computed using the canonical private key	
Reference	ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1	
Configuration	CFG_ENR_ITSS	
PICS Selection		
	Expected behaviour	
with the IUT being in the 'initialized' state ensure that when the IUT is requested to send an EnrolmentRequestMessage then the IUT sends an EtsiTs103097Data-Encrypted containing an encrypted EtsiTs103097Data-Signed containing EtsiTs103097Data containing InnerECRequestSignedForPOP containing InnerEcRequest containing itsId indicating the canonical identifier of the ITS-S and containing signer		
and containing signature computed using the canonical private key		

TP Id	SECPKI_ITSS_ENR_03_BV		
Summary	In presence of a valid EC, the enrolment request of the IUT is a rekeying enrolment request with the itsId (contained in the InnerECRequest) and the SignerIdentifier (contained in the outer EtsiTs1030971Data-Signed) both declared as digest containing the HashedId8 of the EC and the outer signature computed using the current valid EC private key corresponding to the verification public key		
Reference	ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1		
Configuration	CFG_ENR_ITSS		
PICS Selection	PICS_SECPKI_REENROLMENT		
	Expected behaviour		
ensure that when the IUT is requested then the IUT sends an Ets containing an end containing Et containing containing	with the IUT being in the 'enrolled' state ensure that when the IUT is requested to send an EnrolmentRequestMessage		
containing itsId declared as digest containing the HashedId8 of the EC identifier and containing signer declared as digest containing the HashedId8 of the EC identifier and containing signature computed using the current valid EC private key corresponding to the verification public key			

TP ld	SECPKI_ITSS_ENR_04_BV	
Summary	If the EC is revoked, the IUT returns to the state 'initialized'	
Reference	ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1	
Configuration	CFG_ENR_ITSS	
PICS Selection	PICS_SECPKI_CRL	
	Expected behaviour	
with		
the IUT being in the 'enre	olled' state	
ensure that		
when		
the IUT is informed about a revocation of its EC		
then		
the IUT returns to the 'initialized' state		

TP ld	SECPKI_ITSS_ENR_05_BV		
Summary	If the EC expires, the IUT returns to the state 'initialized'		
Reference	ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1		
Configuration	CFG_ENR_ITSS		
PICS Selection			
	Expected behaviour		
with the IUT being in the 'enrolled' state ensure that when the EC of the IUT expires then the IUT returns to the 'initialized' state			

TP Id		SECPKI_ITSS_ENR_06_BV
Summary	For each enrolment request, the ITS-S shall generate a new verification key pair	
		corresponding to an approved signature algorithm as specified in ETSI TS 103 097 [2]
Reference		ETSI TS 102 941 [1], clause 6.2.3.2.1
Kererence		ETSI TS 103 097 [2], clause 7
Configura	tion	CFG_ENR_ITSS
PICS Sele	ction	PICS_SECPKI_REENROLMENT
		Expected behaviour
with		
the IUT	being in the 'initia	alized' state
ensure tha	t	
when	when	
the IUT is requested to send multiple EnrolmentRequestMessage		
then		
each EnrolmentRequestMessage		
contains a different and unique verification key pair within the InnerECRequest.		
NOTE:	NOTE: The first EnrolmentRequestMessage should be an initial request, the following EnrolmentRequestMessages	
	should be rekeyin	g requests.

TP Id	SECPKI_ITSS_ENR_07_BV		
Summary	Within the InnerECRequest, the requestedSubjectAttributes shall not contain a		
	certIssuePermissions field		
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.1		
Configuration	CFG_ENR_ITSS		
PICS Selection			
	Expected behaviour		
with			
the IUT being in the X_S	STATE		
ensure that			
when			
the IUT is requested	the IUT is requested to send an EnrolmentRequestMessage		
then			
the IUT sends an EtsiTs103097Data-Encrypted			
containing an end	crypted EtsiTs103097Data-Signed		
containing Ef	tsiTs103097Data		
containin	containing InnerECRequestSignedForPOP		
containing InnerEcRequest			
containing requestedSubjectAttributes			
not containing certIssuePermissions			
Variants			
nn X_STATE			
1 'initialized' state			
2 'enrolled' state			

TP Id	SECPKI_ITSS_ENR_08_BV		
Summary	In the headerInfo of the tbsData of the InnerECRequestSignedForPOP all other components of the component tbsdata.headerInfo except generationTime and psid are not used and absent. The psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [i.2] and the generationTime shall be present		
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.1		
Configurat	ion CFG_ENR_ITSS		
PICS Selec	etion		
	Expected behaviour		
with			
the IUT	being in the X_STATE		
ensure that			
when			
	the IUT is requested to send an EnrolmentRequestMessage		
	then		
the IUT sends an EtsiTs103097Data-Encrypted			
	containing an encrypted EtsiTs103097Data-Signed		
	containing EtsiTs103097Data		
containing InnerECRequestSignedForPOP			
	containing the Data		
	containing headerInfo		
	containing psid indicating AID_CERT_REQ		
and containing generationTime			
	and not containing any other component of tbsdata.headerInfo		
Variants	, y . /		
nn	X_STATE		
1	'initialized' state		
2	'enrolled' state		

TP ld	SECPKI_ITSS_ENR_09_BV	
	In the headerInfo of the tbsData of the outer EtsiTs102941Data-Signed all other	
Summary	components of the component tbsdata.headerInfo except generationTime and psid are not	
Cullinary	used and absent. The psid shall be set to "secured certificate request" as assigned in ETSI	
	TS 102 965 [i.2] and the generationTime shall be present	
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.1	
Configuration	CFG_ENR_ITSS	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the X	_STATE	
ensure that		
when		
the IUT is requeste	ed to send an EnrolmentRequestMessage	
then		
	the IUT sends an EtsiTs103097Data-Encrypted	
	encrypted EtsiTs103097Data-Signed	
	containing tbsData	
containing headerInfo		
	containing psid	
indicating AID_CERT_REQ		
and containing generationTime		
	and not containing any other component of tbsdata.headerInfo	
Variants		
nn X_STATE		
1 'initialized' sta		
2 'enrolled' stat	е	

TP Id	SECPKI_ITSS_ENR_10_BV
Summary	The EtsiTs103097Data-Encrypted containing the correctly encrypted ciphertext and a recipients component containing one instance of RecipientInfo of choice certRecipInfo containing the hashedId8 of the EA certificate in recipientId and the encrypted data encryption key in encKey. The data encryption key is encrypted using the public key found in the EA certificate referenced in the recipientId
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.1
Configura	tion CFG_ENR_ITSS
PICS Selec	ction
	Expected behaviour
ensure that when the then the	being in the X_STATE t  IUT is requested to send an EnrolmentRequestMessage  IUT sends an EtsiTs103097Data-Encrypted containing recipients     containing exactly one instance of RecipientInfo of choice certRecipInfo     containing recipientId
	indicating the hashedId8 referencing to the EA certificate containing encryptionKey (KEY) and containing encKey being a symmetric key (SYMKEY) encrypted using the key KEY containing ciphertext which is encrypted using the symmetric key SYMKEY contained in encKey
Variants	
nn	X_STATE
1	'initialized' state

'enrolled' state

TP Id	SECPKI_ITSS_ENR_11_BV		
	In the inner signed data structure (InnerECRequestSignedForPOP), the signature is		
Summary	computed on InnerECRequest with the private key corresponding to the new		
	verificationKey to prove possession of the generated verification key pair		
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.1		
Configuration	CFG_ENR_ITSS		
PICS Selection			
	Expected behaviour		
with			
the IUT being in the X_S	STATE		
ensure that			
when	when		
the IUT is requested	to send an EnrolmentRequestMessage		
then	·		
	siTs103097Data-Encrypted		
containing an encrypted EtsiTs103097Data-Signed			
containing Et	containing EtsiTs103097Data		
containing	g InnerECRequestSignedForPOP		
conta	aining tbsData		
containing InnerEcRequest			
containing verificationKey (VKEY)			
containing signature			
computed on InnerECRequest			
using the private key corresponding to VKEY			
contained in InnerECRequest			
	Variants		
nn X_STATE			
1 'initialized' state			
2 'enrolled' state			

TP ld	SECPKI_ITSS_ENR_12_BV		
Summary	Check that signing of Enrolment Request message is permitted by the EC certificate		
Reference	ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1		
Configuration	CFG_ENR_ITSS		
PICS Selection	PICS_SECPKI_REENROLMENT		
	Expected behaviour		
with			
the IUT being in the 'enro	olled' state		
ensure that			
when			
	to send an EnrolmentRequestMessage		
	then		
the IUT sends an EtsiTs103097Data-Encrypted			
containing an encrypted EtsiTs103097Data-Signed			
	containing signer containing digest		
indicating HashedId8 of the EC certificate			
containing appPermissions			
containing an item of type PsidSsp			
containing psid			
indicating AID_CERT_REQ			
and containing ssp			
containing opaque[0] (version)			
	indicating 1		
	containing opaque[1] (value)		
indicating 'Enrolment Request' (bit 1) set to 1			

# 5.2.2.2 Enrolment response handling

TP ld	SECPKI_ITSS_ENR_RCV_01_BV		
Summary	If an enrolment request fails, the IUT returns to the state 'initialized		
Reference	ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1		
Configuration	CFG_ENR_ITSS		
PICS Selection			
	Expected behaviour		
with			
the IUT being in the X_S	the IUT being in the X_STATE		
and the IUT has sent the	and the IUT has sent the EnrolmentRequestMessage		
ensure that			
when	when		
the IUT received the	the IUT received the EnrolmentResponseMessage		
containing a responseCode different than 0			
then			
the IUT returns to the X_STATE state			
Variants			
nn X_STATE			
1 'initialized' state			
2 'enrolled' state			

TP Id	SECPKI_ITSS_ENR_RCV_02_BV
Summary	The IUT is capable of parsing and handling of positive EnrolmentResponse messages containing the requested EC. In case of a successful enrolment, the IUT switches to the state 'enrolled'
Reference	ETSI TS 102 941 [1], clauses 6.1.3, 6.2.3.2.1 and 6.2.3.2.2
Configuration	CFG_ENR_ITSS
PICS Selection	
	Expected behaviour
with the IUT being in the 'initialized' state and the IUT has sent the EnrolmentRequestMessage ensure that when the IUT receives a subsequent EnrolmentResponseMessage as an answer of the EA containing a responseCode indicating 0 and containing an enrolment certificate	
the IUT switches to the 'enrolled' state	

# 5.2.2.3 Enrolment request repetition

All test purposes in clause 5.2.2.3 may be included in the test sequence if following PICS items are set:

• PICS\_SECPKI\_ ENROLMENT \_RETRY = TRUE

TP Id	SECPKI_ITSS_ENR_REP_01_BV	
Summary	Check that IUT repeats an enrolment request when response has not been received	
Reference	ETSI TS 103 601 [6], clause 5.1.2	
Configuration	CFG_ENR_ITSS	
PICS Selection		
	Expected behaviour	
with		
the IUT being in th	e 'initialized' state	
and the IUT alread	ly sent the Enrolment Request at the time T1	
and the IUT has no	and the IUT has not yet received the Enrolment Response	
ensure that		
when		
the IUT local time is reached the T1 + PIXIT_ENR_TIMEOUT_TH1		
then		
the IUT sends	the IUT sends to EA an EnrolmentRequestMessage	

TP ld	SECPKI_ITSS_ENR_REP_02_BV
Summary	Check that IUT uses the same message to perform enrolment retry
Reference	ETSI TS 103 601 [6], clause 5.1.2
Configuration	CFG_ENR_ITSS
PICS Selection	
	Expected behaviour
with the IUT being in the 'initialized' state and the IUT already sent the Enrolment Request (M) ensure that when the IUT is triggered to re-send an Enrolment Request then the IUT sends M to EA	

TP Id	SECPKI_ITSS_ENR_REP_03_BV	
Summani	Check that IUT stops sending the Enrolment Request message if Enrolment Response	
Summary	message has been received	
Reference	ETSI TS 103 601 [6], clause 5.1.2	
Configuration	CFG_ENR_ITSS	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the 'initialized' state		
and the IUT has sent the Enrolment Request more than 1 time		
ensure that		
when		
the IUT receives an Enrolment Response		
then		
the IUT stops sending Enrolment Requests to EA		

TP ld	SECPKI_ITSS_ENR_REP_04_BV		
Summary	Check that IUT stops sending the Enrolment Request message if maximum number of		
Summary	retry has been reached		
Reference	ETSI TS 103 601 [6], clause 5.1.2		
Configuration	CFG_ENR_ITSS		
PICS Selection			
	Expected behaviour		
with			
the IUT being in the 'ini	the IUT being in the 'initialized' state		
and the IUT has started sending the Enrolment Request			
ensure that			
when			
the IUT sent the PIXIT_ENR_MAX_N1 Enrolment Request messages			
then			
the IUT stops sending Enrolment Requests			

TP ld	SECPKI_ITSS_ENR_REP_05_BV
Summary	Check that IUT stops sending the Enrolment Request message if timeout has been
	reached
Reference	ETSI TS 103 601 [6], clause 5.1.2
Configuration	CFG_ENR_ITSS
PICS Selection	
	Expected behaviour
with	
the IUT being in th	e 'initialized' state
and the IUT has st	arted sending the Enrolment Request at the time T1
ensure that	
when	
the IUT local tir	me is reached the T1 + PIXIT_ENR_TIMEOUT_TH2
then	
the IUT stops s	ending an Enrolment Request messages

TP Id	SECPKI_ITSS_ENR_REP_05_BV		
Summary	Check that IUT stops sending the Enrolment Request message if sending timeout (TH2)		
	has been reached		
Reference	ETSI TS 103 601 [6], clause 5.1.2		
Configuration	CFG_ENR_ITSS		
PICS Selection			
	Expected behaviour		
with			
the IUT being in the 'init	the IUT being in the 'initialized' state		
and the IUT has started sending the Enrolment Request			
ensure that			
when			
the IUT sent the Enrolment Request messages			
then			
the IUT stops sending Enrolment Requests			

# 5.2.3 Authorization

#### 5.2.3.0 Overview

All test purposes in clause 5.2.3 may be included in the test sequence if following PICS items are set:

PICS\_SECPKI\_AUTHORIZATION = TRUE

# 5.2.3.1 Authorization request

TP Id	SECPKI_ITSS_AUTH_01_BV	
Summary	Check that the ITS-S send the Authorization Request message to the Authorization	
	Authority (AA) to request an authorization ticket	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.0	
Configuration	CFG_AUTH_ITSS	
PICS Selection		
	Expected behaviour	
with		
the IUT in 'enrolled' state	e	
and the AA in 'operation	and the AA in 'operational' state	
ensure that		
when		
the IUT is triggered to request new Authorization Ticket (AT)		
then		
the IUT sends an EtsiTs103097Data to the AA		

TP Id	SECPKI_ITSS_AUTH_02_BV		
Summary	Check that the AuthorizationRequest message is encrypted and sent to only one		
	Authorization Authority		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1		
Configuration	CFG_AUTH_ITSS		
PICS Selection			
	Expected behaviour		
with			
the IUT in 'enrolled' state			
and the AA in 'operation	al' state		
authorized with CER	T_IUT_A_AA certificate		
ensure that	ensure that		
when	when		
the IUT is triggered to request new Authorization Ticket (AT)			
then			
the IUT sends a EtsiTs103097Data to the AA			
containing content.encryptedData.recipients			
indicating size 1			
and containing the instance of RecipientInfo			
containing certRecipInfo			
containing recipientId			
indicating HashedId8 of the CERT_IUT_A_AA			

TP Id	SECPKI_ITSS_AUTH_03_BV		
Summary	Check that the AuthorizationRequest message is encrypted using the encryptionKey		
	found in the AA certificate referenced in recipientId		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1		
Configuration	CFG_AUTH_ITSS		
PICS Selection			
	Expected behaviour		
with			
the IUT in 'enrolled' stat			
and the AA in 'operation			
authorized with AA	authorized with AA certificate		
containing encryptionKey (AA_ENC_PUB_KEY)			
ensure that			
when			
the IUT is triggered to request new Authorization Ticket (AT)			
then			
the IUT sends a EtsiTs103097Data to the AA			
containing content.encryptedData			
containing ciphertext			
containing data			
encry	encrypted using AA_ENC_PUB_KEY		

TP Id	SECPKI ITSS AUTH 04 BV		
Summary	Check that the AuthorizationRequest message is never reused the same encryption key		
	and nonce		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1		
Configuration	CFG_AUTH_ITSS		
PICS Selection			
	Expected behaviour		
with			
the IUT in 'authorized' st	ate		
and the IUT already sen	t one or more Authorization Requests		
and the AA in 'operation	al' state		
ensure that			
when	when		
the IUT is triggered to request new Authorization Ticket (AT)			
then			
the IUT sends a EtsiTs103097Data to the AA			
containing content.encryptedData			
containing ciphertext.aes128ccm.nonce			
indicating value not equal to the nonce in N previous messages			
and containin	and containing recipients[0].certRecipInfo.encKey		
containing encrypted symmetric key (S_KEY)			
indicating symmetric key not equal to the key was used in N previous messages			

TP Id	SECPKI_ITSS_AUTH_05_BV		
Summary	Check that the Authorization request protocol version is set to 1		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1		
Configuration	CFG_AUTH_ITSS		
PICS Selection			
	Expected behaviour		
with			
the IUT in 'enrolled' state	e		
and the AA in 'operation	al' state		
ensure that	ensure that		
when	when		
the IUT is triggered to request new Authorization Ticket (AT)			
then			
the IUT sends a Etsi	the IUT sends a EtsiTs103097Data to the AA		
containing EtsiTs102941Data			
containing version			
containing indicating 1			
containing content			
containing authorizationRequest			

TP Id	SECPKI ITSS AUTH 06 BV
i Fiu	
S	Check that for each Authorization request the ITS-S generates a new verification key pair
Summary	Check that for each Authorization request the ITS-S generates a new encryption key pair
	Check that for each Authorization request the ITS-S generates a new hmac-key
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITSS
PICS Selection	
	Expected behaviour
with	
the IUT in 'enrolled' state	
and the AA in 'operation	al' state
ensure that	
when	
the IUT is triggered to request new Authorization Ticket (AT)	
then	
the IUT sends a Etsi	Ts103097Data to the AA
containing EtsiTs	102941Data
containing authorizationRequest	
containing publicKeys	
containing verificationKey	
indicating value not equal to the field verificationKey of N previous messages	
and not containing encryptionKey	
or containing encryptionKey	
indicating value not equal to the field encryptionKey of N previous messages	
and containing hmacKey	
indicating value not equal to the field hmacKey of N previous messages	
	, , , , , , , , , , , , , , , , , , , ,

TP Id	SECPKI_ITSS_AUTH_07_BV	
Summary	Check that ITS-S sends Authorization request with properly calculated keyTag field	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_ITSS	
PICS Selection		
	Expected behaviour	
with		
the IUT in 'enrolled	' state	
and the AA in 'oper	rational' state	
ensure that	·	
when	when	
the IUT is triggered to request new Authorization Ticket (AT)		
then		
the IUT sends a	a EtsiTs103097Data to the AA	
containing E	containing EtsiTs102941Data	
containing authorizationRequest		
containing sharedAtRequest		
containing keyTag		
	indicating properly calculated value	

	<del>,</del>	
TP Id	SECPKI_ITSS_AUTH_08_BV	
Summary	Check that ITS-S sends Authorization request with eald of EA certificate	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_ITSS	
PICS Selection		
	Expected behaviour	
with		
the IUT is enrolled by the	e EC, signed with the CERT EA certificate	
and the AA in 'operation	and the AA in 'operational' stateensure that	
when	when	
the IUT is triggered t	the IUT is triggered to request new Authorization Ticket (AT)	
then		
the IUT sends a EtsiTs103097Data to the AA		
containing EtsiTs102941Data		
containing authorizationRequest		
containing sharedAtRequest		
contai	containing eald	
ind	indicating HashedId8 of CERT_ EA certificate	

TP Id	CECDIALITES ALTH OD DV	
	SECPKI_ITSS_AUTH_09_BV	
Summary	Check that ITS-S sends Authorization request with the certificateFormat equal to 1	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_ITSS	
PICS Selection		
	Expected behaviour	
with		
the IUT in 'enrolled' state	e	
and the AA in 'operation	al' state	
ensure that		
when		
the IUT is triggered to request new Authorization Ticket (AT)		
then		
the IUT sends a Etsi	Ts103097Data to the AA	
containing EtsiTs102941Data		
containing authorizationRequest		
containing sharedAtRequest		
contair	ning certificateFormat	
ind	licating 1	

TP ld	SECPKI_ITSS_AUTH_10_BV		
Summary	Check that ITS-S sends Authorization request certificate attributes are properly set		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1		
Configuration	CFG_AUTH_ITSS		
PICS Selection			
	Expected behaviour		
with			
the IUT in 'enrolled' state	e		
and the AA in 'operation	al' state		
ensure that			
when	when		
the IUT is triggered t	the IUT is triggered to request new Authorization Ticket (AT)		
then			
the IUT sends a EtsiTs103097Data to the AA			
containing EtsiTs102941Data			
	containing authorizationRequest		
containing sharedAtRequest			
containing requestedSubjectAttributes			
containing appPermissions			
and not containing certIssuePermissions			

TP ld	SECPKI_ITSS_AUTH_11_BV
0	Check that ITS-S sends Authorization request containing EC signature
Summary	Check that the EC signature of the Authorization request contains valid hash algorithm
Reference	Check that the ecSignature DataHash is calculated over the sharedATRequest
	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration PICS Selection	CFG_AUTH_ITSS
PICS Selection	Expected behavious
with	Expected behaviour
the IUT in 'enrolled' state	
and the AA in 'operation	
lensure that	al State
when	
	o request new Authorization Ticket (AT)
then	,
the IUT sends a Etsi	Ts103097Data to the AA
containing EtsiTs	102941Data
	thorizationRequest
	ecSignature
	ning structure of type EtsiTs103097Data-SignedExternalPayload
cor	ntaining hashId
	indicating supported hash algorithm (HASH_ALG)
and	d containing tbsData
	containing payload
	containing extDataHash indicating hash of sharedATRequest using HASH_ALG
	indicating flash of shareun frequest using Finori_neo

TP Id	SECPKI_ITSS_AUTH_12_BV
Summary	Check that the ecSignature psid is set to the proper ITS_AID
Summary	Check that the ecSignature generation time is present
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITSS
PICS Selection	
	Expected behaviour
with	
the IUT in 'enrolled	d' state
and the AA in 'ope	erational' state
ensure that	
when	
the IUT is trigg	ered to request new Authorization Ticket (AT)
then	
the IUT sends	a EtsiTs103097Data to the AA
containing	EtsiTs102941Data
contain	ing authorizationRequest
conf	taining ecSignature
	containing structure of type EtsiTs103097Data-SignedExternalPayload
	containing tbsData
	containing headerInfo
containing psid	
	indicating AID_PKI_CERT_REQUEST
	and containing generationTime
	and not containing any other headers

TP Id	SECPKI_ITSS_AUTH_13_BV	
Summary	Check that ITS-S sends Authorization request containing EC signature	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_ITSS	
PICS Selection		
	Expected behaviour	
with		
the IUT in 'enrolled' state	e	
and the AA in 'operation	al' state	
ensure that		
when		
the IUT is triggered to request new Authorization Ticket (AT)		
then		
the IUT sends a EtsiTs103097Data to the AA		
containing EtsiTs102941Data		
containing authorizationRequest		
containing ecSignature		
contair	containing structure of type EtsiTs103097Data-SignedExternalPayload	
cor	containing hashId	
	indicating supported hash algoritm	

TP Id	SECPKI ITSS AUTH 14 BV		
11 14			
6	Check that the ecSignature of the Authorization request is signed with EC certificate		
Summary	Check that the signature over tbsData computed using the private key corresponding to		
	the EC's verification public key		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1		
Configuration	CFG_AUTH_ITSS		
PICS Selection			
	Expected behaviour		
with			
the IUT is enrolled with (	CERT_EC certificate		
and the AA in 'operation	al' state		
ensure that			
when	when		
the IUT is triggered to request new Authorization Ticket (AT)			
then			
the IUT sends a Etsi	Ts103097Data to the AA		
containing EtsiTs102941Data			
containing authorizationRequest			
containing ecSignature			
contair	containing structure of type EtsiTs103097Data-SignedExternalPayload		
containing signer			
	indicating HashedId8 of the CERT_EC certificate		
cor	ntaining signature		
	indicating signature over sharedATRequest calculated with CERT_EC verificationKey		

TP ld	SECPKI_ITSS_AUTH_15_BV
Summary	Check that the encrypted ecSignature of the Authorization request is encrypted using the
	EA encryptionKey
	Check that the encrypted ecSignature of the Authorization request was done from the
	EtsiTs103097Data-SignedExternalPayload structure
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITSS
PICS Selection	PICS_PKI_AUTH_PRIVACY=TRUE
	Expected behaviour
with	
the IUT in 'enrolled' state	
and the AA in 'operation	
and the EA in 'operation	
authorized with CER	I_EA certificate
ensure that	
when	
	o request new Authorization Ticket (AT)
then	Ts103097Data to the AA
containing EtsiTs	
9	thorizationRequest
	g ecSignature
	ning encryptedEcSignature
	ntaining recipients
	containing only one element of type RecipientInfo
	containing certRecipInfo
	containing recipientId
	indicating HashedId8 of the CERT_EA
	and containing encKey
	indicating encryption key of supported type
and	d containing cypertext
	containing encrypted representation
	of structure EtsiTs103097Data-SignedExternalPayload

TP Id	SECPKI_ITSS_AUTH_16_BV	
Summary	Check that the ecSignature of the Authorization request is not encrypted	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_ITSS	
PICS Selection	PICS_PKI_AUTH_PRIVACY=FALSE	
	Expected behaviour	
with		
the IUT in 'enrolled	d' state	
and the AA in 'ope	rational' state	
ensure that		
when		
the IUT is trigg	ered to request new Authorization Ticket (AT)	
then	. ,	
the IUT sends	the IUT sends a EtsiTs103097Data to the AA	
containing EtsiTs102941Data		
containing authorizationRequest		
containing ecSignature		
containing ecSignature		

TP ld	SECPKI_ITSS_AUTH_17_BV	
Summary	Check that the Authorization request is not signed when Prove of Possession is not used	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_ITSS	
PICS Selection	PICS_PKI_AUTH_POP=FALSE	
	Expected behaviour	
with		
the IUT in 'enrolled	d' state	
and the AA in 'ope	rational' state	
ensure that	ensure that	
when		
the IUT is trigg	the IUT is triggered to request new Authorization Ticket (AT)	
then		
the IUT sends a EtsiTs103097Data-Encrypted to the AA		
containing encrypted representation of the leee1609Dot2Data		
_	containing content.unsecuredData	

TP ld	SECPKI_ITSS_AUTH_18_BV	
	Check that the Authorization request is signed when Prove of Possession is used	
Summary	Check that proper headers is used in Authorization request with POP	
	Check that the Authorization request with POP is self-signed	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_ITSS	
PICS Selection	PICS_PKI_AUTH_POP=TRUE	
	Expected behaviour	
with		
the IUT in 'enrolled' stat	е	
and the AA in 'operation	nal' state	
ensure that		
when		
the IUT is triggered	to request new Authorization Ticket (AT)	
then		
the IUT sends a Etsi	Ts103097Data-Encrypted to the AA	
containing cyphertext		
<u> </u>	ncrypted representation of the EtsiTs103097Data-Signed	
	g content.signedData	
	ning hashId	
indicating valid hash algorithm		
and containing tbsData		
СО	ntaining headerInfo	
containing psid		
	indicating AID_PKI_CERT_REQUEST	
and containing generationTime		
and not containing any other headers		
and containing signer		
	ntaining self	
	ontaining signature	
inc	dicating value calculated over tbsData with the private key	
	correspondent to the verificationKey from this message	

TP Id	SECPKI_ITSS_AUTH_19_BV
Summary	Check that the signing of ecSignature of the Authorization request is permitted by the EC
	certificate
Reference	ETSI TS 102 941 [1], clause B.5
Configuration	CFG_AUTH_ITSS
PICS Selection	
	Expected behaviour
with	
the IUT in 'enrolled' state	е
and the AA in 'operation	al' state
ensure that	
when	
the IUT is triggered t	to request new Authorization Ticket (AT)
then	
the IUT sends a Etsi	Ts103097Data to the AA
containing EtsiTs	
	ıthorizationRequest
	g ecSignature
	ning structure of type EtsiTs103097Data-SignedExternalPayload
CO	ntaining signer
	indicating HashedId8 of EC certificate
	containing appPermissions
	containing an item of type PsidSsp
	containing psid
	indicating AID_CERT_REQ
	and containing ssp
	containing opaque[0] (version)
	indicating 1
	containing opaque[1] (value)
	indicating 'Enrolment Reguest' (bit 1) set to 1

# 5.2.3.2 Authorization response handling

Void.

# 5.2.3.3 Authorization request repetition

All test purposes in clause 5.2.3.3 may be included in the test sequence if following PICS items are set:

#### PICS\_SECPKI\_ AUTHORIZATION \_RETRY = TRUE

TP ld	SECPKI_ITSS_AUTH_REP_01_BV
Summary	Check that IUT repeats an authorization request when response has not been received
Reference	ETSI TS 103 601 [6], clause 5.2
Configuration	CFG_AUTH_ITSS
PICS Selection	
	Expected behaviour
and the IUT has not yet ensure that when the IUT local time is then	the Authorization Request at the time <i>T1</i> received the Authorization Response  reached the <i>T1</i> + PIXIT_AUTH_TIMEOUT_TH1
i the IUT sends to EA	an AuthorizationRequestMessage

TP Id	SECPKI_ITSS_AUTH_REP_02_BV	
Summary	Check that IUT uses the same message to perform authorization retry	
Reference	ETSI TS 103 601 [6], clause 5.1.2	
Configuration	CFG_ENR_ITSS	
PICS Selection		
	Expected behaviour	
with the IUT being in the 'enrolled' state and the IUT already sent the Authorization Request (M) to AA ensure that when the IUT is triggered to re-send an AuthorizationRequestMessage to AA then the IUT sends M to AA		

TP Id	SECPKI_ITSS_AUTH_REP_03_BV	
Summary	Check that IUT stops sending the Authorization Request message if Authorization	
	Response message has been received	
Reference	ETSI TS 103 601 [6], clause 5.1.2	
Configuration	CFG_ENR_ITSS	
PICS Selection		
Expected behaviour		
with		
the IUT being in the 'enr	olled' state	
and the IUT has sent the	and the IUT has sent the Authorization Request more than 1 time	
ensure that		
when		
the IUT receives an Authorization Response		
then		
the IUT stops sending Authorization Requests to AA		

TP ld	SECPKI_ITSS_AUTH_REP_04_BV
Summary	Check that IUT stops sending the Authorization Request message if maximum number of
	retry has been reached
Reference	ETSI TS 103 601 [6], clause 5.1.2
Configuration	CFG_ENR_ITSS
PICS Selection	
Expected behaviour	
with	
the IUT being in the 'enrolled' state	
and the IUT has started sending the Authorization Request	
ensure that	
when	
the IUT sent the PIXIT_AUTH_MAX_N1 Authorization Request messages	
then	
the IUT stops sendin	g Authorization Requests

TP Id	SECPKI ITSS AUTH REP_05_BV	
Summary	Check that IUT stops sending the Authorization Request message if timeout has been	
	reached	
Reference	ETSI TS 103 601 [6], clause 5.1.2	
Configuration	CFG_ENR_ITSS	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the 'e	the IUT being in the 'enrolled' state	
and the IUT has started sending the Authorization Request at the time T1		
ensure that	ensure that	
when		
the IUT local time is reached the T1 + PIXIT_AUTH_TIMEOUT_TH2		
then		
the IUT stops sending an Authorization Request messages		

# 5.2.4 CTL handling

TP Id	SECPKI_ITSS_CTL_01_BV	
Summary	Check that the IUT trust the new RCA from the received ECTL	
Reference	ETSI TS 102 941 [1], clause 6.3.5	
Configuration	CFG_CXL_P2P	
PICS Selection		
	Expected behaviour	
with		
the IUT doesnot trust the	e CERT_RCA_NEW	
the IUT has received the	TLM CTL	
containing the CERT_RCA_NEW		
ensure that	ensure that	
when		
the IUT received a C	AM	
signed with AT certificate		
signed with AA certificate		
signed with CERT_RCA_NEW		
then		
the IUT accepts this CAM		

	<del>-</del>	
TP ld	SECPKI_ITSS_CTL_02_BV	
Summary	Check that the IUT untrust the RCA when it is deleted from ECTL	
Reference	ETSI TS 102 941 [1], clause 6.3.5	
Configuration	CFG_CXL_P2P	
PICS Selection		
	Expected behaviour	
with		
the IUT trusting the CER	RT_RCA	
the IUT has received the	the IUT has received the TLM CTL	
not containing the CERT_RCA		
ensure that	•	
when		
the IUT received a C	the IUT received a CAM	
signed with AT certificate		
signed with AA certificate		
signed with CERT_RCA		
then		
the IUT rejects this CAM		

TP ld	SECPKI_ITSS_CTL_03_BV	
Summary	Check that the IUT trust the AA when it is received in RCA CTL	
Reference	ETSI TS 102 941 [1], clause 6.3.5	
Configuration	CFG_CXL_P2P	
PICS Selection		
	Expected behaviour	
with		
the IUT does not have the CERT_AA_NEW		
the IUT has receive	the IUT has received the RCA CTL	
containing the C	containing the CERT_AA_NEW	
and signed by C	and signed by CERT_RCA	
ensure that	· · · · · · · · · · · · · · · · · · ·	
when		
the IUT received a CAM		
signed with AT certificate		
signed with CERT_AA_NEW digest		
then	-	
the IUT accepts	the IUT accepts this CAM	

TP ld	SECPKI_ITSS_CTL_04_BV	
Summary	Check that the IUT requests new ECTL when current one is expired	
Reference	ETSI TS 102 941 [1], clause 6.3.5	
Configuration	CFG_CXL_P2P	
PICS Selection		
Expected behaviour		
with		
	the IUT already downloaded theTLM CTL	
containing nex	· ·	
9	indicating timestamp T1	
_	and containing CPOC URL	
ensure that		
when		
the T1 < CURRENT TIME		
then		
the IUT sends	the IUT sends a request to the CPOC for a new CTL	

TP ld	SECPKI_ITSS_CTL_05_BV	
Summary	Check that the IUT requests new RCA CTL when current one is expired	
Reference	ETSI TS 102 941 [1], clause 6.3.5	
Configuration	CFG_CXL_P2P	
PICS Selection		
	Expected behaviour	
with the IUT already downloaded the RCA CTL containing nextUpdate indicating timestamp T1 and containing RCA DC URL ensure that		
when the T1 < CURRENT TIME then the IUT sends a request to the RCA DC for a new CTL		

# 5.2.5 CTL distribution

All test purposes in clause 5.2.5.1 may be included in the test sequence if following PICS items are set:

 $PICS\_SECPKI\_ECTL\_BROADCAST = TRUE \ or \ PICS\_SECPKI\_CTL\_BROADCAST = TRUE$ 

TP Id	SECPKI_ITSS_CTLDIST_01_BV
Summary	Check that the IUT retransmits the newly received Delta CTL
Reference	ETSI TS 103 601 [6], clause 4.2.1.4
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-05.2
Expected behaviour	
with	
the IUT is configured to redistribute the Delta CTL and the IUT does not contain an CTL information	
ensure that	
when	
the IUT has received the Delta CTL	
then	
the IUT is started to broadcast the received Delta CTL	
NOTE: This TP is applied for both: ECTL and RootCA CTL handling behaviour.	

TP ld	SECPKI_ITSS_CTLDIST_02_BV
Summary	Check that the IUT retransmits the updated Delta CTL
Reference	ETSI TS 103 601 [6], clause 4.2.1.4
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-05.2

#### **Expected behaviour**

with

the IUT is configured to redistribute the Delta CTL and the IUT contains an CTL information

containing ctlSequence (SN)

ensure that

when

the IUT has received the Delta CTL containing ctlSequence

indicating value greater than SN

then

the IUT is started to broadcast the received Delta CTL

NOTE: This TP is applied for both: ECTL and RootCA CTL handling behaviour.

TP Id	SECPKI_ITSS_CTLDIST_03_BV
Summary	Check that the IUT is using the proper BTP port to broadcast the Delta CTL
Reference	ETSI TS 103 601 [6], clause 5.4.4
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-05.2, <b>X_PICS</b>
Expected behaviour	

#### with

the IUT is configured to support P2P **X\_DISTRIBUTION** distribution and the IUT has received the Delta **X\_DISTRIBUTION** message

ensure that

when

the IUT is triggered to broadcast the Delta X\_DISTRIBUTION message

then

the IUT sends the **X\_MESSAGE** using the BTP port 2014

	Permutation table		
X	X_DISTRIBUTION	X_MESSAGE	X_PICS
Α	ECTL	TlmCertificateTrustListMessage	PICS_SECPKI_ECTL_BROADCAST
В	RootCA CTL	RcaCertificateTrustListMessage	PICS_SECPKI_CTL_BROADCAST

TP ld	SECPKI_ITSS_CTLDIST_04_BV
Summary	Check that the IUT stops to redistribute the Delta CTL if anorther node is also sending it
Reference	ETSI TS 103 601 [6], clause 5.3.1
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-05.2

#### **Expected behaviour**

with

the IUT is configured to support P2P Delta **X\_DISTRIBUTION** distribution and the IUT has started broadcasting the Delta **X\_DISTRIBUTION** message

signed with **X\_CERTIFICATE** and containing ctlSequence (**SN**)

ensure that

when

the IUT has received the Delta X\_DISTRIBUTION

signed with **X\_CERTIFICATE** and containing ctlSequence

indicating value equal or higher than SN

then

the IUT stops broadfcasting the Delta X\_DISTRIBUTION

signed with **X\_CERTIFICATE** and containing ctlSequence (**SN**)

	Permutation table		
X	X_DISTRIBUTION	X_CERTIFICATE	X_PICS
Α	ECTL	CERT_TLM	PICS_SECPKI_ECTL_BROADCAST
В	RootCA CTL	CERT IUT A RCA	PICS SECPKI CTL BROADCAST

TP Id	SECPKI_ITSS_CTLDIST_05_BV	
Summary	Check that the IUT requests the Delta CTL using P2P protocol when no CTL information available	
Reference	ETSI TS 103 601 [6], clause 5.3.4.3	
Configuration	CFG_CXL_P2P	
PICS Selection	UC-SEC-06.1	
Expected behaviour		

#### Expected benaviou

with

the IUT is configured to support P2P Delta CTL distribution

and the IUT contains valid TLM or/and RootCA certificate (CERT)

and the IUT does not contain any CTL information

ensure that

when

the IUT is triggered to request the CTL information for CERT

then

the IUT starts sending Secured GN messages

containing contributedExtensions

containing an item of type  ${\tt ContributedExtensionBlock}$ 

 $\quad \quad \text{containing contributorId} \\$ 

indicating etsiHeaderInfoContributorId (2)

containing an item of type EtsiTs102941CtlRequest

containing issuerId

indicating HashedID8 of the CERT

and not containing lastKnownCtlSequence

NOTE: This TP is applied for both: ECTL and RootCA CTL handling behaviour.

TP ld	SECPKI_ITSS_CTLDIST_06_BV	
Summary	Check that the IUT requests the Delta CTL using P2P protocol when new CTL information	
	is required	
Reference	ETSI TS 103 601 [6], clause 5.3.4.3	
Configuration	CFG_CXL_P2P	
PICS Selection	UC-SEC-06.1	
	Expected behaviour	
with		
the IUT is configured to	support P2P Delta CTL distribution	
and the IUT contains va	lid TLM or/and RootCA certificate ( <i>CERT</i> )	
and the IUT contain the	<b>CERT</b> CTL information	
containing ct1Sequ	nence	
indicating (SN)		
ensure that		
when		
the IUT is triggered to request the CTL information, associated with CERT		
then		
the IUT starts sending Secured GN messages		
<pre>containing contributedExtensions</pre>		
containing an item of type ContributedExtensionBlock		
containing contributorId		
<pre>indicating etsiHeaderInfoContributorId (2)</pre>		
containing an item of type EtsiTs102941CtlRequest		
containing issuerId		
indicating HashedID8 of the CERT		
and co	and containing lastKnownCtlSequence	
inc	dicating <b>SN</b>	
NOTE: This TP is applie	d for both: ECTL and RootCA CTL handling behaviour.	

TP Id	SECPKI_ITSS_CTLDIST_07_BV	
Summary	Check that the IUT requests the Delta CTL using P2P protocol when CTL information is expired	
Reference	ETSI TS 103 601 [6], clause 5.3.6	
Configuration	CFG_CXL_P2P	
PICS Selection	UC-SEC-06.1	
r ico delection	Expected behaviour	
with	Expected behavious	
1	support P2P Delta CTL distribution	
	lid TLM or/and RootCA certificate ( <i>CERT</i> )	
and the IUT contains the		
containing ctlSequer	nce	
indicating (SN)		
ensure that		
when		
the IUT is received the	ne Secured GN Message	
	ributedExtensions	
	containing an item of type ContributedExtensionBlock	
containing	containing contributorId	
indicat	<pre>indicating etsiHeaderInfoContributorId (2)</pre>	
containing an item of type EtsiTs102941CtlRequest		
contai	containing issuerId	
ind	licating HashedID8 of the CERT	
and containing lastKnownCtlSequence		
indicating value higher than <b>SN</b>		
then		
	the IUT starts sending Secured GN messages	
<pre>containing contributedExtensions</pre>		
containing an item of type ContributedExtensionBlock		
containing contributorId		
<pre>indicating etsiHeaderInfoContributorId (2)</pre>		
containing an item of type EtsiTs102941CtlRequest		
containing issuerId		
ind	indicating HashedID8 of the CERT	
and co	and containing lastKnownCtlSequence	
	licating <b>SN</b>	
NOTE: This TP is applied	d for both: ECTL and RootCA CTL handling behaviour.	

Reference ETSI TS 103 601 [6], clause 5.3.6  Configuration CFG_CXL_P2P  PICS Selection UC-SEC-06.2  Expected behaviour  with the IUT is configured to support P2P Delta CTL distribution and the IUT contains valid TLM or/and RootCA certificate (CERT) and the IUT has received a Delta CTL message (M) signed using CERT and containing ct1Sequence indicating (SN)	TDIA	OF ORIVE ITOO OT DIGT OF DV		
Reference ETSLTS 103 601 [6], clause 5.3.6  Configuration CFG_CXL_P2P  PICS Selection UC-SEC-06.2  Expected behaviour  with  the IUT is configured to support P2P Delta CTL distribution and the IUT contains valid TLM or/and RootCA certificate (CERT) and the IUT has received a Delta CTL message (M) signed using CERT and containing ctlSequence indicating (SN)  ensure that when  the IUT is received the Secured Message containing contributedExtensions containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value less than SN  then the IUT starts broadcasting the Delta CTL (M)	I P Ia			
Reference ETSI TS 103 601 [6], clause 5.3.6  Configuration   CFG_CXL_P2P   PICS Selection   UC-SEC-06.2  Expected behaviour  with   Contains valid TLM or/and RootCA certificate (CERT)   and the IUT contains valid TLM or/and RootCA certificate (CERT)   and the IUT contains valid TLM or/and RootCA certificate (CERT)   and containing cERT   and containing ctlSequence   indicating (SN)   ensure that   when   the IUT is received the Secured Message   containing contributedExtensions   containing an item of type EtsiTs102941CtlRequest   containing issuerId   indicating HashedID8 of the CERT   and containing lastKnownCtlSequence   indicating value less than SN   then   the IUT starts broadcasting the Delta CTL (M)	Summary	· · · · · · · · · · · · · · · · · · ·		
Configuration   CFG_CXL_P2P   PICS Selection   UC-SEC-06.2    Expected behaviour    with   UT is configured to support P2P Delta CTL distribution   and the IUT contains valid TLM or/and RootCA certificate (CERT)   and the IUT has received a Delta CTL message (M)   signed using CERT   and containing ctlSequence   indicating (SN)   ensure that   when   the IUT is received the Secured Message   containing contributedExtensions   containing an item of type EtsiTs102941CtlRequest   containing issuerId   indicating HashedID8 of the CERT   and containing lastKnownCtlSequence   indicating value less than SN   then   the IUT starts broadcasting the Delta CTL (M)		F. C.		
### PICS Selection UC-SEC-06.2    Expected behaviour	Reference	ETSI TS 103 601 [6], clause 5.3.6		
with the IUT is configured to support P2P Delta CTL distribution and the IUT contains valid TLM or/and RootCA certificate (CERT) and the IUT has received a Delta CTL message (M) signed using CERT and containing ctlSequence indicating (SN) ensure that when the IUT is received the Secured Message containing contributedExtensions containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value less than SN then the IUT starts broadcasting the Delta CTL (M)	Configuration	CFG_CXL_P2P		
with the IUT is configured to support P2P Delta CTL distribution and the IUT contains valid TLM or/and RootCA certificate (CERT) and the IUT has received a Delta CTL message (M) signed using CERT and containing ctlSequence indicating (SN) ensure that when the IUT is received the Secured Message containing contributedExtensions containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value less than SN then the IUT starts broadcasting the Delta CTL (M)	PICS Selection	UC-SEC-06.2		
the IUT is configured to support P2P Delta CTL distribution and the IUT contains valid TLM or/and RootCA certificate (CERT) and the IUT has received a Delta CTL message (M) signed using CERT and containing ctlSequence indicating (SN) ensure that when the IUT is received the Secured Message containing contributedExtensions containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value less than SN then the IUT starts broadcasting the Delta CTL (M)		Expected behaviour		
and the IUT contains valid TLM or/and RootCA certificate (CERT) and the IUT has received a Delta CTL message (M) signed using CERT and containing ct1Sequence indicating (SN) ensure that when the IUT is received the Secured Message containing contributedExtensions containing an item of type EtsiTs102941Ct1Request containing issuerId indicating HashedID8 of the CERT and containing lastKnownCt1Sequence indicating value less than SN then the IUT starts broadcasting the Delta CTL (M)	with			
and the IUT has received a Delta CTL message (M) signed using CERT and containing ctlSequence indicating (SN) ensure that when the IUT is received the Secured Message containing contributedExtensions containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value less than SN then the IUT starts broadcasting the Delta CTL (M)	the IUT is configured to	support P2P Delta CTL distribution		
signed using CERT and containing ctlSequence indicating (SN) ensure that when the IUT is received the Secured Message containing contributedExtensions containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value less than SN then the IUT starts broadcasting the Delta CTL (M)	and the IUT contains val	id TLM or/and RootCA certificate (CERT)		
and containing ctlSequence indicating (SN) ensure that when the IUT is received the Secured Message containing contributedExtensions containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value less than SN then the IUT starts broadcasting the Delta CTL (M)	and the IUT has received	d a Delta CTL message (M)		
indicating (SN) ensure that when the IUT is received the Secured Message containing contributedExtensions containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value less than SN then the IUT starts broadcasting the Delta CTL (M)	signed using CERT			
ensure that when the IUT is received the Secured Message containing contributedExtensions containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value less than SN then the IUT starts broadcasting the Delta CTL (M)	and containing ctls	and containing ctlSequence		
when the IUT is received the Secured Message containing contributedExtensions containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value less than SN then the IUT starts broadcasting the Delta CTL (M)	indicating ( <b>SN</b> )			
the IUT is received the Secured Message containing contributedExtensions containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value less than SN then the IUT starts broadcasting the Delta CTL (M)	ensure that			
containing contributedExtensions	when			
containing an item of type EtsiTs102941CtlRequest	the IUT is received the Secured Message			
containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value less than SN then the IUT starts broadcasting the Delta CTL (M)	<pre>containing contributedExtensions</pre>			
indicating HashedID8 of the <b>CERT</b> and containing lastKnownCtlSequence indicating value less than <b>SN</b> then the IUT starts broadcasting the Delta CTL ( <b>M</b> )	containing an item of type EtsiTs102941CtlRequest			
and containing lastKnownCtlSequence indicating value less than <b>SN</b> then the IUT starts broadcasting the Delta CTL ( <b>M</b> )	containing issuerId			
indicating value less than <b>SN</b> then the IUT starts broadcasting the Delta CTL ( <b>M</b> )	indicating HashedID8 of the CERT			
indicating value less than <b>SN</b> then the IUT starts broadcasting the Delta CTL ( <b>M</b> )	and containing lastKnownCtlSequence			
then the IUT starts broadcasting the Delta CTL ( <i>M</i> )				
		·		
	the IUT starts broadd	easting the Delta CTL (M)		

TP ld	SECPKI_ITSS_CTLDIST_09_BV	
Summary	Check that the IUT stops broadcasting the Delta CTL when broadcasting period is expired	
Reference	ETSI TS 103 601 [6], clause 5.3.6	
Configuration	CFG_CXL_P2P	
PICS Selection	UC-SEC-06.2	
	Expected behaviour	
with		
the IUT is configured to support P2P Delta CTL distribution and the IUT is configured to broadcast the Delta CTL during <i>D1</i> time		
at the time <b>T</b>	and the IUT has started to broadcast a Delta CTL message at the time <i>T</i>	
ensure that		
when		
the IUT local time is reached the T + D1		
then		
the IUT stops broadcasting the Delta CTL		
NOTE 1: This TP is applied for both: ECTL and RootCA CTL handling behaviour.		
NOTE 2: The D1 value	e shall be provided as a PIXIT.	

TP Id	SECPKI_ITSS_CTLDIST_10_BV
Summary	Check that the IUT stops broadcasting the requested Delta CTL when broadcasting period
	is expired
Reference	ETSI TS 103 601 [6], clause 5.3.6
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-06.2
	Expected behaviour
with	
the IUT is configured to	support P2P Delta CTL distribution
and the IUT is configure	d to broadcast the requested Delta CTL during D2 time
and the IUT has started to broadcast a Delta CTL message	
at the time <b>T</b>	
ensure that	
when	
the IUT local time is reached the <b>T + D2</b>	
then	
the IUT stops broadcasting the Delta CTL	
NOTE 1: This TP is applied for both: ECTL and RootCA CTL handling behaviour.	
NOTE 2: The <b>D2</b> value shall be provided as a PIXIT.	

# 5.2.6 CRL handling

TP Id	SECPKI_ITSS_CRL_01_BV	
Summary	Check that the IUT accept the received CRL information	
Reference	ETSI TS 102 941 [1], clause 5.4.2	
Configuration	CFG_CXL_P2P	
PICS Selection		
	Expected behaviour	
with		
	lid RootCA certificate (CERT_IUT_A_RCA)	
and the IUT has not reco	and the IUT has not received yet the CRL information issued by the RootCA	
ensure that	ensure that	
when		
the IUT received the CRL information from the DC		
then		
the IUT accepts the	the IUT accepts the received CRL	

TP ld	SECPKI_ITSS_CRL_02_BV		
Summary	Check that the IUT can handle the revocation of its own AA		
Reference	ETSI TS 102 941 [1], clause 5.4.2		
Configuration	CFG_CXL_P2P		
PICS Selection			
	Expected behaviour		
with and the IUT contains valid RootCA certificate (CERT_IUT_A_RCA) and the IUT is authorized using AT certificate signed with CERT_IUT_A_B_AA ensure that when the IUT received the CRL information from the DC containing revocation of CERT_IUT_A_B_AA then			
the IUT switched to '	enrolled' state		

TP Id	SECPKI_ITSS_CRL_03_BV	
Summary	Check that the IUT can handle the revocation of its own EA	
Reference	ETSI TS 102 941 [1], clause 5.4.2	
Configuration	CFG_CXL_P2P	
PICS Selection		
	Expected behaviour	
the IUT is in 'authorized and the IUT contains value and the IUT been enrol signed with CERT_lensure that when the IUT the IUT received.	when the IUT the IUT received the CRL information from the DC containing revocation of CERT_IUT_A_EA then	

TP Id	SECPKI ITSS CRL 04 BV		
Summary	Check that the IUT can handle the revocation of its own RootCA		
Reference	ETSI TS 102 941 [1], clause 5.4.2		
Configuration	CFG_CXL_P2P		
PICS Selection			
	Expected behaviour		
with			
the IUT is in 'authorized'	state		
and the IUT contains val	lid RootCA certificate (CERT_IUT_A_RCA)		
and the IUT been enrolle	and the IUT been enrolled with EC certificate		
	signed with EA certificate		
signed with CERT_IUT_A_RCA			
ensure that			
when			
the IUT the IUT received the CRL information from the DC			
containing revocation of CERT_IUT_A_RCA			
then			
the IUT switches to t	he 'initial' state		

TP Id	SECPKI_ITSS_CRL_05_BV
Summary	Check that the IUT skips incoming messages when revoked AA certificate is in the signing chain of the current AT certificate
Reference	ETSI TS 102 941 [1], clause 5.4.2
Configuration	CFG_CXL_P2P
PICS Selection	
	Expected behaviour
with	
and the IUT has not reco and the IUT is authorize signed with CERT_IU and the IUT contains an and the IUT has already signed with CERT_IU and the IUT received the containing revocation	JT_A_AA other AA certificate (CERT_IUT_A_B_AA) accepted messages signed with AT certificate
when the IUT receives a Secured Message signed with AT certificate signed with CERT_IUT_A_B_AA then the IUT discards this message	

# 5.2.7 CRL distribution

TP ld	SECPKI_ITSS_CRLDIST_01_BV
Summary	Check that the IUT starts broadcasting the CRL using P2P protocol when CRL information
	is received
Reference	ETSI TS 103 601 [6], clause 5.4.2
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-07.2
	Expected behaviour
with	
	red to support P2P CRL distribution
	ins valid RootCA certificate (CERT_IUT_A_RCA)
	ot received yet the CRL information issued by the RootCA
ensure that	
when	
the IUT received the CRL information from the DC	
containing thisUpdate (T)	
and containing nextUpdate (N)	
then	
the IUT starts	broadcasting the received CRL

TP ld	SECPKI_ITSS_CRLDIST_02_BV
Summary	Check that the IUT is using the proper BTP port to broadcast the CRL
Reference	ETSI TS 103 601 [6], clause 5.4.4
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-07.2
	Expected behaviour
and the IUT contains val and the IUT has not rece ensure that when the IUT is triggered to then	ertificateRevocationListMessage

TP ld	SECPKI_ITSS_CRLDIST_02_BV		
Summary	Check that the IUT stops broadcasting the CRL when distribution time (d1) has been		
	expired after receiving of CRL information		
Reference	ETSI TS 103 601 [6], clauses 5.4.2 and 5.4.3		
Configuration	CFG_CXL_P2P		
PICS Selection	UC-SEC-07.2		
	Expected behaviour		
with			
the IUT is configured to	support P2P CRL distribution		
and the IUT contains va	lid RootCA certificate (CERT_IUT_A_RCA)		
and the IUT has already	received the CRL information from DC		
at the time <b>T</b>			
and the IUT has started broadcasting the received CRL			
and the IUT is configured to limit the broadcasting time to <b>D1</b>			
ensure that			
when			
the IUT current time is equal or more than <b>T+D1</b>			
then	·		
the IUT stops broade	casting the CRL		
NOTE: The <b>D1</b> value sha	all be provided as a PIXIT		

TP ld	SECPKI_ITSS_CRLDIST_03_BV	
Summary	Check that the IUT stops broadcasting the CRL when the CRL became outdated because	
	of the nextUpdate value	
Reference	ETSI TS 103 601 [6], clause 5.4.3	
Configuration	CFG_CXL_P2P	
PICS Selection	UC-SEC-07.2	
	Expected behaviour	
with		
the IUT is configured to	support P2P CRL distribution	
and the IUT contains va	and the IUT contains valid RootCA certificate (CERT_IUT_A_RCA)	
and the IUT has already	received the CRL information from DC	
containing nextUpda	containing nextUpdate (N)	
and the IUT has started broadcasting the received CRL		
ensure that		
when		
the IUT current time	is equal or more than <b>N</b>	
then		
the IUT stops broad	casting the CRL	

TP ld	SECPKI ITSS CRLDIST 04 BV	
Summary	Check that the IUT stops broadcasting the CRL when another station starts to broadcast	
	the same or more recent CRL	
Reference	ETSI TS 103 601 [6], clause 5.4.3	
Configuration	CFG_CXL_P2P	
PICS Selection	UC-SEC-07.2	
	Expected behaviour	
with		
the IUT is configured to	support P2P CRL distribution	
and the IUT contains v	alid RootCA certificate (CERT_IUT_A_RCA)	
and the IUT has alread	ly received the CRL	
containing thisUpda	containing thisUpdate (7)	
and the IUT has starte	and the IUT has started broadcasting the received CRL	
ensure that		
when		
the IUT receives the CRL signed by CERT_IUT_A_RCA		
containing thisUpdate		
indicating the value equal or greate than <b>T</b>		
then		
the IUT stops broad	dcasting the CRL	

TP Id	SECPKI_ITSS_CRLDIST_04_BV		
Summary	Check that the IUT skips the lastKnownUpdate field in the P2P CRL request when no CRL		
	information has been previously available		
Reference	ETSI TS 103 601 [6], clause 5.3.4.2		
Configuration	CFG_CXL_P2P		
PICS Selection	UC-SEC-08.1		
	Expected behaviour		
with			
the IUT is configured to	support P2P CRL distribution		
and the IUT contains val	lid RootCA certificate (CERT_IUT_A_RCA)		
and the IUT has never re	eceived a CRL information issued by the RootCA		
ensure that			
when			
	the IUT is triggered to request the CRL		
then			
the IUT starts sending Secured GN messages			
<pre>containing contributedExtensions</pre>			
containing an item of type ContributedExtensionBlock			
containing contributorId			
<pre>indicating etsiHeaderInfoContributorId (2)</pre>			
containing	an item of type EtsiTs102941CrlRequest		
contair	ning issuerId		
ind	licating HashedID8 of the CERT_IUT_A_RCA		
and no	ot containing lastKnownUpdate		

TP ld	SECPKI_ITSS_CRLDIST_05_BV	
Summary	Check that the IUT includes the lastKnownUpdate information in the P2P CRL request if	
Summary	the CRL information was previously available	
Reference	ETSI TS 103 601 [6], clause 5.3.4.2	
Configuration	CFG_CXL_P2P	
PICS Selection	UC-SEC-08.1	
	Expected behaviour	
with		
	support P2P CRL distribution	
	lid RootCA certificate (CERT_IUT_A_RCA)	
and the IUT has already	received the CRL information issued by the RootCA	
containing thisUpd	ate ( <b>7</b> )	
ensure that		
when		
the IUT is triggered to	o request the CRL	
then		
	g Secured GN messages	
<pre>containing contributedExtensions</pre>		
containing an item of type ContributedExtensionBlock		
containing contributorId		
<pre>indicating etsiHeaderInfoContributorId (2)</pre>		
containing an item of type EtsiTs102941CrlRequest		
containing issuerId		
indicating HashedID8 of the CERT_IUT_A_RCA		
and co	and containing lastKnownUpdate	
indicating $oldsymbol{ au}$		
<u> </u>		

TP ld	SECPKI_ITSS_CRLDIST_06_BV	
Summary	Check that the IUT starts broadcasting the CRL using P2P protocol when CRL information	
	has been requested by another ITS station	
Reference	ETSI TS 103 601 [6], clause 5.4.2	
Configuration	CFG_CXL_P2P	
PICS Selection	UC-SEC-08.2	
	Expected behaviour	
with		
the IUT is configured to	support P2P CRL distribution	
and the IUT contains va	lid RootCA certificate (CERT_IUT_A_RCA)	
and the IUT has already	and the IUT has already received the CRL information issued by the RootCA	
and the IUT has already stopped broadcasting the CRL information		
ensure that		
when		
the IUT received the CRL request information issued by the RootCA		
not containing thislastKnownUpdate		
then		
the IUT starts broad	casting the received CRL	

TP ld	SECPKI ITSS CRLDIST 06 BV		
Summary	Check that the IUT stops broadcasting the CRL when distribution time (d2) has been expired after receiving of CRL request		
Reference	ETSI TS 103 601 [6], clause 5.4.2		
Configuration	CFG_CXL_P2P		
PICS Selection	UC-SEC-08.2		
	Expected behaviour		
and the IUT contains va and the IUT has already at the time <i>T</i> and the IUT has started and the IUT is configure ensure that when the IUT current time then	is equal or more than <b>T+D1</b>		

## 5.3 Common CA behaviour

#### 5.3.0 Overview

All test purposes in the present clause may be included in the test sequence if one of the following PICS items are set:

```
PICS_SECPKI_IUT_RCA = TRUE; or
PICS_SECPKI_IUT_AA = TRUE; or
PICS_SECPKI_IUT_EA = TRUE.
```

# 5.3.1 Certificate validation

### 5.3.1.1 Basic certificate content

TP ld	SECPKI_CA_CERTGEN_01_BV	
Summary	Check that the issuing certificate has version 3	
Reference	ETSI TS 103 097 [2], clause 6	
Reference	IEEE Std 1609.2 [3], clause 6.4.3	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
CA is in 'operational' state		
ensure that		
when		
the CA is requested to issue the certificate		
then		
this certificate is of type EtsiTs103097Certificate		
containing version		
indicating 3		

TP ld	SECPKI_CA_CERTGEN_02_BV_01		
Summary	Check that the issuing certificate has type explicit		
Reference	ETSI TS 103 097 [2], clause 6		
	IEEE Std 1609.2 [3], clause 6.4.3		
PICS Selection			
	Expected behaviour		
with			
CA is in 'operational' sta	te		
CA is initialized with the	explicit certificate (CERT_IUT_A_CA)		
ensure that			
when			
the CA is requested to issue the explicit certificate			
then			
	/pe EtsiTs103097Certificate		
containing version			
indicating 3			
and containing type			
indicating 'exp			
and containing toBeSigned			
•	rifyKeyIndicator		
_	g verificationKey		
and containing si	and containing signature		

TP Id	SECPKI_CA_CERTGEN_02_BV_02		
Summary	Check that the CA, been authorized using explicit certificate, is able to issue an implicit		
	certificate		
Reference	ETSI TS 103 097 [2], clause 6		
	IEEE Std 1609.2 [3], clause 6.4.3		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_IMPLICIT_CERTIFICATES AND		
PICS Selection	PICS_SEC_EXPLICIT_CERTIFICATES		
	Expected behaviour		
with			
CA is in 'operational'	state		
CA is initialized with	the explicit certificate (CERT_IUT_A_CA)		
ensure that			
when			
the CA is requested to issue the implicit certificate			
then			
this certificate is	of type EtsiTs103097Certificate		
containing ve	containing version		
indicating			
containing typ	containing type		
indicating 'implicit'			
and containing toBeSigned			
	y verifyKeyIndicator		
	ning reconstructionValue		
and not containing signature			

TP Id	SECPKI_CA_CERTGEN_02_BV_03
Summary	Check that the CA, been authorized using explicit certificate, is able to issue an implicit
	certificate
Reference	ETSI TS 103 097 [2], clause 6
	IEEE Std 1609.2 [3], clause 6.4.3
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_IMPLICIT_CERTIFICATES
	Expected behaviour
with	
CA is in 'operational	l' state
CA is initialized with	the implicit certificate (CERT_IUT_I_CA)
ensure that	
when	
the CA is reques	sted to issue the implicit certificate
then	
this certificate is	of type EtsiTs103097Certificate
containing ve	
indicating	
containing ty	pe
indicating	
and containing	ng toBeSigned
	g verifyKeyIndicator
conta	ining reconstructionValue
and not cont	aining signature

TP ld	SECPKI_CA_CERTGEN_02_BO_01	
Summary	Check that the CA, been authorized using implicit certificate, does not issue an explicit	
	certificate	
Reference	ETSI TS 103 097 [2], clause 6	
Neielelice	IEEE Std 1609.2 [3], clause 6.4.3	
DICC Coloction	PICS_GN_SECURITY AND PICS_SEC_IMPLICIT_CERTIFICATES AND	
PICS Selection	PICS_SEC_EXPLICIT_CERTIFICATES	
Expected behaviour		
with		
CA is in 'operationa	l' state	
CA is initialized with the implicit certificate (CERT_IUT_I_CA)		
ensure that		
when		
the CA is requested to issue the explicit certificate		
then		
the CA does not	the CA does not issue the certificate	

FP Id SECPKI_CA_CERTGEN_03_BV			
Check that CA issues certificate conformed to ETSI TS 103 097 [2], clause 6			
Reference ETSI TS 103 097 [2], clause 6			
PICS Selection PICS_GN_SECURITY			
	Expected behaviour		
with			
CA is in 'operational' sta	te		
ensure that			
when			
the CA is issued the	the CA is issued the certificate		
then			
this certificate is of type EtsiTs103097Certificate			
S	containing toBeSigned		
containing id			
indicating 'none' or 'name'			
and containing cracald			
indicating '000000'H			
and containing crlSeries			
	indicating '0'D		
	ining certRequestPermissions		
and not containing canRequestRollover			

TP ld	SECPKI_CA_CERTGEN_04_BV_X	
	Check that the issuer of certificates is referenced using digest	
	Check that right digest field is used to reference to the certificate	
Reference	IEEE Std 1609.2 [3], clause 6.4.3	
PICS Selection	PICS_GN_SECURITY AND X_PICS	
Expected behaviour		
141		

with

CA is in 'operational' state

and CA is authorized with CA certificate C\_ISSUER

ensure that

when

the CA is issued the explicit certificate

then

this certificate is of type EtsiTs103097Certificate

containing issuer

containing X\_DIGEST

indicating last 8 bytes of the hash of the certificate calculated using  $\textit{X\_ALGORITHM}$ 

referenced to certificate C\_ISSUER

and containing toBeSigned containing verifyKeyIndicator containing verificationKey containing X\_KEY

Permutation table				
X	X_DIGEST	X_ALGORITM	X_KEY	X_PICS
Α	sha256AndDigest	ISHA-256		PICS_SEC_SHA256 AND PICS_SEC_BRAINPOOL_P256R1
В	sha384AndDigest	SHA-384	IecdsaBrainnoolP384r1	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1

### 5.3.1.2 Check certificate region validity restriction

P Id SECPKI_CA_CERTGEN_05_BV			
Summary	Check that the CA is able to issue the certificate with the well-formed circular region		
Summary	validity restriction		
Reference IEEE Std 1609.2 [3], clauses 6.4.20, 6.4.17 and 5.1.2.4			
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_CIRCULAR_REGION		
	Expected behaviour		
with			
CA is in 'operational' s	tate		
the CA is authorized w	rith CA certificate		
containing toBeSig			
containing region	on		
indicating R	EGION		
ensure that			
when			
-	d to issue the certificate		
	lar region restriction		
then			
	certificate of type EtsiTs103097Certificate		
containing toBe	· ·		
containing r			
	ng circularRegion		
containing center			
	ndicating a point inside the REGION		
	containing radius		
ıi i	ndicating a value when all points of the circle are inside the REGION		

TP Id	SECPKI_CA_CERTGEN_06_BV		
_	Check that the CA is able to issue the certificate with the well-formed rectangular region		
Summary	validity restriction		
Reference IEEE Std 1609.2 [3], clauses 6.4.20, 6.4.17 and 5.1.2.4			
PICS Selection PICS_GN_SECURITY AND PICS_SEC_RECTANGULAR_REGION			
	Expected behaviour		
with			
CA is in 'operational' sta			
the CA is authorized with	h CA certificate		
containing toBeSigne			
containing region	containing region		
indicating RE	GION		
ensure that			
when			
the CA is requested to issue the certificate			
containing rectangular region restriction			
then			
the CA issues the certificate of type EtsiTs103097Certificate			
containing toBeSigned			
containing region			
containing rectangularRegion			
containing items of type RectangularRegion			
containing northwest			
	indicating a point inside the REGION		
and	d containing southeast		
	indicating a point on the south and east from northwest		
	and inside the REGION		

TP ld	SECPKI_CA_CERTGEN_07_BV
Summary	Check that CA is able to issue certificate with polygonal region validity restriction where:  - the polygonal certificate validity region contains at least three points  - the polygonal certificate validity region does not contain intersections  - the polygonal certificate validity region is inside the validity region of the issuing certificate
Reference	IEEE Std 1609.2 [3], clauses 6.4.21, 6.4.17 and 5.1.2.4
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_POLYGONAL_REGION
	Expected behaviour
ensure that when the CA is reques containing po then the CA issues th containing to containing conta	With CA certificate Signed gion REGION  sted to issue the certificate olygonal region validity restriction e certificate of type EtsiTs103097Certificate BeSigned

TP ld	SECPKI_CA_CERTGEN_08_BV		
	Check that the CA is able to issue the certificate with identified region validity restriction		
Summary	contains values that correspond to numeric country codes as defined by United Nations		
· · · · · · · · · · · · · · · · · · ·	Statistics Division [i.8]		
Reference	IEEE Std 1609.2 [3], clause 6.4.23		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_IDENTIFIED_REGION		
	Expected behaviour		
with	·		
CA is in 'operationa	al' state		
the CA is authorize	ed with CA certificate		
containing toBe	containing toBeSigned		
containing region			
indicating REGION			
ensure that	·		
when			
the CA is reque	ested to issue the certificate		
containing id	dentified region validity restriction		
indicatin	g country or area <b>COUNTRY</b>		
then			
the CA issued t	he certificate of type EtsiTs103097Certificate		
containing to			
containir	ng region		
conta	aining identifiedRegion		
С	ontaining 1 entry of type IdentifiedRegion		
	containing countryOnly		
	indicating integer representation of the identifier of country or area COUNTRY		
	· · · · · · · · · · · · · · · · · · ·		

or containing countryAndRegions
containing countryOnly
indicating integer representation of the identifier of country or area COUNTRY
or containing countryAndSubregions

indicating integer representation of the identifier of country or area COUNTRY

containing country

TP Id	SECPKI_CA_CERTGEN_09_BV	
IF IU	Check that the identified region validity restriction of the subordinate certificate is included	
Summary	in the identified region validity restriction of the issuing certificate	
Reference	IEEE Std 1609.2 [3], clauses 6.4.17 and 5.1.2.4	
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_IDENTIFIED_REGION	
Expected behaviour		
with	Expected beliavious	
the CA is in 'operational	' ctato	
and the CA is authorized		
containing toBeSign		
containing region		
0 0	entifiedRegion	
	g country Only	
	ting COUNTRY	
or contain	ning countryAndRegions	
	ning countryOnly	
	dicating COUNTRY	
	ontaining regions	
	dicating <b>REGIONS</b>	
	ning countryAndSubregions	
	ining country dicating <b>COUNTRY</b>	
	ontaining regionAndSubregions	
	dicating REGIONS and SUBREGIONS	
ensure that		
when		
the CA issued the ce	ertificate	
containing toBeS	Signed	
containing re		
1	g identifiedRegion	
then		
this certificate is of type EtsiTs103097Certificate		
containing toBeSigned		
containing region		
containing identifiedRegion containing countryOnly		
indicating value = <b>COUNTRY</b>		
or containing countryAndRegions		
containing country/midrograms		
indicating value = <b>COUNTRY</b>		
and containing regions		
containing region identifiers contained in REGIONS		
	taining countryAndSubregions	
СО	ntaining country	
	indicating value = <b>COUNTRY</b>	
an	d containing regionAndSubregions	
	containing region identifiers contained in <b>REGIONS</b>	
	and containing subRegion identifiers contained in SUBREGIONS for every region	

# 5.3.1.3 Check ECC point type of the certificate signature

TP ld	SECPKI_CA_ CERTGEN_10_BV_XX		
Summary	Check that the certificate signature contains ECC point of type set to either		
Summary	compressed_lsb_y_0, compressed_lsb_y_1 or x_coordinate_only		
Reference	IEEE Std 1609.2 [3], clauses 6.3.29, 6.3.30 and 6.3.31		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_EXPLICIT_CERTIFICATES AND X_PICS		
	Expected behaviour		
with			
the CA is in 'operational'	' state		
ensure that			
when			
the CA issued the ex	xplicit certificate		
then			
	this certificate is of type EtsiTs103097Certificate		
	containing signature		
containing <b>X_SIGNATURE</b>			
containing rSig			
containing x-only			
or containing compressed-y-0			
or containing compressed-y-1			
Permutation table			
XX X_SIGNATURE	X_PICS		
A ecdsaNistP256Signatu			
B ecdsaBrainpoolP256r1	Signature PICS_SEC_BRAINPOOL_P256R1		
C   ecdsaBrainpoolP384r1Signature   PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1			

## 5.3.1.4 Check ECC point type of the certificate public keys

TP Ic	ł	SECPKI_CA_CERTGEN_11_BV
Summary	moru	Check that the certificate verification key contains ECC point of type set to either
	compressed_lsb_y_0, compressed_lsb_y_1 or uncompressed	
Refe	rence	IEEE Std 1609.2 [3], clause 6.4.38
PICS	Selection	PICS_GN_SECURITY AND PICS_SEC_EXPLICIT_CERTIFICATES AND X_PICS
		Expected behaviour
with		·
th	ne CA is in 'operational	state
ensu	re that	
W	hen en	
	the CA issued the ex	cplicit certificate
th	nen	
	this certificate is of ty	ype EtsiTs103097Certificate
	containing toBeS	igned
	containing ve	rifyKeyIndicator
		verificationKey
	contai	ning X_KEY
	cont	aining uncompressed
	or co	ontaining compressed-y-0
	or containing compressed-y-1	
Permutation table		
XX	X_KEY	X_PICS
Α	ecdsaNistP256	
В	ecdsaBrainpoolP256r1	PICS_SEC_BRAINPOOL_P256R1
С		

TP Id	SECPKI_CA_CERTGEN_12_BV		
_	Check that the certificate encryption key contains ECC point of type set to either		
Summary	compressed_lsb_y_0, compressed_lsb_y_1 or uncompressed		
Reference	IEEE Std 1609.2 [3], clause 6.4.38		
PICS Selection	PICS_GN_SECURITY		
FICS Selection	Expected behaviour		
الماند	Expected benaviour		
with			
the CA is in 'operation	ai state		
ensure that			
when			
the CA issued the	certificate		
then			
this certificate is of type EtsiTs103097Certificate			
	containing toBeSigned		
	containing encryptionKey		
containing publicKey			
containing X_KEY			
containing uncompressed			
or containing compressed-y-0			
or containing compressed-y-1			
Permutation table			
XX X_KEY	X_PICS		
A eciesNistP256			
B eciesBrainpoolP256	r1 PICS_SEC_BRAINPOOL_P256R1		

## 5.3.1.5 Verify certificate signatures

ecdsaBrainpoolP256r1

ecdsaBrainpoolP384r1

TP Id	SECPKI_CA_CERTGEN_13_BV_01		
Summary	Check the explicit certificate signatur	re	
Reference	ETSI TS 103 097 [2], clause 6		
PICS Selection		EC_EXPLICIT_CERTIFICATES AND <b>X_PICS</b>	
	Expected beha	viour	
with			
the CA is in 'operational'			
and the CA is authorized			
containing toBeSigne			
containing verifyl			
containing ve			
containing	, X_KEY		
ensure that			
*******	when		
the CA issued the explicit certificate			
then			
this certificate is of type EtsiTs103097Certificate			
containing issuer			
referencing the certificate			
	containing toBeSigned		
containing verifyKeyIndicator containing verificationKey			
	containing <b>X_KEY</b>		
indicating KEY			
and containing signature			
containing X_SIGNATURE			
verifiable using KEY			
Permutation table			
XX X_KEY	X_SIGNATURE	X_PICS	
A ecdsaNistP256	ecdsaNistP256Signature		
	1 5 1 155-5 151		

ecdsaBrainpoolP256r1Signature

ecdsaBrainpoolP384r1Signature

PICS\_SEC\_BRAINPOOL\_P256R1 PICS\_SEC\_SHA384 AND PICS\_SEC\_BRAINPOOL\_P384R1 SECPKI\_CA\_CERTGEN\_13\_BV\_02

Summary	Check the explicit certificate signature
Reference	ETSI TS 103 097 [2], clause 6
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_EXPLICIT_CERTIFICATES AND X_PICS
	Expected behaviour
with	
the CA is in 'operation	al' state
and the CA is authoriz	red with explicit certificate
containing toBeSigned	
containing verifyKeyIndicator	
containing verificationKey	
containing <b>X_KEY</b>	
indicating KEY	
and the CA issued the implicit certificate of type EtsiTs103097Certificate (CERT)	
not containing signature	
and containing issuer	
referencing the certificate	
containing toBeSigned	
containing verifyKeyIndicator	
containing reconstructionValue	

ensure that

TP Id

when

the CA is calculated the digital signature

using the private key associated with the CERT

indicating VALUE

this signature can be verified using public key

reconstructed using VALUE and KEY

Permutation table		
XX	X_KEY	X_PICS
Α	ecdsaNistP256	
В	ecdsaBrainpoolP256r1	PICS_SEC_BRAINPOOL_P256R1
С	ecdsaBrainpoolP384r1	PICS SEC SHA384 AND PICS SEC BRAINPOOL P384R1

#### Verify certificate permissions 5.3.1.6

TP Id	SECPKI_CA_CERTGEN_14_BV	
Summary	Check that all PSID entries of the appPermissions component of the certificate are unique	
Reference	IEEE Std 1609.2 [3], clauses 6.4.28 and 5.1.2.4	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the CA is in 'operational	' state	
ensure that		
when		
the CA issued the ce	the CA issued the certificate	
containing toBeSigned		
containing appPermissions		
then		
this certificate is of type EtsiTs103097Certificate		
containing toBeSigned		
containing appPermissions		
containing	containing items of type PsidSsp	
containing psid		
inc	dicating unique values in this sequence	

TP ld	SECPKI_CA_CERTGEN_15_BV	
Summary	Check that all PSID entries of the appPermissions component of the certificate are also	
Summary	contained in the certIssuePermissions component in the issuing certificate	
Reference	IEEE Std 1609.2 [3], clauses 6.4.28 and 5.1.2.4	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the CA is in 'operational	state	
ensure that		
when		
the CA issued the ce		
containing toBeS		
	pPermissions	
then	F. 'T 10000TO .'''	
1	this certificate is of type EtsiTs103097Certificate	
containing issuer		
referenced to the certificate		
containing toBeSigned		
containing certIssuePermissions		
CO	containing items of type PsidGroupPermissions	
containing eeType indicating app(0)		
and containing subjectPermissions		
containing subject remissions		
containing explicit containing items of type PsidSspRange		
indicating X_PSID_RANGE_LIST		
or containing all		
and containing toBeSigned		
containing appPermissions		
	containing items of type PsidSsp	
	ning psid	
co	ntained in the X_PSID_RANGE_LIST	
	as a psid	

TP Id	SECPKI CA CERTGEN 16 BV	
Summary		
	Check that all PSID entries of the certIssuePermissions component of the certificate are	
	unique	
Reference	IEEE Std 1609.2 [3], clauses 6.4.28 and 5.1.2.4	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the CA is in 'operational	' state	
ensure that		
when		
the CA issued the certificate		
containing toBeS	containing toBeSigned	
containing certIssuePermissions		
then		
this certificate is of type EtsiTs103097Certificate		
containing toBeSigned		
containing certIssuePermissions		
containing items of type PsidGroupPermissions		
containing subjectPermissions		
containing explicit		
containing items of type PsidSspRange		
	containing psid	
indicating unique values in this sequence		

TP Id	SECPKI_CA_CERTGEN_17_BV		
Summary.	Check that SSP field in each entry of the appPermissions component of the AT certificate		
Summary	is equal to or a subset of the SSP Range in the corresponding issuing entry		
Reference IEEE Std 1609.2 [3], clauses 6.4.28 and 5.1.2.4			
PICS Selection PICS_GN_SECURITY			
	Expected behaviour		
with			
the CA is in 'operational	' state		
ensure that			
when			
the CA issued the cert			
containing toBeSign			
containing appPe	rmissions		
then			
	e EtsiTs103097Certificate		
containing issuer			
	referenced to the certificate		
containing toBe			
_	containing certIssuePermissions		
	containing items of type PsidGroupPermissions		
containing eeType			
	ating app(0)		
and containing subjectPermissions			
containing explicit			
containing items of type PsidSspRange			
containing psid			
indicating X_PSID_AA			
containing sspRange			
indicating X_SSP_AA [ X_PSID_AA ]			
or containing all containing toBeSigned			
containing tobeogned containing appPermissions			
containing apprentissions containing items of type PsidSsp			
containing psid			
	value equal to X_PSID_AA		
_	containing ssp		
	indicating value permitted by X_SSP_AA [ X_PSID_AA ]		

## 5.3.1.7 Check time validity restriction in the chain

TP Id	SECPKI_CA_CERTGEN_18_BV
Summary	Check that the validityPeriod of the subordinate certificate is inside the validityPeriod of the issuing certificate
Reference	IEEE Std 1609.2 [3], clause 5.1.2.4
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with the CA is in 'operational': and the CA is authorized containing toBeSigned containing validityPe containing start indicating X_ST containing duratio indicating X_DI	with CA certificate  Priod  FART_VALIDITY_CA  On
ensure that when the IUT issued the certificate then this certificate is of type EtsiTs103097Certificate	
containing toBeSigned containing validityPeriod containing start indicating X_START_VALIDITY ( X_START_VALIDITY >= X_START_VALIDITY_CA ) containing duration indicating value <= X_START_VALIDITY_CA + X_DURATION_CA - X_START_VALIDITY	

## 5.4 EA behaviour

### 5.4.0 Overview

All test purposes in the present clause may be included in the test sequence if the following PICS items is set:

PICS\_SECPKI\_IUT\_EA = TRUE

# 5.4.1 Enrolment request handling

TP Id	SECPKI_EA_ENR_RCV_01_BV		
Summary	The EnrolmentResponse message shall be sent by the EA to the ITS-S across the interface at reference point S3 in response to a received EnrolmentRequest message		
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2		
Configuration	CFG_ENR_EA		
PICS Selection			
	Expected behaviour		
with			
the EA is in 'operational'	the EA is in 'operational' state		
ensure that			
when	when		
the IUT receives an EnrolmentRequestMessage			
then			
the IUT answers with an EnrolmentResponseMessage			
across the interface at reference point S3			

TP ld	SECPKI_EA_ENR_RCV_02_BI	
11 14	Check that EA does not accept Enrolment rekeying request when enrolment is not	
Summary	permitted by signing certificate	
Reference	ETSI TS 102 941 [1], clause B.5	
Configuration	CFG_ENR_EA	
PICS Selection		
	Expected behaviour	
with	1	
the EA is in 'operational	state	
ensure that		
when		
	EnrolmentRequestMessage	
	crypted EtsiTs103097Data-Signed	
containing sig		
containing		
	indicating HashedId8 value	
referenced the certificate (CERT)		
containing appPermissions		
	not containing an item of type PsidSsp	
	containing psid	
	indicating AID_CERT_REQ	
or containing an item of type PsidSsp containing psid		
	indicating AID_CERT_REQ	
and containing ssp		
	containing opaque[0] (version)	
	indicating other value than 1	
or containing opaque[1] (value)		
indicating 'Enrolment Request' (bit 1) set to 0		
then	. , ,	
	h an EnrolmentResponseMessage	
containing InnerE0		
containing resp		
indicating 'de	eniedpermissions'	

TP Id	SECOND EVENT DOMESTICATION		
I P I a	SECPKI_EA_ENR_RCV_04_BI		
Summary	Enroll the ITS-Station, but the outer signature, created with the canonical private key, can		
Summary .	not be verified with the registered canonical public key		
Reference	ETSI TS 102 941 [1], clause B.5		
Configuration	CFG_ENR_EA		
PICS Selection			
	Expected behaviour		
with			
the EA is in 'operatio	nal' state		
ensure that	·		
when	when		
the IUT receives	the IUT receives an EnrolmentRequestMessage		
containing an	containing an outer signature		
signed with an unknown canonical private key			
then	· · · · · · · · · · · · · · · · · · ·		
the IUT answers	the IUT answers with an EnrolmentResponseMessage		
containing InnerECResponse			
containing responseCode			
indicating 'invalidsignature'			
and not containing a certificate			
and not com	anning a volument		

TP Id	SECPKI_EA_ENR_RCV_05_BI	
Summary	Enroll an ITS-Station, but with a canonical-ID, that is not registered	
Reference	ETSI TS 102 941 [1], clause B.5	
Configuration	CFG_ENR_EA	
PICS Selection		
	Expected behaviour	
with		
the EA is in 'operational'	state	
ensure that		
when		
the IUT receives an I	EnrolmentRequestMessage	
containing an Inn	erEcRequest	
containing Ho		
indicating an unknown canonical-ID		
then		
the IUT answers with an EnrolmentResponseMessage		
containing InnerECResponse		
containing respo	containing responseCode	
indicating 'deniedpermissions'		
and not containing a certificate		

TP Id	SECPKI_EA_ENR_RCV_06_BI	
Summary	Enroll the ITS-Station, but the CSR requests more permissions than the issuer allows, i.e. request for security management SSP bit which is not set in the EA SSP	
Reference	ETSI TS 102 941 [1], clause B.5	
Configuration	CFG_ENR_EA	
PICS Selection		
	Expected behaviour	
with		
the EA is in 'operati	onal' state	
ensure that		
when		
the IUT receives	s an EnrolmentRequestMessage	
containing a	n InnerEcRequest	
containin	g SSP	
indica	ating more permissions than EA allows	
then		
the IUT answers with an EnrolmentResponseMessage		
containing InnerECResponse		
containing i	containing responseCode	
indicating 'deniedpermissions'		
and not containing a certificate		

Summary	Enroll the ITS-Station, but the CSR requests a AID permission that the issuer does not		
	allow		
Reference ETSI TS 102 941 [1], clause B.5			
Configuration	CFG_ENR_EA		
PICS Selection			
	Expected behaviour		
with			
the EA is in 'operational'	state		
ensure that	ensure that		
when			
the IUT receives an EnrolmentRequestMessage			
containing an InnerEcRequest			
containing SSP			
containing an AID permission not authorized by EA			
then			
the IUT answers with an EnrolmentResponseMessage			
containing InnerECResponse			
containing responseCode			
indicating 'deniedpermissions'			
and not containing a certificate			

SECPKI\_EA\_ENR\_RCV\_07\_BI

TP Id

TP ld	SECPKI_EA_ENR_RCV_08_BI	
Summary	Enroll the ITS-Station, but the expiring date of the CSR is before the start date of the EA	
Reference	ETSI TS 102 941 [1]	
Configuration	CFG_ENR_EA	
PICS Selection		
	Expected behaviour	
with	·	
the EA is in 'operational'	state	
ensure that		
when		
the IUT receives an	EnrolmentRequestMessage	
containing an Inn	nerEcRequest	
containing Va	alidityPeriod	
indicating a value less than the start date of the EA		
then		
the IUT answers with	the IUT answers with an EnrolmentResponseMessage	
containing InnerECResponse		
containing resp	containing responseCode	
indicating 'deniedpermissions'		
and not contain	and not containing a certificate	

TP ld	SECPKI_EA_ENR_RCV_09_BI	
Summary	EEnroll the ITS-Station, but the start date of the CSR is before the start date of the EA	
Reference	ETSI TS 102 941 [1]	
Configuration	CFG_ENR_EA	
PICS Selection		
	Expected behaviour	
with		
the EA is in 'operational'	state	
ensure that		
when		
the IUT receives an EnrolmentRequestMessage		
containing an Inn	containing an InnerEcRequest	
containing Va	containing ValidityPeriod	
containing start date		
indicating a value less than the start date of the EA		
then		
the IUT answers with an EnrolmentResponseMessage		
containing InnerECResponse		
containing responseCode		
indicating 'de	eniedpermissions'	
and not containi	ing a certificate	

TP Id	SECPKI_EA_ENR_RCV_10_BI	
Summary	Enroll the ITS-Station, but expiring date of the CSR is after the expiring date of the EA	
Reference	ETSI TS 102 941 [1]	
Configuration	CFG_ENR_EA	
PICS Selection		
	Expected behaviour	
with		
the EA is in 'operational'	state	
ensure that		
when		
	the IUT receives an EnrolmentRequestMessage	
containing an InnerEcRequest		
containing ValidityPeriod		
indicating a value greater than the ValidityPeriod of the EA		
then		
the IUT answers with an EnrolmentResponseMessage		
containing InnerECResponse		
containing responseCode		
indicating 'deniedpermissions'		
and not containing a certificate		

TP Id	SECPKI_EA_ENR_RCV_11_BI	
Summary	Enroll the ITS-Station, but the start date of the CSR is after the expiring date of the EA	
Reference	ETSI TS 102 941 [1]	
Configuration	CFG_ENR_EA	
PICS Selection		
	Expected behaviour	
with		
the EA is in 'operational'	state	
ensure that		
when		
the IUT receives an I	the IUT receives an EnrolmentRequestMessage	
containing an InnerEcRequest		
containing ValidityPeriod		
containing start date		
indicating a value greater than the start date of the EA		
then		
the IUT answers with an EnrolmentResponseMessage		
containing InnerEC	containing InnerECResponse	
containing respo		
indicating 'deniedpermissions'		
and not containi	ng a certificate	

TP ld	SECPKI_EA_ENR_RCV_12_BI		
Summary	Enroll the ITS-Station, but the lifetime of the EC would be grater than allowed (considering		
	values in C-ITS CP)		
Reference	ETSI TS 102 941 [1]		
Configuration	CFG_ENR_EA		
PICS Selection			
	Expected behaviour		
with			
the EA is in 'operational'	state		
ensure that			
when			
	the IUT receives an EnrolmentRequestMessage		
containing an Inn	·		
containing ValidityPeriod			
indicating a value greater than 100 years			
then	· ·		
the IUT answers with an EnrolmentResponseMessage			
containing InnerECResponse			
	containing responseCode		
indicating 'deniedpermissions'			
and not containing a certificate			

TP Id	SECPKI_EA_ENR_RCV_13_BI		
Summary	Enroll the ITS-Station, but the inner PoP signature in the CSR, created with the EC private		
	key, can not be verified with the provided public key		
Reference	ETSI TS 102 941 [1]		
Configuration	CFG_ENR_EA		
PICS Selection			
	Expected behaviour		
with			
the EA is in 'operational'	state		
ensure that			
when	when		
the IUT receives an EnrolmentRequestMessage			
	containing an InnerEcRequest		
signed with a	signed with a private key SIGN_POP_PRIVATE_KEY		
and containing public verification keys			
indicating a value which does not match with the private key SIGN_POP_PRIVATE_KEY			
then			
the IUT answers with an EnrolmentResponseMessage			
containing InnerECResponse			
containing responseCode			
indicating 'inv	/alidsignature'		
and not containing a certificate			

TP Id	SECPKI_EA_ENR_RCV_14_BV		
Summary	Check that EA send the same response for the repeated EC request		
Reference	ETSI TS 103 601 [6], clause 5.1		
Configuration	CFG_ENR_EA		
PICS Selection	PICS_SECPKI_ENROLMENT_RETRY		
	Expected behaviour		
with			
the EA is in 'operational'	state		
	ived EnrolmentRequestMessage ( <i>REQ</i> )		
having checksum (C			
Š	and the EA has sent the EnrolmentResponseMessage ( <i>RES</i> )		
containing responseCode			
indicating OK			
ensure that			
when			
the IUT receives an EnrolmentRequestMessage			
having checksum			
indicating value equal to <b>CS</b>			
then			
the IUT answers with an EnrolmentResponseMessage			
indicating <b>RES</b>			
	. •		

TP ld	SECPKI_EA_ENR_RCV_15_BV		
Summary	Check that EA does not accept emrollment when message generation time is too far in the		
Summary	past		
Reference	ETSI TS 103 601 [6], clause 5.1.4		
Configuration	CFG_ENR_EA		
PICS Selection	PICS_SECPKI_ENROLMENT_RETRY		
	Expected behaviour		
with			
the EA is in 'operational	' state		
and the EA already rece	eived the EnrolmentRequestMessage ( <i>REQ</i> )		
containing generation	containing generationTime <i>TG</i>		
and having checksum (CS)			
ensure that			
when			
the IUT receives an	EnrolmentRequestMessage		
at the moment T	R2		
indicating TR	R2 > TG + PIXIT_EA_ENROLLMENT_TIMEOUT		
and having checksum			
indicating value equal to CS			
then			
the IUT answers with	h an EnrolmentResponseMessage		
containing responseCode			
indicating de	niedrequest		
NOTE: PIXIT_EA_ENRO	OLLMENT_TIMEOUT shall be set as a TP parameter.		

# 5.4.2 Enrolment response

TP ld	SECPKI_EA_ENR_01_BV
Summary	The EnrolmentResponse message shall be encrypted using an ETSI TS 103 097 [2] approved algorithm and the encryption shall be done with the same AES key as the one used by the ITS-S requestor for the encryption of the EnrolmentRequest message
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT receive	es an EnrolmentRequestMessage
containing e	ncKey
containing	g an encrypted AES key (SYMKEY)
then	
the IUT answe containing cip	ers with an EnrolmentResponseMessage oherText
being enc	rypted using SYMKEY

TP ld	SECPKI_EA_ENR_02_BV	
Summary	The EnrolmentResponse message shall be encrypted using an ETSI TS 103 097 [2] approved algorithm and the encryption shall be done with the same AES key as the one used by the ITS-S requestor for the encryption of the EnrolmentRequest message	
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2	
Configuration	CFG_ENR_EA	
PICS Selection		
	Expected behaviour	
ensure that		
when		
the IUT receives an I	the IUT receives an EnrolmentRequestMessage	
containing encKey	containing encKey	
containing an encrypted AES key (SYMKEY)		
then	then	
the IUT answers with an EnrolmentResponseMessage		
containing cipherText		
being encrypted		
using SYMKEY		
and using an ETSI TS 103 097 [2] approved algorithm		

TP ld	SECPKI_EA_ENR_03_BV
Summary	The outermost structure is an EtsiTs103097Data-Encrypted structure containing the component recipients containing one instance of RecipientInfo of choice pskRecipInfo, which contains the HashedId8 of the symmetric key used by the ITS-S to encrypt the EnrolmentRequest message to which the response is built and containing the component ciphertext, once decrypted, contains an EtsiTs103097Data-Signed structure
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
then	rolmentResponseMessage as an answer for an EnrolmentRequestMessage siTs103097Data-Encrypted structure

TP Id	SECPKI_EA_ENR_04_BV
Summary	If the ITS-S has been able to decrypt the content, this expected EtsiTs103097Data-Signed structure shall contain hashId, tbsData, signer and signature. The hashId shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [2], the signer shall be declared as a digest, containing the HashedId8 of the EA certificate and the signature over tbsData shall be computed using the EA private key corresponding to its publicVerificationKey found in the referenced EA certificate
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
ensure that when	

the IUT sends an  ${\tt EnrolmentResponseMessage}$  as an answer for an  ${\tt EnrolmentRequestMessage}$  then

the IUT sends an EtsiTs103097Data-Encrypted structure containing an encrypted EtsiTs103097Data-Signed structure

containing hashId

indicating the hash algorithm to be used as specified in ETSI TS 103 097 [2]

and containing tbsData and containing signer

declared as a digest

containing the HashedId8 of the EA certificate

and containing signature computed over tbsData using the EA private key

corresponding to the public Verification Key found in the referenced EA certificate

TP Id	SECPKI_EA_ENR_05_BV
Summary	Within the headerInfo of the tbsData, the psid shall be set to "secured certificate request"
	as assigned in ETSI TS 102 965 [i.2] and the generationTime shall be present
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2
Configuration	CFG_ENR_EA
PICS Selection	
Provide III also the control of the	

#### **Expected behaviour**

#### ensure that

when

the IUT sends an  ${\sf EnrolmentResponseMessage}$  as an answer for an  ${\sf EnrolmentRequestMessage}$  then

the IUT sends an EtsiTs103097Data-Encrypted structure containing an encrypted EtsiTs103097Data-Signed structure containing tbsData containing headerInfo containing psid

indicating AID\_CERT\_REQ and containing generationTime

TP Id	SECPKI_EA_ENR_06_BV	
Summary	Within the headerInfo of the tbsData, aside from psid and generationTime, all other	
	components of the component tbsData.headerInfo not used and absent	
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2	
Configuration	CFG_ENR_EA	
PICS Selection		
	Expected behaviour	
ensure that		
when		
the IUT sends an EnrolmentResponseMessage as an answer for an EnrolmentRequestMessage		
then		
	the IUT sends an EtsiTs103097Data-Encrypted structure	
containing an encry	containing an encrypted EtsiTs103097Data-Signed structure	
containing tbsData		
containing headerInfo		
containing psid		
and containing generationTime		
and not containing any other component of tbsData.headerInfo		

TP ld	SECPKI_EA_ENR_07_BV		
Summary.	The EtsiTS102941Data shall contain the version set to v1 (integer value set to 1) and the		
Summary	content set to InnerECResponse		
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2		
Configuration	CFG_ENR_EA		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the IUT sends an En	the IUT sends an EnrolmentResponseMessage as an answer for an EnrolmentRequestMessage		
then	then		
	the IUT sends an EtsiTs103097Data-Encrypted structure		
containing an encrypted EtsiTs103097Data-Signed structure			
containing tbsData			
containing EtsiTS102941Data			
containing version			
indicating v1 (integer value set to 1)			

Summary	The InnerECResponse shall contain the requestHash, which is the left-most 16 octets of the SHA256 digest of the EtsiTs103097Data - Signed structure received in the request and		
,	a responseCode indicating the result of the request		
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2		
Configuration	CFG_ENR_EA		
PICS Selection			
	Expected behaviour		
ensure that			
when	· ·		
the IUT sends an En	rolmentResponseMessage as an answer for an EnrolmentRequestMessage		
then			
	the IUT sends an EtsiTs103097Data-Encrypted structure		
containing an encry	/pted EtsiTs103097Data-Signed structure		
containing tbsDa	ata		
containing Ets	siTS102941Data		
containing InnerECResponse			
containing requestHash			
indicating the left-most 16 octets of the SHA256 digest			
	the EtsiTs103097Data-Signed structure received in the request		
and containing responseCode			

SECPKI\_EA\_ENR\_08\_BV

TP Id

TP ld	SECPKI_EA_ENR_09_BV	
Summary	If the responseCode is 0, the InnerECResponse shall also contain an (enrolment)	
	certificate	
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2	
Configuration	CFG_ENR_EA	
PICS Selection		
	Expected behaviour	
ensure that		
when		
the IUT is requested	to send an EnrolmentResponseMessage	
containing a respo	containing a responseCode	
indicating 0		
then		
the IUT sends an Ets	siTs103097Data-Encrypted structure	
containing an encrypted EtsiTs103097Data-Signed structure		
containing tbsData		
containing EtsiTS102941Data		
containing InnerECResponse		
containing an enrolment certificate		

TP Id	SECPKI_EA_ENR_10_BV
Summary	If the responseCode is different than 0, the InnerECResponse shall not contain a
	certificate
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT is requ	uested to send an EnrolmentResponseMessage
containing a	responseCode
indicating	a value different than 0
then	
the IUT sends	an EtsiTs103097Data-Encrypted structure
	n encrypted EtsiTs103097Data-Signed structure
containing	
	ing EtsiTS102941Data
	ining InnerECResponse
	t containing a certificate

TP Id	SECPKI_EA_ENR_11_BV			
Summary	Check that signing of Enrolment response message is permitted by the EA certificate			
Reference	ETSI TS 102 941 [1], clause B.5			
Configuration	CFG_ENR_EA			
PICS Selection				
Expected behaviour				
ensure that				
when				
the IUT sends an En	rolmentResponseMessage as an answer for an EnrolmentRequestMessage			
then				
	siTs103097Data-Encrypted structure			
containing an encrypted EtsiTs103097Data-Signed structure				
containing signe				
declared as a				
•	he HashedId8 of the EA certificate			
	containing appPermissions			
containing an item of type PsidSsp				
containing psid				
indicating AID_CERT_REQ				
ar	nd containing ssp			
containing opaque[0] (version)				
	indicating 1			
	containing opaque[1] (value)			
	indicating bit 'Enrolment Response' (5) set to 1			

TP Id	SECPKI_EA_ENR_12_BV				
Summary	Check that generated EC certificate contains only allowed permissions				
Reference	ETSI TS 102 941 [1], clause B.5				
Configuration	CFG_ENR_EA				
PICS Selection					
	Expected behaviour				
ensure that					
when					
•	to send an EnrolmentResponseMessage				
containing a certific	cate (EC_CERT)				
then					
the EC_CERT					
containing appPe					
•	item of type PsidSsp				
containing psid					
	ring AID_CERT_REQ				
and conta	ning ssp ning opaque[0] (version)				
indicating 1 containing opaque[1] (value)					
indicating 'Enrolment Request' (bit 0) set to 1					
indicating 'Authorization Request' (bit 1) set to 1					
indicating other bits set to 0					
and NOT containing an item of type PsidSsp					
containing psid					
indicating AID_CTL					
and NOT con	taining an item of type PsidSsp				
containing	psid				
indicat	ing AID_CRL				

# 5.4.3 Authorization validation request handling

TP Id	SECPKI_EA_AUTHVAL_RCV_01_BV		
	The AuthorizationValidationResponse message shall be sent by the EA to the AA across		
Summary	the interface at reference point S4 in response to a received		
	AuthorizationValidationRequest message		
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2		
Configuration	CFG_AVALID_EA		
PICS Selection			
Expected behaviour			
ensure that			
when			
the IUT receive	es a AuthorizationValidationRequest message		
then			
the IUT sends a	a AuthorizationValidationResponse message		
across the i	reference point S4 to the AA		

TP ld	SECPKI_EA_AUTHVAL_RCV_02_BI
Summary	Check that EA does not accept Authorization Validation Request when SharedAtRequest
	is signed with certificate without appropriate permissions
Reference	ETSI TS 102 941 [1], clause B.5
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT receive	es an AuthorizationValidationRequestMessage
containing I	EtsiTs102941Data
containing	g ecSignature
	ning signer
	ntaining digest
	indicating HashedId8 of the certificate EC certificate
	containing appPermissions
	not containing an item of type PsidSsp
	containing psid
	indicating AID_CERT_REQ
	or containing an item of type PsidSsp
	containing psid
	indicating AID_CERT_REQ
	and containing ssp
	containing opaque[0] (version)
	indicating other value than 1
	or containing opaque[1] (value)
	indicating 'Authorization Request' (bit 2) set to 0
then	
	rs with an AuthorisationValidationResponseMessage
containing re	sponseCode
indicating	'deniedpermissions'

# 5.4.4 Authorization validation response

TP Id	SECPKI_EA_AUTHVAL_01_BV
Summary	The EtsiTs103097Data-Encrypted is built with the component recipients containing one instance of RecipientInfo of choice pskRecipInfo, which contains the HashedId8 of the symmetric key used by the ITS-S to encrypt the AuthorizationRequest message to which the response is built and the component ciphertext containing the encrypted representation of the EtsiTs103097Data-Signed. The encryption uses a ETSI TS 103 097 [2] approved algorithm
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2
I/CICI CITOC	ETSI TS 103 097 [2], clause 7
Configuration	CFG_AVALID_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT receive	s a AuthorizationValidationRequest message
containing ench	Key
containing the	e encrypted symmetric data encryption key (SYMKEY)
then	
the IUT sends a	a AuthorizationValidationResponse message
containing Ets	siTs103097Data-Encrypted
containing	recipients
containi	ng one instance of RecipientInfo of choice pskRecipInfo
indic	ating the HashedId8 of SYMKEY
and contain	ning ciphertext
containi	ng EtsiTs103097Data-Signed
being	g encrypted using SYMKEY and an ETSLTS 103 097 [2] approved algorithm

TP ld	SECPKI_EA_AUTHVAL_02_BV		
Summary	To read an authorization validation response, the AA shall receive an EtsiTs103097Data- Encrypted structure, containing a EtsiTs103097Data-Signed structure, containing a EtsiTs102941Data structure, containing an AuthorizationValidationResponse structure		
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2		
Configuration	CFG_AVALID_EA		
PICS Selection			
	Expected behaviour		
ensure that			
when	when		
the IUT receives a AuthorizationValidationRequest message			
then			
the IUT sends a AuthorizationValidationResponse message containing EtsiTs103097Data-Signed containing EtsiTs102941Data containing AuthorizationValidationResponse			

TP Id	SECPKI_EA_AUTHVAL_03_BV
Summary	The AuthorizationValidationResponse structure contains the requestHash being the left-most 16 octets of the SHA256 digest of the EtsiTs103097Data-Signed structure received in the AuthorizationValidationRequest and a responseCode
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2
Configuration	CFG_AVALID_EA
PICS Selection	
	Expected behaviour
containing EtsiTs10 then the IUT sends a Auth containing EtsiTs1 containing EtsiT containing Ar containing indicatir	uthorizationValidationRequest message 03097Data-Signed structure (REQDSS) norizationValidationResponse message 03097Data-Signed

TP Id	SECPKI_EA_AUTHVAL_04_BV
	If the responseCode is 0, the AuthorizationValidationResponse structure contains the
Summary	component confirmedSubjectAttributes with the attributes the EA wishes to confirm, except
	for certIssuePermissions which is not allowed to be present
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2
Configuration	CFG_AVALID_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT receive	s a AuthorizationValidationRequest message
and the IUT res	sponds with a AuthorizationValidationResponse message
containing Au	uthorizationValidationResponse
containing	responseCode
indicatii	ng Ö
then	
the sent Author	rizationValidationResponse message
contains an A	AuthorizationValidationResponse structure
containing	confirmedSubjectAttributes
not con	taining certIssuePermissions

TP ld	SECPKI_EA_AUTHVAL_05_BV	
Summary	If the responseCode is different than 0, the AuthorizationValidationResponse structure	
	does not contain the component confirmedSubjectAttributes	
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2	
Configuration	CFG_AVALID_EA	
PICS Selection		
	Expected behaviour	
ensure that		
when		
	the IUT receives a AuthorizationValidationRequest message	
	and the IUT responds with a AuthorizationValidationResponse message	
_	containing AuthorizationValidationResponse	
containing resp		
	indicating a value different than 0	
then		
the sent AuthorizationValidationResponse message		
contains an AuthorizationValidationResponse structure		
not containing confirmedSubjectAttributes		

TP Id	SECPKI_EA_AUTHVAL_06_BV
Summary	The component version of the EtsiTs102941Data structure is set to v1 (integer value set
	to 1)
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2
Configuration	CFG_AVALID_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT receives	s a AuthorizationValidationRequest message
then	
the IUT sends a	a AuthorizationValidationResponse message
containing Ets	siTs103097Data-Signed
containing	EtsiTs102941Data
containi	ng version
indica	ating v1 (integer value set to 1)

TP ld	SECPKI_EA_AUTHVAL_07_BV
Summary	EtsiTs103097Data-Signed.tbsData contains the EtsiTs102941Data as payload and the headerInfo containing psid and generationTime. The psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [i.2] and the generationTime shall be present. All other components of the component tbsdata.headerInfo are not used and absent
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2
Configuration	CFG_AVALID_EA
PICS Selection	
	Expected behaviour
ensure that when the IUT receives a AuthorizationValidationRequest message then the IUT sends a AuthorizationValidationResponse message containing EtsiTs103097Data-Signed containing tbsData containing headerInfo containing psid indicating AID_CERT_REQ and containing generationTime and not containing any other component of tbsdata.headerInfo	

TP Id	SECPKI EA AUTHVAL 08 BV	
	EtsiTs103097Data-Signed structure shall contain hashld, tbsData, signer and signature. The hashld shall indicate the hash algorithm to be used as specified in ETSI	
Summary	TS 103 097 [2], the signer shall be declared as a digest, containing the Hashedld8 of the	
	EA certificate and the signature over tbsData shall be computed using the EA private key corresponding to its publicVerificationKey found in the referenced EA certificate	
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2	
Configuration	CFG_AVALID_EA	
PICS Selection	0.0	
	Expected behaviour	
ensure that	·	
when		
	authorizationValidationRequest message	
then		
	the IUT sends a AuthorizationValidationResponse message	
	containing an EtsiTs103097Data-Signed structure	
containing hashId		
indicating the hash algorithm to be used as specified in ETSI TS 103 097 [2]		
	and containing tbsData	
and containing signer		
declared as a digest		
containing the HashedId8 of the EA certificate		
and containing signature		
computed over tbsData		
using the EA private key		
correspo	onding to the publicVerificationKey found in the referenced EA certificate	

TP ld	SECPKI_EA_AUTHVAL_09_BV
Summary	Check that signing of Authorization Validation response message is permitted by the EA
	certificate
Reference	ETSI TS 102 941 [1], clause B.5
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT is requested	to send an AuthorizationValidationResponseMessage
then	
	siTs103097Data-Encrypted structure
containing an encry	/pted EtsiTs103097Data-Signed structure
containing signe	yr
containing dig	
	lashedId8 of the EA certificate
containir	ng appPermissions
conta	ining an item of type PsidSsp
со	ntaining psid
į i	ndicating AID_CERT_REQ
an	d containing ssp
	containing opaque[0] (version)
	indicating 1
	containing opaque[1] (value)
	indicating 'Authorisation Validation Response' (bit 4) set to 1

# 5.4.5 CA Certificate Request

TP ld	SECPKI_EA_CERTGEN_01_BV
Summary	SubCA certificate requests of the EA are transported to the RCA using
	CACertificateRequest messages across the reference point S10
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_INIT
PICS Selection	
	Expected behaviour
ensure that	·
when	
the IUT is requ	ested to send a CACertificateRequestMessage
then	
the IUT sends	a CACertificateRequestMessage
across the	reference point S10 to the RCA

TP ld	SECPKI_EA_CERTGEN_02_BV	
Summary	The application form should include the digital fingerprint of the CACertificateRequestMessage in printable format. The digital fingerprint of the CACertificateRequestMessage is computed using a ETSLTS 103 097 [2] approved hash algorithm	
Reference	ETSI TS 102 941 [1], clause 6.2.1	
Configuration	CFG_CAGEN_INIT	
PICS Selection		
	Expected behaviour	
with the IUT being in the 'i ensure that when	initial' state	
the IUT is requested to send a CACertificateRequestMessage		
then		
the IUT sends a CACertificateRequestMessage containing a signature (SIG) being computed using a ETSI TS 103 097 [2] approved hash algorithm		
and the IUT expo	and the IUT exports the digital fingerprint SIG in a printable format.	

TP ld	SECPKI_EA_CERTGEN_03_BV
Summary	The hashId shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [2], the signer is set to 'self' and the signature over the tbsData is computed using the private key corresponding to the new verificationKey to be certified (i.e. the request is self-signed)
Reference	ETSI TS 102 941 [1], clause 6.2.1 ETSI TS 103 097 [2], clause 7
Configuration	CFG_CAGEN_INIT
PICS Selection	
	Expected behaviour
then the IUT sends a being an Ets containing indicati and conta indicati and conta	ested to send a CACertificateRequestMessage a CACertificateRequestMessage siTs103097Data-Signed structure hashId ng the hash algorithm to be used ining signer ng 'self' ining tbsData
containing CaCertificateRequest containing publicKeys containing verification_key (VKEY) and containing signature computed over tbsData using the private key corresponding to the verificationKey (VKEY)	

TP ld	SECPKI_EA_CERTGEN_04_BV
	An ECC private key is randomly generated, the corresponding public key (verificationKey)
Summary	is provided to be included in the CaCertificateRequest.  An ECC encryption private key is randomly generated, the corresponding public key
Juninary	(encryptionKey) is provided to be included in the CACertificateRequest.
	CaCertificateRequest.publicKeys shall contain verification_key and encryption_key
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_INIT
PICS Selection	
	Expected behaviour
with	
the IUT being in th	ne 'initial' state
ensure that	
when	
the IUT is requ	uested to send a CACertificateRequestMessage
then	
the IUT sends	a CACertificateRequestMessage
containing	CaCertificateRequest
containin	g publicKeys
contai	ning verification_key
and co	ontaining encryption_key

TP Id	SECPKI_EA_CERTGEN_05_BV		
Summary	The EtsiTs102941Data structure is built with version set to v1 (integer value set to 1)		
Reference	ETSI TS 102 941 [1], clause 6.2.1		
Configuration	CFG_CAGEN_INIT		
PICS Selection			
	Expected behaviour		
with			
the IUT being in the 'in	itial' state		
ensure that	ensure that		
when			
the IUT is requeste	the IUT is requested to send a CACertificateRequestMessage		
then			
the IUT sends a CACertificateRequestMessage			
containing EtsiTs102941Data			
containing version			
indicating v1 (integer value set to 1)			

TP Id	SECPKI_EA_CERTGEN_06_BV	
Summary	CaCertificateRequest.requestedSubjectAttributes shall contain the requested certificates	
-	attributes as specified in ETSI TS 103 097 [2] clause 7.2.4	
Reference	ETSI TS 102 941 [1], clause 6.2.1	
Kelefelle	ETSI TS 103 097 [2], clause 7.2.4.	
Configuration	CFG_CAGEN_INIT	
PICS Selection		
Expected behaviour		
with		
the IUT being in the 'initial' state		
ensure that		
when		
the IUT is requested to send a CACertificateRequestMessage		
then		
the IUT sends a CACertificateRequestMessage		
containing	CaCertificateRequest	
containin	g requestedSubjectAttributes	
as specified in ETSI TS 103 097 [2] clause 7.2.4.		

TP ld	SECPKI_EA_CERTGEN_07_BV		
Summary	EtsiTs103097Data-Signed.tbsData contains the EtsiTs102941Data as payload and the headerInfo containing psid and generationTime. The psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [i.2] and the generationTime shall be present. All other components of the component tbsdata.headerInfo are not used and absent		
Reference	ETSI TS 102 941 [1], clause 6.2.1		
Configuration	CFG_CAGEN_INIT		
PICS Selection			
	Expected behaviour		
with			
the IUT being in the 'initi	al' state		
ensure that			
when	when		
the IUT is requested to send a CACertificateRequestMessage			
then			
the IUT sends a CACertificateRequestMessage			
containing headerInfo			
containing psid			
indicating SEC_CERT_REQ			
and containing generationTime			
and not containing any other component of tbsdata.headerInfo			

TP ld	SECPKI_EA_CERTGEN_08_BV
Summary.	If the current private key has reached its end of validity period or is revoked, the SubCA
Summary	shall restart the initial certificate application process
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_REKEY
PICS Selection	
	Expected behaviour
and SubCA certificate then the IUT switches to tl	to send a CACertificateRekeyingMessage e is no longer valid (due to end of validity or revocation)

TP ld	SECPKI_EA_CERTGEN_09_BV		
Summary	For the re-keying application to the RCA (CaCertificateRekeyingMessage), an EtsiTs103097Data-Signed structure is built, containing: hashId, tbsData, signer and signature. The hashId shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [2]. The signer declared as a digest, containing the hashedId8 of the EA certificate and the signature over tbsData is computed using the currently valid private key corresponding to the EA certificate (outer signature)		
Reference	ETSI TS 102 941 [1], clause 6.2.1 ETSI TS 103 097 [2], clause 7		
Configuration	CFG_CAGEN_REKEY		
PICS Selection			
	Expected behaviour		
with			
the IUT being in the 'op-	erational' state		
	ensure that		
when			
the IUT is requested to send a CACertificateRekeyingMessage			
	then		
the sends a CACertificateRekeyingMessage			
being an EtsiTs103097Data-Signed structure			
containing hashId			
	indicating the hash algorithm to be used		
and containing the Data			
and containing signer			
containing digest indicating HashedId8 of the SubCA certificate (CERT)			
and containing signature			
computed ov			
using the private key corresponding to CERT			
doing the p	mate to, conceptioning to certi		

TP ld	SECPKI_EA_CERTGEN_10_BV
Summary	The (outer) tbsData of the CACertificateRekeyingMessage shall contain the CaCertificateRequestMessage as payload
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_REKEY
PICS Selection	
	Expected behaviour
with	
the IUT being in th	e 'operational' state
ensure that	
when	
the IUT is requ	ested to send a CACertificateRekeyingMessage
then	
the sends a CACertificateRekeyingMessage	
containing tbsData	
containing CaCertificateRequestMessage	

TP ld	SECPKI_EA_CERTGEN_11_BV
	The (outer) tbsData of the CACertificateRekeyingMessage shall contain a headerInfo containing psid and generationTime. The psid shall be set to "secured"
Summary	certificate request" as assigned in ETSI TS 102 965 [i.2] and the generationTime shall be
	present. All other components of the component tbsdata.headerInfo are not used and
	absent
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_REKEY
PICS Selection	
	Expected behaviour
with	
the IUT being in the 'ope	erational' state
ensure that	
when	
the IUT is requested to send a CACertificateRekeyingMessage	
then	
the sends a CACertificateRekeyingMessage	
containing tbsData	
Containing headerInfo	
containing psid	
indicating SEC_CERT_REQ	
and containing generationTime	
and not containing any other component of tbsdata.headerInfo	

TP Id	SECPKI EA CERTGEN 12 BV	
Summary	Check that the CaCertificateRekeyingMessage is permitted by CA certificate	
	ETSI TS 102 941 [1], clause 6.2.1	
Configuration	CFG_CAGEN_REKEY	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the 'ope	erational' state	
ensure that		
when		
the IUT is requested	to send a CACertificateRekeyingMessage	
then		
the sends a CACertif	ricateRekeyingMessage	
being an EtsiTs103	3097Data-Signed structure	
and containing tbsData		
and containing	g signer	
containing dig	jest	
indicating HashedId8 of the CA certificate		
containing appPermissions		
containing an item of type PsidSsp		
containing psid		
indicating AID_CERT_REQ		
and containing ssp		
containing opaque[0] (version)		
indicating 1		
С	ontaining opaque[1] (value)	
indicating 'CA Certificate Response' (bit 6) set to 1		

### 5.5 AA behaviour

### 5.5.0 Overview

All test purposes in the present clause may be included in the test sequence if the following PICS items is set:

```
PICS\_SECPKI\_IUT\_AA = TRUE
```

# 5.5.1 Authorization request handling

TP Id	SECPKI_AA_AUTH_RCV_01_BV	
	Check that the AA is able to decrypt the AuthorizationRequest message using the	
	encryption private key corresponding to the recipient certificate	
Summari.	Check that the AA is able to verify the inner signature	
Summary	Check that the AA is able to verify the request authenticity using the hmacKey verification	
	Check that the AA sends the AuthorizationValidationRequest message to the	
	correspondent EA	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_AA	
PICS Selection	PICS_PKI_AUTH_POP=TRUE	
	Expected behaviour	
with		
the AA in 'operational' s		
	certificate CERT_AA	
	ptionKey (AA_ENC_PUB_KEY)	
ensure that when		
the IUT is received t	he EtsiTs103097Data message	
	nt.encryptedData	
containing re	cipients	
	the instance of RecipientInfo	
	ining certRecipInfo	
СО	ntaining recipientId	
	indicating HashedId8 of the certificate CERT_AA	
an	d containing encKey	
	indicating symmetric key (S_KEY)	
and containin	encrypted with the private key correspondent to the AA_ENC_PUB_KEY	
	and containing cyphertext (ENC_DATA)	
	containing encrypted representation of the EtsiTs103097Data-Signed	
containing content.signedData		
containing hashId indicating valid hash algorithm		
and containing signer		
	intaining self	
and containing tbsData (SIGNED_DATA)		
containing babata (of one beath)		
containing EtsiTs102941Data		
containing content.authorizationRequest		
containing publicKeys.verificationKey (V_KEY)		
and containing hmacKey (HMAC)		
and containing sharedAtRequest		
containing keyTag (KEY_TAG)		
and containing eald (EA_ID)		
indicating HashedId8 of the known EA certificate		
	ontaining signature (SIGNATURE)	
then	convert the C. V.C.V.	
the IUT is able to de using the private		
corresponding to the AA_ENC_PUB_KEY and the IUT is able to decrypt the cypthertext ENC_DATA		
using the S_KE		
	to verify the signature over the SIGNED_DATA	
using the V_KE		
	to verify integrity of HMAC and KEY_TAG	
	he AuthorizationValidationRequest message to the EA	
identified by the		
identified by the		

TP Id	SECPKI_AA_AUTH_RCV_02_BV
	Check that the AA is able to decrypt the AuthorizationRequest message using the
	encryption private key corresponding to the recipient certificate
Summary	Check that the AA is able to verify the request authenticity using the hmacKey verification
	Check that the AA sends the AuthorizationValidationRequest message to the
	correspondent EA
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS_PKI_AUTH_POP=FALSE
	Expected behaviour
with	
the AA in 'operational' st	
authorized with the o	
	otionKey (AA_ENC_PUB_KEY)
ensure that	
when	
	ne EtsiTs103097Data message
containing conter	
containing red	
	the instance of RecipientInfo
	ning certRecipInfo
containing recipientId	
indicating HashedId8 of the certificate CERT_AA	
and containing encKey	
indicating symmetric key (S_KEY)	
encrypted with the private key correspondent to the AA_ENC_PUB_KEY	
and containing cyphertext (ENC_DATA)	
containing EtsiTs102941Data	
containing content.authorizationRequest	
containing hmacKey (HMAC)	
and containing sharedAtRequest	
containing keyTag (KEY_TAG)	
and containing eald (EA_ID)	
thon	indicating HashedId8 of the known EA certificate
then	crupt the S. KEV
the IUT is able to decrypt the S_KEY using the private key	
using the private key corresponding to the AA_ENC_PUB_KEY	
and the IUT is able to decrypt the cypthertext ENC_DATA	
using the S_KEY	
and the IUT is able to verify integrity of HMAC and KEY_TAG	
and the IUT sends the AuthorizationValidationRequest message to the EA	
identified by the I	EA_IU

TP Id	SECPKI_AA_AUTH_RCV_03_BI	
Summary	Check that the AA skips the AuthorizationRequest message if it is not addressed to this AA	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_AA	
PICS Selection		
	Expected behaviour	
with		
the AA in 'operational' st	ate	
authorized with the o	certificate CERT_AA	
containing encry	ptionKey (AA_ENC_PUB_KEY)	
ensure that		
when		
the IUT is received the	he EtsiTs103097Data message	
containing content.encryptedData		
containing red	$\cdot$	
	g only one instance of RecipientInfo	
	ning certRecipInfo	
containing recipientId		
indicating value		
NOT equal to the HashedId8 of the certificate CERT_AA		
and containing encKey		
indicating symmetric key (S_KEY)		
1	encrypted with the private key correspondent to the AA_ENC_PUB_KEY	
then		
the IUT does not ser	nd the AuthorizationValidationRequest message	

TP Id	SECPKI_AA_AUTH_RCV_04_BI	
Summary	Check that the AA skips the AuthorizationRequest message if it unable to decrypt the encKey	
Reference	ETSLTS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_AA	
PICS Selection		
	Expected behaviour	
with		
the AA in 'operational' st	ate	
authorized with the c	ertificate CERT_AA	
containing encryp	otionKey (AA_ENC_PUB_KEY)	
ensure that		
when		
the IUT is received the	ne EtsiTs103097Data message	
containing content.encryptedData		
containing recipients		
containing the instance of RecipientInfo		
	ning certRecipInfo	
containing recipientId		
indicating value		
equal to the HashedId8 of the certificate CERT_AA		
and containing encKey		
indicating symmetric key (S_KEY)		
	encrypted with the OTHER private key than the correspondent to the	
AA_ENC_PUB_KEY		
then		
the IUT does not ser	nd the AuthorizationValidationRequest message	

TP Id	SECPKI_AA_AUTH_RCV_05_BI	
Summary	Check that the AA skips the AuthorizationRequest message if it unable to decrypt the	
	cyphertext	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_AA	
PICS Selection		
	Expected behaviour	
with		
the AA in 'operational' st	tate	
authorized with the o	certificate CERT_AA	
containing encryptionKey (AA_ENC_PUB_KEY)		
ensure that		
when		
the IUT is received the	he EtsiTs103097Data message	
containing conter	containing content.encryptedData	
containing red	containing recipients[0].encKey	
indicating	indicating encrypted symmetric key (S_KEY)	
and containing cyphertext (ENC_DATA)		
encrypted with the OTHER key than S_KEY		
then		
and the IUT does not send the AuthorizationValidationRequest message to the correspondent EA		

TP Id	SECPKI_AA_AUTH_RCV_06_BI		
Summary	Check that the AA rejects the AuthorizationRequest message if it unable to verify the POP		
Summary	signature		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1		
Configuration	CFG_AUTH_AA		
PICS Selection	PICS_PKI_AUTH_POP=TRUE		
	Expected behaviour		
with			
the AA in 'operational' st	ate		
authorized with the o	<del>-</del>		
	ptionKey (AA_ENC_PUB_KEY)		
ensure that			
when			
	he EtsiTs103097Data message		
_	containing content.encryptedData.cyphertext		
	containing encrypted representation of the EtsiTs103097Data-Signed (SIGNED_DATA)		
	containing content.signedData		
containing tbsData			
COI	containing payload		
containing EtsiTs102941Data containing content.authorizationRequest			
	containing content.authorizationRequest containing publicKeys.verificationKey (V_KEY)		
and containing signature (SIGNATURE)			
	indicating value calculated with OTHER key than private key correspondent to V_KEY		
then			
and the IUT does no	and the IUT does not send the AuthorizationValidationRequest message		
and the IUT sends to the TS the AuthorizationResponse message			
containing authorizationResponse			
containing red	questHash		
indicating the leftmost 16 bits of the SHA256 value			
	calculated over the SIGNED_DATA		
	ng responseCode		
indicating the value NOT EQUAL to 0			
and not conta	aining certificate		

TP ld	SECPKI_AA_AUTH_RCV_07_BI
Summary	Check that the AA rejects the AuthorizationRequest message if it unable to verify the
	integrity of the request using hmacKey
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	X_PICS

#### **Expected behaviour**

with

the AA in 'operational' state

authorized with the certificate CERT\_AA

containing encryptionKey (AA\_ENC\_PUB\_KEY)

ensure that

when

the IUT is received the EtsiTs103097Data message

containing EtsiTs102941Data

containing content.authorizationRequest containing hmacKey (HMAC) and containing sharedAtRequest containing keyTag (KEY\_TAG)

indicating wrong value

then

and the IUT does not send the AuthorizationValidationRequest message

and the IUT sends to the TS the Authorization Response message  $\,$ 

containing authorizationResponse

containing requestHash

indicating the leftmost 16 bits of the SHA256 value

calculated over the X\_HASH\_STRUCTURE

and containing responseCode

indicating the value NOT EQUAL to 0

and not containing certificate

	Variants	
nn	X_PICS	X_HASH_STRUCTURE
1	PICS_PKI_AUTH_POP=TRUE	EtsiTs103097Data-Signed
2	PICS_PKI_AUTH_POP=FALSE	EtsiTs102941Data

FP Id   SECPKI_AA_AUTH_RCV_08_BI	
Send a correctly encoded AT request, but the ITS-Station is not enrolled at the EA	
ETSI TS 102 941 [1], clause 6.2.3.3.1	
CFG_AUTH_AA	
PICS_PKI_AUTH_POP=TRUE	
Expected behaviour	
state	
certificate CERT_AA	
yptionKey (AA_ENC_PUB_KEY)	
the AuthorizationRequest message	
gnature	
Signer	
g an unknown EC hashedId8 value	
ot send the AuthorizationValidationRequest message	
to the TS the AuthorizationResponse message	
containing authorizationResponse	
containing responseCode	
indicating the value 'unknownits'	

TP Id	SECPKI_AA_AUTH_RCV_09_BI	
Summary	Send an AT request, but the inner signer (valid EC) is not issued by the EA which is known	
	trusted by the AA. The AA trusts only EAs listed on the RCA-CTL	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_AA	
PICS Selection	PICS_PKI_AUTH_POP=TRUE	
	Expected behaviour	
with		
the AA in 'operation	nal' state	
authorized with	authorized with the certificate CERT_AA	
containing e	containing encryptionKey (AA_ENC_PUB_KEY)	
ensure that		
when		
the IUT is received the AuthorizationRequest message		
containing SharedAtRequest		
containi	ng eald	
indic	eating an unknown value	
then		

and the IUT does not send the AuthorizationValidationRequest message and the IUT sends to the TS the AuthorizationResponse message containing authorizationResponse containing responseCode indicating the value 'its-aa-unknownea' and not containing certificate

TP Id	SECPKI_AA_AUTH_RCV_10_BI
Summary	Send an AT request, but the generation time of the POP signature of the CSR is in the
	past
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS_PKI_AUTH_POP=TRUE
	Expected behaviour
with	
the AA in 'operational' state	
authorized with the certificate CERT_AA	
containing encryptionKey (AA_ENC_PUB_KEY)	

ensure that

when

the IUT is received the AuthorizationRequest message containing POP signature containing tbsData containing generationTime indicating a value in the past

then

and the IUT does not send the AuthorizationValidationRequest message and the IUT sends to the TS the AuthorizationResponse message containing authorizationResponse containing responseCode indicating the value 'its-aa-outofsyncrequest' and not containing certificate

TP Id	SECPKI_AA_AUTH_RCV_11_BI
Summary	Send an AT request, but the generation time of the POP signature of the CSR is in the
	future
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS_PKI_AUTH_POP=TRUE
Expected behaviour	

with

the AA in 'operational' state

authorized with the certificate CERT\_AA

containing encryptionKey (AA\_ENC\_PUB\_KEY)

ensure that

when

the IUT is received the AuthorizationRequest message

containing POP signature containing tbsData

containing tostata

containing generationTime

indicating a value in the past

then

and the IUT does not send the AuthorizationValidationRequest message

and the IUT sends to the TS the AuthorizationResponse message

containing authorizationResponse

containing responseCode

indicating the value 'its-aa-outofsyncrequest'

and not containing certificate

TP Id	SECPKI_AA_AUTH_RCV_12_BI
Summary	Send an AT request, but the expiry date of the CSR is before the start date of the EC
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS_PKI_AUTH_POP=TRUE
Expected behaviour	

#### with

the AA in 'operational' state

authorized with the certificate CERT\_AA

containing encryptionKey (AA\_ENC\_PUB\_KEY)

ensure that

when

the IUT is received the AuthorizationRequest message

containing SharedAtRequest

containing requested Subjec Attributes

containing ValidityPeriod

indicating a value less than the start date of the EC

then

and the IUT does not send the AuthorizationValidationRequest message

and the IUT sends to the TS the Authorization Response message  $\,$ 

 $containing \ authorization Response$ 

containing responseCode

indicating the value 'deniedpermissions'

TP ld	SECPKI_AA_AUTH_RCV_13_BI
Summary	Send an AT request, but the start date of the CSR is before the start date of the EC
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS_PKI_AUTH_POP=TRUE

#### **Expected behaviour**

with

the AA in 'operational' state

authorized with the certificate CERT\_AA

containing encryptionKey (AA\_ENC\_PUB\_KEY)

ensure that

when

the IUT is received the AuthorizationRequest message

containing SharedAtRequest

containing requestedSubjecAttributes

containing ValidityPeriod

containing start date

indicating a value less than the start date of the EC

then

and the IUT does not send the AuthorizationValidationRequest message

and the IUT sends to the TS the AuthorizationResponse message

containing authorizationResponse

containing responseCode

indicating the value 'deniedpermissions'

and not containing certificate

TP ld	SECPKI_AA_AUTH_RCV_14_BI
Summary	Send an AT request, but the expiry date of the CSR is after the expiry date of the EC
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS_PKI_AUTH_POP=TRUE
Expected behaviour	

#### with

the AA in 'operational' state

authorized with the certificate CERT\_AA

containing encryptionKey (AA\_ENC\_PUB\_KEY)

ensure that

when

the IUT is received the AuthorizationRequest message

containing SharedAtRequest

containing requested Subjec Attributes

containing ValidityPeriod

indicating a value greater than the ValidityPeriod of the EC

then

and the IUT does not send the AuthorizationValidationRequest message

and the IUT sends to the TS the Authorization Response message  $\,$ 

containing authorizationResponse

containing responseCode

indicating the value 'deniedpermissions'

TP Id	SECPKI_AA_AUTH_RCV_15_BI
Summary	Send an AT request, but the start date of the CSR is after the expiring date of the EC
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS_PKI_AUTH_POP=TRUE
Expected behaviour	
with	

the AA in 'operational' state

authorized with the certificate CERT\_AA

containing encryptionKey (AA\_ENC\_PUB\_KEY)

ensure that

when

the IUT is received the AuthorizationRequest message

containing SharedAtRequest

containing requestedSubjecAttributes

containing ValidityPeriod

containing start date

indicating a value greater than the start date of the EC

and the IUT does not send the AuthorizationValidationRequest message

and the IUT sends to the TS the AuthorizationResponse message

containing authorizationResponse

containing responseCode

indicating the value 'deniedpermissions'

and not containing certificate

Expected behaviour	
PICS Selection	PICS_PKI_AUTH_POP=TRUE
Configuration	CFG_AUTH_AA
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Summary	SSend an AT request, but the expiry date of the CSR is after now + maximum preloading period (considering values in C-ITS CP)
TP Id	SECPKI_AA_AUTH_RCV_16_BI

#### with

the AA in 'operational' state

authorized with the certificate CERT\_AA

containing encryptionKey (AA\_ENC\_PUB\_KEY)

ensure that

when

the IUT is received the AuthorizationRequest message

containing SharedAtRequest

containing requestedSubjecAttributes

containing ValidityPeriod

containing start date

indicating the current date

and a duration

indication 100 years

and the IUT does not send the AuthorizationValidationRequest message

and the IUT sends to the TS the AuthorizationResponse message

containing authorizationResponse

containing responseCode

indicating the value 'deniedpermissions'

TP Id	SECPKI_AA_AUTH_RCV_17_BV		
Summary	Check that AA send the same response for the repeated AT request		
Reference	ETSI TS 103 601 [6], clause 5.1		
Configuration	CFG_ENR_AA		
PICS Selection	PICS_SECPKI_AUTHORIZATION_RETRY		
	Expected behaviour		
with			
the AA is in 'operational'	state		
and the AA already rece	vived AuthorizationRequestMessage ( <i>REQ</i> )		
having checksum (C	having checksum (CS)		
and the AA has sent the AuthorizationResponseMessage (RES)			
containing response	containing responseCode		
indicating OK			
ensure that			
when			
the IUT receives an AuthorizationRequestMessage			
having checksum			
indicating value equal to <b>CS</b>			
then			
the IUT answers with an AuthorizationResponseMessage			
indicating <b>RES</b>			

TP ld	SECPKI_AA_AUTH_RCV_18_BV
Summary	Check that AA does not accept authorization requests when message generation time is
	too far in the past
Reference	ETSI TS 103 601 [6], clause 5.1.4
Configuration	CFG ENR AA
PICS Selection	PICS_SECPKI_AUTHORIZATION_RETRY
	Expected behaviour
with	·
the EA is in 'opera	ational' state
and the AA alread	dy received the AuthorizationRequestMessage ( <i>REQ</i> )
	nerationTime <b>TG</b>
and having ch	
ensure that	** ** <b>*</b> ***
when	
the IUT receiv	es an AuthorizationRequestMessage
at the mon	· ·
indicati	ng TR2 > TG + PIXIT_AA_AUTH_TIMEOUT
and having	gichecksum
indicating value equal to <b>CS</b>	
then	
the IUT answe	ers with an AuthorizationResponseMessage
containing responseCode	
indicati	ng deniedrequest
NOTE: PIXIT_AA	AUTH_TIMEOUT shall be set as a TP parameter.

# 5.5.2 Authorization validation request

TDII	OFORK AA AUTUVAL OF BY	
TP ld	SECPKI_AA_AUTHVAL_01_BV	
Summary	Check that the AA sends AuthorizationValidationRequest after receiving of the	
	AuthorizationRequest	
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1	
Configuration	CFG_AUTH_AA	
PICS Selection		
	Expected behaviour	
with		
the EA in 'operational' st	ate	
authorized with CERT_EA certificate		
ensure that		
when		
	the IUT received the AuthorizationRequest	
containing EtsiTs		
•	ntent.authorizationRequest	
containing sharedAtRequest		
containing eald (EA_ID)		
indicating HashedId8 of the CERT_EA		
then		
and the IUT sends the EtsiTs103097Data message		
to the EA identified by EA_ID		

TP Id	SECPKI AA AUTHVAL 02 BV		
IFIU			
	Check that the AuthorizationValidationRequest message is encrypted using approved		
	algorithm and sent to only one Enrolment Authority		
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1		
Configuration	CFG_AUTH_ITSS		
PICS Selection			
	Expected behaviour		
with			
the EA in 'operational' st	ate		
authorized with CER	T_EA certificate		
ensure that			
when			
the IUT is triggered to send the AuthorizationValidationRequest to the EA			
then			
the IUT sends a Etsi	the IUT sends a EtsiTs103097Data		
containing content.encryptedData.recipients			
	indicating size 1		
	and containing the instance of RecipientInfo		
	containing certRecipInfo		
containing recipientId			
indicating HashedId8 of the CERT_EA			
	and containing encKey		
containing eciesNistP256			
Or	containing eciesBrainpoolP256r1		

TD L-I	OFODIAL AA ALITHIAAL OO DA	
TP ld	SECPKI_AA_AUTHVAL_03_BV	
Summary	Check that the AA sends AuthorizationValidationRequest signed by AA	
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1	
Configuration	CFG_AUTH_AA	
PICS Selection		
	Expected behaviour	
with		
the AA in 'operational' st	ate	
authorized with CER	T AA certificate	
and the EA in 'operational' state		
ensure that		
when		
the IUT is triggered to send the AuthorizationValidationRequest to the EA		
then		
the IUT sends a EtsiTs103097Data-Encrypted message		
containing EtsiTs103097Data-Signed		
containing signedData		
containing signer		
containing digest		
IIIu	icating HashedId8 value of the CERT_AA	

I			
TP ld	SECPKI_AA_AUTHVAL_04_BV		
Summary	Check that the AA sends signed AuthorizationValidationRequest with signature properly		
	calculated using approved hash algorithm		
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1		
Configuration	CFG_AUTH_AA		
PICS Selection			
	Expected behaviour		
with			
the AA in 'operational' st	ate		
authorized with CER	T_AA certificate		
containing verific	ationKey (AA_PUB_V_KEY)		
and the EA in 'operation	and the EA in 'operational' state		
authorized with CERT_EA certificate			
ensure that			
when			
the IUT is triggered to send the AuthorizationValidationRequest to the EA			
then			
the IUT sends a Etsi	Ts103097Data-Encrypted message		
containing EtsiTs103097Data-Signed			
containing signedData			
containing hashld			
_	indicating supported hash algorytm (HASH_ALG)		
	ining signature		
	ated using the HASH_ALG and private key correspondent to the AA_PUB_V_KEY		

TP Id	SECPKI_AA_AUTHVAL_05_BV		
Summary	Check that the AA sends signed AuthorizationValidationRequest using proper signed data		
	headers		
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1		
Configuration	CFG_AUTH_AA		
PICS Selection			
	Expected behaviour		
with			
the AA in 'operational' st	ate		
authorized with CER	<del>-</del>		
	containing verificationKey (AA_PUB_V_KEY)		
	and the EA in 'operational' state		
authorized with CER	T_EA certificate		
ensure that			
when	Id. A.d. C. A.P.I.C. B d. EA		
	o send the AuthorizationValidationRequest to the EA		
then	To102007Data Engrunted massage		
the IUT sends a EtsiTs103097Data-Encrypted message			
containing EtsiTs103097Data-Signed containing signedData			
containing signedData  containing tbsData			
containing tost at a containing headerInfo			
containing reddorning containing psid			
	indicating AID_PKI_CERT_REQUEST		
and	d containing generationTime		
	and not containing any other headers		

TP Id	SECPKI_AA_AUTHVAL_06_BV	
Summary	Check that the AA sends AuthorizationValidationRequest version 1	
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1	
Configuration	CFG_AUTH_AA	
PICS Selection		
	Expected behaviour	
with		
the EA in 'operational' s	tate	
ensure that	ensure that	
when	when	
the IUT is triggered to send the AuthorizationValidationRequest to the EA		
then		
the IUT sends a EtsiTs103097Data-Encrypted message		
containing EtsiTs102941Data		
containing version		
indicating 1		

Expected behaviour	
PICS Selection	
Configuration	CFG_AUTH_AA
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1
Summary	Check that the AA sends AuthorizationValidationRequest with sharedAtRequest and ecSignature as it was requested in the triggering AuthorizationRequest
TP ld	SECPKI_AA_AUTHVAL_07_BV

with
the AA in 'operational' state
and the EA in 'operational' state
ensure that
when
the IUT received the AuthorizationRequest
containing EtsiTs102941Data
containing content.authorizationRequest
containing sharedAtRequest (SHARED\_AT\_REQUEST)
and containing ecSignature (EC\_SIGNATURE)
then
the IUT sends a EtsiTs103097Data-Encrypted message

e IUT sends a EtsiTs103097Data-Encrypted message containing EtsiTs102941Data containing content.authorizationValidationRequest containing sharedAtRequest indicating SHARED\_AT\_REQUEST and containing ecSignature indicating EC\_SIGNATURE

TP Id	SECPKI_AA_AUTHVAL_08_BV
Summary	Check that signing of Authorization Validation request message is permitted by the AA
	certificate
Reference	ETSI TS 102 941 [1], clause B.5
Configuration	CFG_AUTH_AA
PICS Selection	
Expected helpovious	

#### Expected behaviour

with

the AA in 'operational' state and the EA in 'operational' state

ensure that

when

the IUT is triggered to send the AuthorizationValidationRequest to the EAthen

the IUT sends an EtsiTs103097Data-SignedAndEncrypted structure containing signer

declared as a digest

containing the HashedId8 of the AA certificate containing appPermissions

containing an item of type PsidSsp containing psid indicating AID\_CERT\_REQ

and containing ssp

containing opaque[0] (version)

indicating 1

containing opaque[1] (value)

indicating 'Enrolment Request' (bit 1) set to 1

# 5.5.3 Authorization validation response handling

TP Id	SECPKI AA AUTHVAL RCV 01 BV
Summary	Check that the AA sends AuthorizationResponse after receiving the AuthorizationRequest
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
and the IUT sent the Au ensure that when the IUT received the then	tate

TP ld	SECPKI_AA_AUTHVAL_RCV_02_BI
Summary	Check that AA does not accept Authorization Validation Response message when this
Summary	message is signed with certificate without appropriate permissions
Reference	ETSI TS 102 941 [1], clause B.5
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with	
the ITSS in 'enrolled' sta	te
the EA in 'operational' st	ate
and the IUT(AA) in 'oper	
	d the AuthorizationRequest from the ITSS
	thorizationValidationRequest
ensure that	
when	
the IUT receives the AuthorizationValidationResponseMessage	
containing signer	.1
containing diges	
indicating HashedId8 of the certificate containing appPermissions	
	aining an item of type PsidSsp iining psid
	dicating AID_CERT_REQ
	ntaining an item of type PsidSsp
	ntaining psid
1	indicating AID_CERT_REQ
an	d containing ssp
	containing opaque[0] (version)
	indicating other value than 1
	or containing opaque[1] (value)
	indicating 'AuthorizationValidationResponse' (bit 4) set to 0
then	
	an AuthorizationValidationResponseMessage
containing respons	
indicating non-z	ero value

### 5.5.4 Authorization response

TP Id	SECPKI_AA_AUTH_01_BV
Summary	Check that the AA sends encrypted AuthorizationResponse
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
Configuration	CFG_AUTH_AA
PICS Selection	
Expected behaviour	

```
with
the ITSS in 'enrolled' state
has sent the AuthorizationRequestMessage
containing encrypted enkKey
containing AES symmetric key (SYM_KEY)
the EA in 'operational' state
ensure that
when
the IUT is triggered to send the authorization response to the ITSS
```

then
the IUT sends the EtsiTs103097Data-Encrypted message

the IUT sends the EtsiTs103097Data-Encrypted message containing content.encryptedData containing recipients of size 1 containing the instance of RecipientInfo containing pskRecipInfo

indicating HashedId8 of the SYM\_KEY and containing cyphertext encrypted using SYM\_KEY

TP Id	SECPKI_AA_AUTH_02_BV
Summary	Check that the AA sends signed AuthorizationResponse
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
Configuration	CFG_AUTH_AA
PICS Selection	

#### **Expected behaviour**

#### with

```
the ITSS in 'enrolled' state
and the IUT(AA) in 'operational' state
authorized with CERT_AA certificate
and the EA in 'operational' state
ensure that
when
the IUT is triggered to send the authorization response to the ITSS
then
the IUT sends the EtsiTs103097Data-Encrypted message
containing the EtsiTs103097Data-Signed
containing signedData
```

containing signer containing digest

indicating HashedId8 value of the CERT\_AA

	T	
TP ld	SECPKI_AA_AUTH_03_BV	
Summary	Check that the AA sends signed AuthorizationResponse with signature properly calculated	
	using approved hash algorithm	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2	
Configuration	CFG_AUTH_AA	
PICS Selection		
	Expected behaviour	
with		
the ITSS in 'enrolled' sta	ate	
and the IUT(AA) in 'oper	rational' state	
authorized with CER	T_AA certificate	
containing verificationKey (AA_PUB_V_KEY)		
and the EA in 'operational' state		
ensure that		
when		
the IUT is triggered to send the authorization response to the ITSS		
then		
and the IUT sends th	ne EtsiTs103097Data-Encrypted message	
containing the Et	siTs103097Data-Signed	
containing sig	gnedData	
containing	g hashld	
	indicating supported hash algorytm (HASH_ALG)	
and conta	ining signature	
calcula	ated using the HASH_ALG and private key correspondent to the AA_PUB_V_KEY	

TP ld	SECPKI_AA_AUTH_04_BV
Summary	Check that the AA sends signed AuthorizationResponse with signature properly calculated
	using approved hash algorithm
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with	
the ITSS in 'enrolled	J' state
and the IUT(AA) in '	operational' state
and the EA in 'opera	ational' state
ensure that	
when	
	red to send the authorization response to the ITSS
then	
	EtsiTs103097Data-Encrypted message
	tsiTs103097Data-Signed
	g signedData
	ining tbsData
co	ontaining headerInfo
	containing psid
	indicating AID_PKI_CERT_REQUEST
	and containing generationTime
	and not containing any other headers

TP Id	SECPKI_AA_AUTH_05_BV	
ISHIMMARV	Check that the AA sends signed AuthorizationResponse with signature properly calculated	
	using approved hash algorithm	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2	
Configuration	CFG_AUTH_AA	
PICS Selection	X_PICS	

#### **Expected behaviour**

with

the ITSS in 'enrolled' state

has sent the AuthorizationRequestMessage containing EtsiTs102941Data containing authorizationResponse containing X\_DATA\_STRUCTURE

and the IUT(AA) in 'operational' state and the EA in 'operational' state

ensure that

when

the IUT is triggered to send the authorization response to the ITSS

then

the IUT sends a EtsiTs103097Data-Encrypted message containing EtsiTs103097Data-Signed containing EtsiTs102941Data

containing authorizationResponse containing requestHash

indicating the leftmost 16 bits of the SHA256 value calculated over the **X\_DATA\_STRUCTURE** 

and containing responseCode

	variants	
nn	X_PICS	X_DATA_STRUCTURE
1	PICS_PKI_AUTH_POP=TRUE	EtsiTs103097Data-Signed
2	PICS_PKI_AUTH_POP=FALSE	EtsiTs102941Data

SECPKI_AA_AUTH_06_BV
Check that the AA includes the certificate in the positive AuthorizationResponse
ETSI TS 102 941 [1], clause 6.2.3.3.2
CFG_AUTH_AA
Expected behaviour
ate
izationRequestMessage
erational' state

and the EA in 'operational' state ensure that

when

the IUT is sending to the ITSS the AuthorizationResponseMessage (MSG)

containing responseCode

indicating 0

then

the message MSG containing certificate

TP Id	SECPKI_AA_AUTH_07_BV	
Summary	Check that the AA does not include the certificate in the negative AuthorizationResponse	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2	
Configuration	CFG_AUTH_AA	
PICS Selection		
	Expected behaviour	
with		
the ITSS in 'enrolled' sta	ate	
has sent the Authoriz	zationRequestMessage	
and the IUT(AA) in 'oper	and the IUT(AA) in 'operational' state	
and the EA in 'operational' state		
ensure that		
when		
the IUT is sending to	the IUT is sending to the ITSS the AuthorizationResponseMessage (MSG)	
containing responseCode		
indicating neg	gative value	
then		
the message MSG		
not containing ce	ertificate	

TP ld	SECPKI_AA_AUTH_08_BV
Summary	Check that signing of Authorization response message is permitted by the AA certificate
Reference	ETSI TS 102 941 [1], clause B.5
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT sends an Au	thorizationResponseMessage as an answer for an AuthorizationRequestMessage
then	
the IUT sends an Ets	siTs103097Data-SignedAndEncrypted structure
containing signer	
declared as a di	gest
	e HashedId8 of the AA certificate
containing	appPermissions
	ng an item of type PsidSsp
	nining psid
	dicating AID_CERT_REQ
	containing ssp
СО	ntaining opaque[0] (version)
	indicating 1
со	ntaining opaque[1] (value)
	indicating 'Authorization Response' (bit 3) set to 1

# 5.5.5 CA Certificate Request

TP ld	SECPKI_AA_CERTGEN_01_BV
<b>6</b>	SubCA certificate requests of the AA are transported to the RCA using
Summary	CACertificateRequest messages across the reference point S9
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_INIT
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT is reque	ested to send a CACertificateRequestMessage
then	·
the IUT sends a	ı CACertificateRequestMessage
	eference point S9 to the RCA

TP ld	SECPKI_AA_CERTGEN_02_BV		
Summary	The application form should include the digital fingerprint of the CACertificateRequestMessage in printable format. The digital fingerprint of the		
	CACertificateRequestMessage is computed using a ETSLTS 103 097 [2] approved hash		
	algorithm		
Reference	ETSI TS 102 941 [1], clause 6.2.1		
	ETSI TS 103 097 [2], clause 7		
Configuration	CFG_CAGEN_INIT		
PICS Selection			
	Expected behaviour		
with			
the IUT being in the 'initial' state			
ensure that			
when			
the IUT is requested to send a CACertificateRequestMessage			
then			
the IUT sends a CACertificateRequestMessage containing a signature (SIG)			
being computed using a ETSI TS 103 097 [2] approved hash algorithm and the IUT exports the digital fingerprint (SIG) in a printable format.			

TDU	DEODIG AA OFFICEN OO DY	
TP ld	SECPKI_AA_CERTGEN_03_BV	
	The hashId shall indicate the hash algorithm to be used as specified in ETSI	
Summary	TS 103 097 [2], the signer is set to 'self' and the signature over the tbsData is computed	
Canimal y	using the private key corresponding to the new verificationKey to be certified (i.e. the	
	request is self-signed)	
Reference	ETSI TS 102 941 [1], clause 6.2.1	
Keieieiice	ETSI TS 103 097 [2], clause 7	
Configuration	CFG_CAGEN_INIT	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the 'ini	itial' state	
ensure that		
when		
the IUT is requested to send a CACertificateRequestMessage		
then		
the IUT sends a CACertificateRequestMessage		
being an EtsiTs103097Data-Signed structure		
containing hashld		
indicating the hash algorithm to be used		
and containing signer		
indicating 'self'		
and containing tbsData		
containing CaCertificateRequest		
containing publicKeys		
containing verification_key (VKEY)		
and containing signature		
computed of	over tbsData using the private key corresponding to the verificationKey (VKEY)	

TP Id	SECPKI_AA_CERTGEN_04_BV	
Summary	An ECC private key is randomly generated, the corresponding public key (verificationKey) is provided to be included in the CaCertificateRequest.  An ECC encryption private key is randomly generated, the corresponding public key (encryptionKey) is provided to be included in the CACertificateRequest.  CaCertificateRequest.publicKeys shall contain verification_key and encryption_key	
Reference	ETSI TS 102 941 [1], clause 6.2.1	
Configuration	CFG_CAGEN_INIT	
PICS Selection		
	Expected behaviour	
with the IUT being in the 'ir ensure that when	nitial' state	
the IUT is requested to send a CACertificateRequestMessage		
then		
the IUT sends a CACertificateRequestMessage containing CaCertificateRequest containing publicKeys containing verification_key		
and contai	and containing encryption_key	

TP Id	SECPKI_AA_CERTGEN_05_BV		
Summary	The EtsiTs102941Data structure is built with version set to v1 (integer value set to 1).		
Reference	ETSI TS 102 941 [1], clause 6.2.1		
Configuration	CFG_CAGEN_INIT		
PICS Selection			
	Expected behaviour		
with			
the IUT being in the 'initi	al' state		
ensure that			
when	when		
the IUT is requested to send a CACertificateRequestMessage			
then			
the IUT sends a CACertificateRequestMessage			
containing EtsiTs102941Data			
containing version			
indicating v1 (integer value set to 1)			

TP ld	SECPKI_AA_CERTGEN_06_BV	
Summary	CaCertificateRequest.requestedSubjectAttributes shall contain the requested certificates attributes as specified in ETSI TS 103 097 [2] clause 7.2.4	
Reference	ETSI TS 102 941 [1], clause 6.2.1	
	ETSI TS 103 097 [2], clause 7.2.4	
Configuration	CFG_CAGEN_INIT	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the	e 'initial' state	
ensure that		
when		
the IUT is reque	ested to send a CACertificateRequestMessage	
then	·	
the IUT sends a CACertificateRequestMessage		
containing CaCertificateReguest		
containing requestedSubjectAttributes		
as specified in ETSI TS 103 097 [2], clause 7.2.4.		

TP Id	SECPKI_AA_CERTGEN_07_BV	
Summary	EtsiTs103097Data-Signed.tbsData contains the EtsiTs102941Data as payload and the headerInfo containing psid and generationTime. The psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [i.2] and the generationTime shall be present. All other components of the component tbsdata.headerInfo are not used and absent	
Reference	ETSI TS 102 941 [1], clause 6.2.1	
Configuration	CFG_CAGEN_INIT	
PICS Selection		
	Expected behaviour	
with the IUT being in the 'initial' state ensure that when the IUT is requested to send a CACertificateRequestMessage then		
the IUT sends a CACertificateRequestMessage containing headerInfo containing psid indicating SEC_CERT_REQ and containing generationTime and not containing any other component of tbsdata.headerInfo		

TP ld	SECPKI_AA_CERTGEN_08_BV
Summary	If the current private key has reached its end of validity period or is revoked, the SubCA
	shall restart the initial certificate application process
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_REKEY
PICS Selection	
	Expected behaviour
with	•
the IUT being in th	e 'operational' state
ensure that	
when	
the IUT is requ	ested to send a CACertificateRekeyingMessage
and SubCA certificate is no longer valid (due to end of validity or revocation)	
then	,
the IUT switche	es to the "initial" state
and sends a Co	A Certificate Request Message

TP ld	SECPKI_AA_CERTGEN_09_BV
Summary	For the re-keying application to the RCA (CaCertificateRekeyingMessage), an EtsiTs103097Data-Signed structure is built, containing: hashId, tbsData, signer and signature. The hashId shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [2]. The signer declared as a digest, containing the hashedId8 AA certificate and the signature over tbsData is computed using the currently valid private key corresponding to the AA certificate (outer signature)
Reference	ETSI TS 102 941 [1], clause 6.2.1 ETSI TS 103 097 [2], clause 7
Configuration	CFG_CAGEN_REKEY
PICS Selection	
	Expected behaviour
with the IUT being in the 'operational' state ensure that when the IUT is requested to send a CACertificateRekeyingMessage then the sends a CACertificateRekeyingMessage being an EtsiTs103097Data-Signed structure containing hashId indicating the hash algorithm to be used and containing tbsData and containing signer declared as digest indicating the hashedId8 of the SubCA certificate (CERT) and containing signature computed over tbsData	

TP ld	SECPKI_AA_CERTGEN_10_BV
Summary	The (outer) tbsData of the CACertificateRekeyingMessage shall contain the
	CaCertificateRequestMessage as payload
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_REKEY
PICS Selection	
Expected behaviour	<u> </u>
with	
the IUT being in the	e 'operational' state
ensure that	
when	
the IUT is reque	ested to send a CACertificateRekeyingMessage
then	
the sends a CACertificateRekeyingMessage	
containing tbsData	
containing CaCertificateRequestMessage	

TP Id	SECPKI_AA_CERTGEN_11_BV	
i Fiu		
	The (outer) tbsData of the CACertificateRekeyingMessage shall contain a	
	headerInfo containing psid and generationTime. The psid shall be set to "secured	
Summary	certificate request" as assigned in ETSI TS 102 965 [i.2] and the generationTime shall be	
-	present. All other components of the component tbsdata.headerInfo are not used and	
	absent	
Reference	ETSI TS 102 941 [1], clause 6.2.1	
Configuration	CFG_CAGEN_REKEY	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the 'ope	erational' state	
ensure that		
when		
the IUT is requested to send a CACertificateRekeyingMessage		
then		
the sends a CACertificateRekeyingMessage		
containing tbsData		
containing headerInfo		
containing psid		
indicating SEC CERT REQ		
and containing generationTime		
	sining any other component of tbsdata.headerInfo	

T		
TP ld	SECPKI_AA_CERTGEN_12_BV	
Summary	Check that the CaCertificateRekeyingMessage is permitted by AA certificate	
Reference	ETSI TS 102 941 [1], clause 6.2.1	
Configuration	CFG_CAGEN_REKEY	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the 'ope	erational' state	
ensure that		
when		
•	to send a CACertificateRekeyingMessage	
then		
	ficateRekeyingMessage	
being an EtsiTs103097Data-Signed structure		
and containing the		
and containin		
containing dig	lashedId8 of the AA certificate	
containing appPermissions containing an item of type PsidSsp		
containing an item of type Fsidosp containing psid		
	indicating AID_CERT_REQ	
and containing ssp		
containing opportunity opportu		
	indicating 1	
c	containing opaque[1] (value)	
indicating 'CA Certificate Response' (bit 6) set to 1		

## 5.6 RootCA behaviour

### 5.6.0 Overview

All test purposes in the present clause may be included in the test sequence if the following PICS items is set:

```
PICS\_SECPKI\_IUT\_RCA = TRUE
```

## 5.6.1 CTL generation

For the scope of test purposes of this clause, the EtsiTs103097Data and EtsiTs102941Data envelopes are already removed from the analysing messages if it is not explicitly specified in the test purpose.

TP ld	SECPKI_RCA_CTLGEN_01_BV	
Summary	Check that the RootCA generates the Full CTL when new EA is about to be added to the	
	Root CTL	
Reference	ETSI TS 102 941 [1], clauses 6.3.2 and 6.3.4	
Configuration	CFG_CTLGEN_RCA	
PICS Selection		
	Expected behaviour	
ensure that		
when		
the RootCA is trigge	red to add new EA certificate (CERT_EA) in the CTL	
then		
the IUT issue a new CTL of type CtlFormat		
containing isFullCtl		
indicating TRUE		
and containing ctlCommands		
containing CtlCommand		
containing add		
containing ea		
containing eaCertificate		
indicating CERT_EA		

TP Id	SECPKI_RCA_CTLGEN_02_BV		
Summary	Check that the RootCA generates the Delta CTL when new EA is about to be added to the Root CTL		
Reference	ETSI TS 102 941 [1], clauses 6.3.2 and 6.3.4		
Configuration	CFG_CTLGEN_RCA		
PICS Selection			
Expected behaviour			
ensure that			
when			
the RootCA is triggered to add new EA certificate (CERT_EA) in the CTL			
then	then		
the IUT issue a new	CTL of type CtlFormat		
containing isFullC	containing isFullCtl		
indicating FALSE			
and containing ctlCommands			
containing CtlCommand			
containing add			
containing ea			
containing eaCertificate			
	indicating CERT_EA		

TP Id	SECPKI RCA CTLGEN 03 BV		
Summary	Check that the RootCA generates the Full CTL when EA certificate is about to be deleted		
Reference	ETSI TS 102 941 [1], clauses 6.3.2 and 6.3.4		
Configuration	CFG_CTLGEN_RCA		
PICS Selection			
Expected behaviour			
ensure that			
when			
the RootCA is triggered to delete EA certificate (CERT_EA) from the CTL			
then			
the IUT issue a new CTL of type CtlFormat			
containing isFullC	containing isFullCtl		
indicating TRUE			
and containing ctlCommands			
not containing CtlCommand			
containing add			
containing ea			
containing eaCertificate			
indicating CERT_EA			

TP ld	SECPKI_RCA_CTLGEN_04_BV		
Summary	Check that the RootCA generates the Delta CTL when EA certificate is about to be deleted		
Reference	ETSI TS 102 941 [1], clauses 6.3.2 and 6.3.4		
Configuration	CFG_CTLGEN_RCA		
PICS Selection			
Expected behaviour			
ensure that			
when			
the RootCA is triggered to delete EA certificate (CERT_EA) from the CTL			
then			
the IUT issue a new CTL of type CtlFormat			
containing isFullCtl			
indicating FALSE			
and containing ctlCommands			
not containing CtlCommand			
containing delete			
containing cert			
inc	dicating Hashedid8 of CERT_EA		

Summary  Check that the RootCA generates the Full CTL when EA access point is about to be changed  Reference ETSI TS 102 941 [1], clause 6.3.2  Configuration CFG_CTLGEN_RCA  PICS Selection  Expected behaviour	TP Id	SECPKI_RCA_CTLGEN_05_BV				
Reference ETSLTS 102 941 [1], clause 6.3.2  Configuration CFG_CTLGEN_RCA  PICS Selection  Expected behaviour  ensure that when the RootCA is triggered to add new EA access point URL (URL) to the CTL then the IUT issue a new CTL of type CtlFormat containing isFullCtl indicating TRUE containing ctlCommands containing ctlCommand containing add containing add containing ea containing eaCertificate (CERT_EA) and containing any other CtlCommand containing add containing ea containing ea	Summary					
Reference ETSI TS 102 941 [1], clause 6.3.2  Configuration CFG_CTLGEN_RCA  PICS Selection  Expected behaviour  ensure that when the RootCA is triggered to add new EA access point URL (URL) to the CTL then the IUT issue a new CTL of type CtlFormat containing isFullCtl indicating TRUE containing ctlCommands containing ctlCommand containing add containing add containing add containing add containing dea containing tisAccessPoint indicating URL and NOT containing any other CtlCommand containing add containing add containing add containing any other CtlCommand containing add containing any other CtlCommand containing add containing add containing any other CtlCommand containing add containing add containing ea containing eacertificate		·				
CFG_CTLGEN_RCA  PICS Selection  Expected behaviour  ensure that when the RootCA is triggered to add new EA access point URL (URL) to the CTL then the IUT issue a new CTL of type CtlFormat containing isFullCtl indicating TRUE containing ctlCommands containing ctlCommand containing add containing add containing ea  containing isAccessPoint indicating URL and NOT containing any other CtlCommand containing add containing add containing add containing uRL and NOT containing any other CtlCommand containing add containing ea containing ea						
ensure that when the RootCA is triggered to add new EA access point URL (URL) to the CTL then the IUT issue a new CTL of type CtlFormat containing isFullCtl indicating TRUE containing ctlCommands containing CtlCommand containing add containing ea containing eaCertificate (CERT_EA) and containing itsAccessPoint indicating URL and NOT containing any other CtlCommand containing add containing add containing add containing add containing any contered to the containing and the containing and containing and containing and containing ea containing ea						
ensure that when the RootCA is triggered to add new EA access point URL (URL) to the CTL then the IUT issue a new CTL of type CtlFormat containing isFullCtl indicating TRUE containing ctlCommands containing CtlCommand containing add containing ea containing eaCertificate (CERT_EA) and containing isAccessPoint indicating URL and NOT containing any other CtlCommand containing add containing add containing add containing any other CtlCommand containing add containing add containing add containing add containing add containing add containing ad containing ad		CFG_CTLGEN_RCA				
ensure that when the RootCA is triggered to add new EA access point URL (URL) to the CTL then the IUT issue a new CTL of type CtlFormat containing isFullCtl indicating TRUE containing ctlCommands containing CtlCommand containing add containing ea containing eaCertificate (CERT_EA) and containing itsAccessPoint indicating URL and NOT containing any other CtlCommand containing add containing ea containing ea containing ea containing add containing ea containing ea	PICS Selection					
when the RootCA is triggered to add new EA access point URL (URL) to the CTL then the IUT issue a new CTL of type CtlFormat containing isFullCtl indicating TRUE containing ctlCommands containing CtlCommand containing add containing ea containing ea containing eaCertificate (CERT_EA) and containing itsAccessPoint indicating URL and NOT containing any other CtlCommand containing add containing add containing ea containing ea		Expected behaviour				
the RootCA is triggered to add new EA access point URL (URL) to the CTL then the IUT issue a new CTL of type CtlFormat containing isFullCtl indicating TRUE containing ctlCommands containing CtlCommand containing add containing ea containing ea containing eaCertificate (CERT_EA) and containing itsAccessPoint indicating URL and NOT containing any other CtlCommand containing add containing add containing ea containing ea	ensure that					
then the IUT issue a new CTL of type CtlFormat containing isFullCtl indicating TRUE containing ctlCommands containing add containing ea containing ea containing itsAccessPoint indicating URL and NOT containing any other CtlCommand containing ea containing add containing add containing any other CtlCommand containing add containing ea containing ea	when					
then the IUT issue a new CTL of type CtlFormat containing isFullCtl indicating TRUE containing ctlCommands containing add containing ea containing ea containing itsAccessPoint indicating URL and NOT containing any other CtlCommand containing ea containing add containing add containing any other CtlCommand containing add containing ea containing ea	the RootCA is triggered to add new EA access point URL (URL) to the CTL					
containing isFullCtl indicating TRUE containing ctlCommands containing add containing ea containing eaCertificate (CERT_EA) and containing itsAccessPoint indicating URL and NOT containing any other CtlCommand containing add containing ea containing add containing ea containing ea containing ea						
indicating TRUE containing ctlCommands containing add containing ea containing ea containing itsAccessPoint indicating URL and NOT containing any other CtlCommand containing ea containing add containing add containing add containing ea containing ea containing ea	the IUT issue a new	VCTL of type CtlFormat				
indicating TRUE containing ctlCommands containing add containing ea containing ea containing itsAccessPoint indicating URL and NOT containing any other CtlCommand containing ea containing add containing add containing add containing ea containing ea containing ea	containing isFul	ICtl				
containing CtlCommand						
containing CtlCommand	containing ctlCo					
containing add	containing C					
containing eaCertificate (CERT_EA) and containing itsAccessPoint indicating URL and NOT containing any other CtlCommand containing add containing ea containing ea						
containing eaCertificate (CERT_EA) and containing itsAccessPoint indicating URL and NOT containing any other CtlCommand containing add containing ea containing ea	conta	· · · · · · · · · · · · · · · · · · ·				
and containing itsAccessPoint indicating URL and NOT containing any other CtlCommand containing add containing ea containing eaCertificate		· · · · · · · · · · · · · · · · · · ·				
indicating URL and NOT containing any other CtlCommand containing add containing ea containing eaCertificate						
and NOT containing any other CtlCommand containing add containing ea containing eaCertificate						
containing add containing ea containing eaCertificate						
containing ea containing eaCertificate						
containing eaCertificate	· · · · · · · · · · · · · · · · · · ·					

	T		
TP ld	SECPKI_RCA_CTLGEN_06_BV		
Summary	Check that the RootCA generates the Delta CTL when EA access point is about to be		
	changed		
Reference	ETSI TS 102 941 [1], clauses 6.3.2 and 6.3.4		
Configuration	CFG_CTLGEN_RCA		
PICS Selection			
Expected behaviour			
ensure that			
when			
the RootCA is trigge	red to add new EA access point URL (URL) to the CTL		
then			
the IUT issue a new	CTL of type CtlFormat		
containing isFull(	Ctl Control of the Co		
indicating FALSE			
containing ctlCommands			
containing CtlCommand			
containing add			
containing ea			
col	containing eaCertificate (CERT_EA)		
and containing itsAccessPoint			
indicating URL			

TP ld	SECPKI_RCA_CTLGEN_07_BV
II IM	Check that the RootCA generates the Full CTL when EA access point URL for AA
Summary	
<u> </u>	communication is about to be changed
Reference	ETSI TS 102 941 [1], clause 6.3.2
Configuration	CFG_CTLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	
when	
the RootCA is trigger	red to add new URL for EA-AA communication (URL) to the CTL
then	
the IUT issue a new	CTL of type CtlFormat
containing isFull0	Ctl
indicating TRUE	
containing ctlCommands	
containing Ctl	ICommand
containing add	
containing ea	
containing eaCertificate (CERT_EA)	
containing aaAccessPoint	
indicating URL	
and NOT containing any other CtlCommand	
containing add	
	ning ea
	ntaining eaCertificate
indicating CERT_EA	

TP Id	SECPKI_RCA_CTLGEN_08_BV		
Summary	Check that the RootCA generates the Delta CTL when EA access point URL for AA		
	communication is about to be changed		
Reference	ETSI TS 102 941 [1], clause 6.3.2		
Configuration	CFG_CTLGEN_RCA		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the RootCA is t	riggered to add new URL for EA-AA communication (URL) to the CTL		
then			
the IUT issue a	the IUT issue a new CTL of type CtlFormat		
containing is	containing isFullCtl		
indicating FALSE			
containing o	containing ctlCommands		
containing CtlCommand			
containing add			
containing ea			
	containing eaCertificate (CERT_EA)		
containing aaAccessPoint			
	indicating URL		

TP ld	SECPKI_RCA_CTLGEN_09_BV		
Summary	Check that the RootCA generates the Full CTL when new AA is about to be added to the		
	Root CTL		
Reference	ETSI TS 102 941 [1], clause 6.3.2		
Configuration	CFG_CTLGEN_RCA		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the RootCA is trigger	the RootCA is triggered to add new AA certificate (CERT_AA) in the CTL		
then			
the IUT issue a new	the IUT issue a new CTL of type CtlFormat		
containing isFull(	Ctl		
indicating TR			
and containing ct	and containing ctlCommands		
containing CtlCommand			
containing add			
containing aa			
containing aaCertificate			
	indicating CERT_AA		

TP Id	SECPKI_RCA_CTLGEN_10_BV		
Summary	Check that the RootCA generates the Delta CTL when new AA is about to be added to the		
	Root CTL		
Reference	ETSI TS 102 941 [1], clauses 6.3.2 and 6.3.4		
Configuration	CFG_CTLGEN_RCA		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the RootCA is trigge	the RootCA is triggered to add new AA certificate (CERT_AA) in the CTL		
then			
the IUT issue a new	the IUT issue a new CTL of type CtlFormat		
containing isFull(	Ctl Ctl		
indicating FALSE			
and containing ctlCommands			
containing CtlCommand			
containing add			
contai	containing aa		
containing aaCertificate			
	indicating CERT_AA		

TP Id	SECPKI_RCA_CTLGEN_11_BV	
Summary	Check that the RootCA generates the Full CTL when AA is about to be deleted from the Root CTL	
Reference	ETSI TS 102 941 [1], clause 6.3.2	
Configuration	CFG_CTLGEN_RCA	
PICS Selection		
	Expected behaviour	
ensure that		
when		
the RootCA is triggered to delete AA certificate (CERT_AA) from the CTL		
then		
the IUT issue a new CTL of type CtlFormat		
containing isFullCtl		
indicating TRUE		
and containing ctlCommands		
not containing CtlCommand		
containing add		
containing aa		
containing aaCertificate		
indicating CERT_AA		

TP Id	SECPKI_RCA_CTLGEN_12_BV		
Summary	Check that the RootCA generates the Delta CTL when AA is about to be deleted from the		
	Root CTL		
Reference	ETSI TS 102 941 [1], clauses 6.3.2 and 6.3.4		
Configuration	CFG_CTLGEN_RCA		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the RootCA is trigger	the RootCA is triggered to delete AA certificate (CERT_AA) from the CTL		
then	then		
the IUT issue a new CTL of type CtlFormat			
containing isFullCtl			
indicating FAI	indicating FALSE		
and containing ctlCommands			
not containing CtlCommand			
containing delete			
containing cert			
indicating HashedId8 of CERT_AA			

TP ld	SECPKI_RCA_CTLGEN_13_BV	
Summary	Check that the RootCA generates the Full CTL when AA access point URL is about to be	
	changes	
Reference	ETSI TS 102 941 [1], clause 6.3.2	
Configuration	CFG_CTLGEN_RCA	
PICS Selection		
	Expected behaviour	
ensure that		
when		
the RootCA is trigger	red to add new URL for AA access point (URL) to the CTL	
then		
	CTL of type CtlFormat	
	containing isFullCtl	
indicating TRUE		
containing ctlCommands		
containing CtlCommand		
containing add		
containing aa		
containing aaCertificate		
containing accessPoint		
indicating URL		
and NOT containing any other CtlCommand		
containing add		
	ning aa	
containing aaCertificate		
	indicating CERT_AA	

```
TP Id
                          SECPKI_RCA_CTLGEN_14_BV
                          Check that the RootCA generates the Delta CTL when AA access point URL is about to be
Summary
                          changes
Reference
                          ETSI TS 102 941 [1], clause 6.3.2
Configuration
                          CFG_CTLGEN_RCA
PICS Selection
                                            Expected behaviour
ensure that
   when
      the RootCA is triggered to add new URL for AA access point (URL) to the CTL
      the IUT issue a new CTL of type CtlFormat
         containing isFullCtl
             indicating TRUE
         containing ctlCommands
             containing CtlCommand
                containing add
                   containing aa
                      containing aaCertificate
                      containing accessPoint
                          indicating URL
```

TP Id	SECPKI_RCA_CTLGEN_15_BV		
Summary	Check that the RootCA CTL is signed using RootCA verification key		
	Check that signing of the RootCA CTL is permitted by the RootCA certificate		
Reference	ETSI TS 102 941 [1], clause 6.3.2		
Configuration	CFG_CTLGEN_RCA		
PICS Selection			
	Expected behaviour		
with			
the TLM already issued			
	ertificate (CERT_RCA)		
ensure that			
when	L		
	red to issue a new CTL		
then	CTL of them a Dea Contificate Trunch in the Annual CTL		
	CTL of type RcaCertificateTrustListMessage		
containing signed			
	containing signer.digest		
indicating HashedID8 of the RootCA certificate (CERT_RCA) containing appPermissions			
	ining an item of type PsidSsp		
containing an item of type Fsidosp containing psid			
indicating AID_CTL			
and containing ssp			
containing opportunity cop			
indicating 1			
containing opaque[1] (value)			
indicating 'TLM entries' (bit 0) set to 0			
	indicating 'RCA entries' (bit 1) set to 0		
	indicating 'EA entries' (bit 2) set to 1		
	indicating 'AA entries' (bit 3) set to 1		
	indicating 'DC entries' (bit 4) set to 1		
NOTE: The EtsiTs10309	7Data and EtsiTs102941Data envelopes are not yet removed from the analysing message.		

TP Id	CECDIAL DOA CTLOEN 40 DV	
	SECPKI_RCA_CTLGEN_16_BV	
Summary	Check that the RCA CTL sequence counter is monotonically increased	
Reference	ETSI TS 102 941 [1], clause 6.3.2	
Configuration	CFG_CTLGEN_RCA	
PICS Selection		
	Expected behaviour	
with		
the RCA already has iss	ued the previous CTL of type CtlFormat	
containing ctlSequen		
indicating N		
· · · · · · · · · · · · · · · · · · ·		
ensure that		
when		
the RCA is triggered	the RCA is triggered to issue a new CTL	
then		
the IUT issue a new CTL of type CtlFormat		
containing ctlSequence		
indicating N+1		
indicating N+	1	

TP ld	SECPKI_RCA_CTLGEN_17_BV
Summary	Check that the RCA CTL sequence counter is rounded on the value of 256
Reference	ETSI TS 102 941 [1], clause 6.3.2
Configuration	CFG_CTLGEN_RCA
PICS Selection	
	Expected behaviour
with the RCA already has iss containing ctlSequer indicating 255 ensure that when the RCA is triggered	
the IUT issue a new CTL of type CtlFormat containing ctlSequence indicating 0	

TP ld	SECPKI_RCA_CTLGEN_18_BV	
Summary	Check that the RCA CTL has an end-validity time	
Reference	ETSI TS 102 941 [1], clause 6.3.2	
Configuration	CFG_CTLGEN_RCA	
PICS Selection		
Expected behaviour		
ensure that		
when		
the RCA is triggered to issue a new CTL at time T1		
then		
the IUT issue a new CTL of type CtlFormat		
containing nextUpdate		
indicating timestamp greater then T1		

TP ld	SECPKI_RCA_CTLGEN_19_BV		
Summary	Check that the RCA CTL does not contain not allowed entities		
Reference	ETSI TS 102 941 [1], clause 6.3.2		
Configuration	CFG_CTLGEN_RCA		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the RCA is triggered	the RCA is triggered to issue a new CTL		
then			
the IUT issue a new	the IUT issue a new CTL of type CtlFormat		
containing ctlCo	containing ctlCommands		
not containing any item of type CtlCommand			
containing add			
containing tlm			
or containing rea			

TP ld	SECPKI_RCA_CTLGEN_20_BV	
	Check that the RCA Delta CTL is generated at the same time as FullCTL.	
Summary	Check that the RCA Delta CTL is a difference between correspondent Full CTL and the	
	previous Full CTL	
Reference	ETSI TS 102 941 [1], clause 6.3.2	
Configuration	CFG_CTLGEN_RCA	
PICS Selection		
	Expected behaviour	
with		
the RCA already issued	the previous CTL of type CtlFormat (CTL_FULL_PREV)	
containing isFullCtl		
indicating TRUE		
containing ctlSequen	nce	
indicating N		
ensure that		
when	4 · OTI	
the RCA is triggered	to issue a new CTL	
then	CTL of tune Ctl Formet (CTL FULL)	
containing isFullC	CTL of type CtlFormat (CTL_FULL)	
indicating TRUE and containing ctlSequence		
indicating N+1		
and the IUT issue a new CTL of type CtlFormat (CTL_DELTA)		
containing isFullCtl		
indicating FALSE		
and containing ctlSequence		
indicating N+		
containing ctlCon		
indicating diffe	erence between CTL_FULL and CTL_FULL_PREV	

TP ld	SECPKI_RCA_CTLGEN_21_BV		
Summary	Check that the RCA CTL version is set to 1		
Reference	ETSI TS 102 941 [1], clause 6.3.2		
Configuration	CFG_CTLGEN_RCA		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the IUT is triggered to issue a new CTL			
then			
the IUT issue a new CTL of type CtlFormat			
containing version			
indicating 1			

TP Id	SECPKI_RCA_CTLGEN_22_BV	
Summary	Check that the RCA Full CTL does not contain commands of type 'delete'	
Reference	ETSI TS 102 941 [1], clause 6.3.2	
Configuration	CFG_CTLGEN_RCA	
PICS Selection		
	Expected behaviour	
ensure that		
when		
the IUT is trigg	pered to delete the CA from the CTL	
then		
the IUT issue a	a new CTL of type CtlFormat (CTL FULL)	
containing	isFullCtl	
indicati	ng TRUE	
and containing ctlCommands		
	NOT containing any item of type CtlCommand	
containing delete		

TP ld	SECPKI_RCA_CTLGEN_23_BV		
Summary	Check that the RCA CTL contains at least one DC entry		
Reference	ETSI TS 102 941 [1], clause 6.3.2		
Configuration	CFG_CTLGEN_RCA		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the IUT is triggered t	o issue a new CTL		
then	then		
the IUT issue a new CTL of type CtlFormat			
containing isFullCtl			
indicating TRUE			
and containing ct	lCommands		
containing at least one ctlCommand			
containing add			
containing url			
indicating URL of the DC of the IUT			
contai	ning cert		
containing the item of type HashedId8			
	indicating the HashedId8 of the IUT certificate		

#### 5.6.2 CRL generation

For the scope of test purposes of this clause, the EtsiTs103097Data and EtsiTs102941Data envelopes are already removed from the analysing messages if it is not explicitly specified in the test purpose.

TP ld	SECPKI_RCA_CRLGEN_01_BV
Summary	Check that the RootCA generates the CRL signed with appropriate certificate
Reference	ETSI TS 102 941 [1], clause 6.3.3
Configuration	CFG_CRLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	
when	
the RootCA is trigger	red to generate new CRL
then	
the IUT generates the CertificateRevocationListMessage	
containing signer	
containing diges	st
indicating Ha	ashedId8 of RootCA certificate
containir	ng appPermissions
	ining an item of type PsidSsp
COI	ntaining psid
į ir	ndicating AID_CRL
and	d containing ssp
c	containing opaque[0] (version)
	indicating 1

TP Id	SECPKI_RCA_CRLGEN_02_BV
Summary	Check that the RootCA generates the CRL when CA certificate is about to be revoked
Reference	ETSI TS 102 941 [1], clause 6.3.3
Configuration	CFG_CRLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	
when	
the RootCA is triggered to add new CA certificate (CERT_CA) to the revocation list	
then	
the IUT issue a new CRL of type ToBeSignedCrl	
and containing entries	
containing item of type CrlEntry	
indicating HashID8 of the CERT_CA	

NOTE: The EtsiTs103097Data and EtsiTs102941Data envelopes are not yet removed from the analysing message.

TP Id	SECPKI_RCA_CRLGEN_03_BV
Summary	Check that the RootCA generates the CRL when its own certificate is about to be revoked
Reference	ETSI TS 102 941 [1], clause 6.3.3
Configuration	CFG_CRLGEN_RCA
PICS Selection	
	Expected behaviour
with the TLM already issued the CTL containing the RCA certificate CERT_RCA ensure that when the RootCA is triggered to revoke itself then the IUT issue a new CRL of type ToBeSignedCrl containing entries containing item of type CrlEntry indicating HashID8 of the CERT_RCA	

TP ld	SECPKI_RCA_CRLGEN_04_BV	
Summary	Check that the CRL of the RCA is timestamped	
Reference	ETSI TS 102 941 [1], clause 6.3.3	
Configuration	CFG_CRLGEN_RCA	
PICS Selection		
Expected behaviour		
ensure that		
when	when	
the RootCA is triggered to issue a new CRL at the time T1		
then		
the IUT issue a new CRL of type ToBeSignedCrl		
containing thisUpdate		
indicating timestamp greater or equal to the T1		

TP ld	SECPKI_RCA_CRLGEN_05_BV
Summary	Check that the RCA issuing a new CRL when previous one is expired
Reference	ETSI TS 102 941 [1], clause 6.3.3
Configuration	CFG_CRLGEN_RCA
PICS Selection	
	Expected behaviour
with	
the RCA already issued	the CRL
containing nextUpda	te
indicating time Tprev	
ensure that	
when	
the Tprev is less than current time (Tcur)	
then	
the IUT issue a new CRL of type ToBeSignedCrl	
containing thisUpdate	
indicating timestamp greater or equal to the Tcur	
and containing nextUpdate	
indicating time	estamp greater than Tcur and greater than thisUpdate

TP Id	SECPKI_RCA_CRLGEN_06_BV		
Summary	Check that the RootCA is generated the CRL when its own certificate is about to be		
	revoked		
Reference	ETSI TS 102 941 [1], clause 6.3.3		
Configuration	CFG_CRLGEN_RCA		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the RootCA is triggered to issue a new CRL			
then			
the IUT issue a new CRL of type ToBeSignedCrl			
and containing entries			
does not containing item of type CrlEntry			
indicating HashID8 of other RootCA			

TP ld	SECPKI_RCA_CRLGEN_07_BV		
Summary	Check that the RootCA generates the CRL when CA certificate is about to be revoked		
Reference	ETSI TS 102 941 [1], clause 6.3.3		
Configuration	CFG_CRLGEN_RCA		
PICS Selection			
	Expected behaviour		
ensure that			
when	when		
the RootCA is triggered to issue a new CRL			
then			
the IUT issue a new CRL of type ToBeSignedCrl			
and containing entries			
does not containing item of type CrlEntry			
indicating HashID8 of other RootCA			

TP Id	SECPKI_RCA_CRLGEN_08_BV		
Summary	Check that the RCA CRL version is set to 1		
Reference	ETSI TS 102 941 [1], clause 6.3.3		
Configuration	CFG_CRLGEN_RCA		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the RCA is triggered to issue a new CRL			
then			
the IUT issue a new CRL of type ToBeSignedCrl			
containing version			
indicating	indicating 1		

#### 5.6.3 CA certificate generation

TP Id	SECPKI_RCA_CAGEN_01_BV
Summary	Check that generated EA certificate contains only allowed permissions
Reference	ETSI TS 102 941 [1], clause B.5
Configuration	CFG_CAGEN_RCA
PICS Selection	

```
Expected behaviour
ensure that
   when
      the IUT is requested to generate EA certificate
   then
       the IUT generate the certificate
          containing appPermissions
              containing an item of type PsidSsp
                 containing psid
                    indicating AID_CERT_REQ
                 and containing ssp
                    containing opaque[0] (version)
                        indicating 1
                    containing opaque[1] (value)
                        indicating 'Authorization validation Response' (bit 4) set to 1
                        and indicating 'Enrolment Response' (bit 5) set to 1
                        and indicating 'CA certificate request' (bit 6) set to 1
                        and indicating other bits set to 0
              and NOT containing an item of type PsidSsp
                 containing psid
                    indicating AID_CTL
              and NOT containing an item of type PsidSsp
                 containing psid
                    indicating AID_CRL
          containing certIssuePermissions
              containing an item of type PsidGroupPermissions
                 containing eeType
                    indicating app
                 containing subjectPermissions
                    containing explicit
                        containing en item of type PsidSspRange
                           containing psid
                               indicating AID_CERT_REQ
                           and containing sspRange
                               containing bitmapSspRange
                                  containing sspBitmask
                                      indicating FFh
                                   containing sspValue
                                      indicating 01h A0h
                        and NOT containing an item of type PsidSspRange
                           containing psid
                               indicating AID_CTL
                        and NOT containing an item of type PsidSsp
                           containing psid
                               indicating AID_CRL
```

TP Id	SECPKI_RCA_CAGEN_02_BV		
Summary	Check that generated AA certificate contains only allowed permissions		
Reference	ETSI TS 102 941 [1], clause B.5		
Configuration	CFG_CAGEN_RCA		
PICS Selection			
	Expected behaviour		
ensure that	·		
when			
the IUT is requested	to generate AA certificate		
then			
the IUT generate the	e certificate		
containing appPe	ermissions		
containing an	item of type PsidSsp		
containing	g psid		
indicat	ting AID_CERT_REQ		
and conta	ining ssp		
contai	ning opaque[0] (version)		
	dicating 1		
	ning opaque[1] (value)		
	licating 'Authorization validation Request (bit 2) set to 1		
	d indicating 'Authorization Response' (bit 3) set to 1		
an	d indicating 'CA certificate request' (bit 6) set to 1		
	d indicating other bits set to 0		
	taining an item of type PsidSsp		
containing			
	ting AID_CTL		
	and NOT containing an item of type PsidSsp		
containing psid			
indicating AID_CRL			
	containing certIssuePermissions containing an item of type PsidGroupPermissions		
	containing eeType indicating app		
containing subjectPermissions			
containing explicit			
NOT containing en item of type PsidSspRange			
containing psid			
indicating AID_CERT_REQ			
or containing en item of type PsidSspRange			
containing psid			
indicating AID_CERT_REQ			
	and containing sspRange		
	containing bitmapSspRange		
	containing sspBitmask		
	indicating FFh		
	containing sspValue		
	indicating 01h 00h		
an	d NOT containing an item of type PsidSspRange		
	containing psid		
	indicating AID_CTL		
an	d NOT containing an item of type PsidSsp		
	containing psid indicating AID_CRL		
	Indicating AID_CAL		

```
TP Id
                           SECPKI_RCA_CAGEN_03_BV
Summary
                           Check that generated RootCA certificate contains only allowed permissions
Reference
                           ETSI TS 102 941 [1], clause B.5
Configuration
                           CFG_CAGEN_RCA
PICS Selection
                                              Expected behaviour
ensure that
   when
      the IUT is requested to generate AA certificate
      the IUT generate the certificate
          containing appPermissions
             NOT containing an item of type PsidSsp
                 containing psid
                    indicating AID_CERT_REQ
             and containing an item of type PsidSsp
                 containing psid
                    indicating AID_CTL
                 and containing ssp of length 2
                       indicating 01h 38h
             and containing an item of type PsidSsp
                 containing psid
                    indicating AID_CRL
                 and containing ssp of length 1
                    containing opaque[0] (version)
                       indicating 1
          and containing certIssuePermissions
             containing an item of type PsidGroupPermissions
                 containing eeType
                    indicating app
                 containing subjectPermissions
                    containing explicit
                       containing en item of type PsidSspRange
                           containing psid
                              indicating AID_CERT_REQ
                           and containing sspRange
                              containing bitmapSspRange
                                  containing sspBitmask of length 2
                                     indicating FFh FFh
                                  containing sspValue of length 2
                                     indicating 01h FEh
                       and NOT containing an item of type PsidSspRange
                           containing psid
                              indicating AID_CTL
                       and NOT containing an item of type PsidSsp
                           containing psid
                              indicating AID_CRL
```

#### 5.7 DC behaviour

TP Id	SECPKI_DC_LISTDIST_01_BV	
Summary	Check that the RCA CRL is published and accessible when issued	
Reference	ETSI TS 102 941 [1], clause 6.3.3	
Configuration	CFG_DC	
PICS Selection		
Expected behaviour		
with		
the TLM issued a new CRL		
ensure that		
when		
the ITS-S asked the IUT for the newly issued CRL		
then	then	
the IUT is answered with this CRL		

TP ld	SECPKI_DC_LISTDIST_02_BV		
Summary	Check that the RCA CTL is published and accessible when issued		
Reference	ETSI TS 102 941 [1], clauses 6.3.2 and 6.3.3		
Configuration	CFG_DC		
PICS Selection			
Expected behaviour			
with			
the TLM issued a new C	the TLM issued a new CTL		
ensure that			
when			
the ITS-S asked the IUT for the newly issued CTL			
then			
the IUT is answered with this CTL			

## 5.8 TLM behaviour

## 5.8.1 CTL generation

For the scope of test purposes of this clause, the <code>EtsiTs103097Data</code> and <code>EtsiTs102941Data</code> envelopes are already removed from the analysing messages if it is not explicitly specified in the test purpose.

TP Id	SECPKI_TLM_ECTLGEN_01_BV		
Summary	Check that the TLM generates the ECTL when new RootCA is about to be added		
Reference	ETSI TS 102 941 [1], clause 6.3.1		
Configuration	CFG_CTLGEN_TLM		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the TLM is triggered to add new RootCA certificate (CERT_RCA) in the CTL			
then			
the IUT issue a new	the IUT issue a new CTL of type CtlFormat		
containing isFullC	containing isFullCtl		
indicating TRUE			
and containing ctlCommands			
containing CtlCommand			
containing add			
containing rca			
cor	containing selfsignedRootCa		
indicating CERT_RCA			

TP ld	SECPKI_TLM_ECTLGEN_02_BV		
Summary	Check that the TLM generates the Delta ECTL when new RootCA is about to be added		
Reference	ETSI TS 102 941 [1], clause 6.3.1		
Configuration	CFG_CTLGEN_TLM		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the TLM is triggered	to add new RootCA certificate (CERT_RCA) in the CTL		
then			
the IUT issue a new	the IUT issue a new CTL of type CtlFormat		
containing isFullC	Ctl		
indicating FALSE			
and containing ctlCommands			
containing CtlCommand			
containing add			
containing rca			
cor	ntaining selfsignedRootCa		
indicating CERT_RCA			

TP Id	SECPKI_TLM_ECTLGEN_03_BV		
Summary	Check that the TLM generates the Full ECTL when RootCA is about to be deleted		
Reference	ETSI TS 102 941 [1], clause 6.3.1		
Configuration	CFG_CTLGEN_TLM		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the TLM is triggered	the TLM is triggered to delete RootCA certificate (CERT_RCA) from the CTL		
then			
the IUT issue a new	the IUT issue a new CTL of type CtlFormat		
containing isFullO	containing isFullCtl		
indicating TRUE			
and containing ct	and containing ctlCommands		
not containing CtlCommand			
containing add			
containing rca			
COI	containing selfsignedRootCa		
indicating CERT_RCA			

TP Id	SECPKI_TLM_ECTLGEN_04_BV		
Summary	Check that the TLM generates the Delta ECTL when RootCA is about to be deleted		
Reference	ETSI TS 102 941 [1], clause 6.3.1		
Configuration	CFG_CTLGEN_TLM		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the TLM is triggered	the TLM is triggered to delete RootCA certificate (CERT_RCA) from the CTL		
then	then		
the IUT issue a new	CTL of type CtlFormat		
containing isFull(	Ctl Ctl		
indicating FAI	LSE		
and containing ctlCommands			
containing CtlCommand			
containing delete			
containing cert			
	indicating HashedId8 of CERT_RCA		

TP Id	SECPKI_TLM_ECTLGEN_05_BV		
Summary	Check that the TLM generates the ECTL when TLM certificate shall be changed		
Reference	ETSI TS 102 941 [1], clause 6.3.1		
Configuration	CFG_CTLGEN_TLM		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the TLM is triggered	to add new the TLM certificate (CERT_TLM) in the CTL		
then	· · · · · · · · · · · · · · · · · · ·		
the IUT issue a new	the IUT issue a new CTL of type CtlFormat		
containing isFull(	Ctl Ctl		
indicating TR			
and containing ctlCommands			
not containing CtlCommand			
containing add			
contai	containing tlm		
containing selfSignedTLMCertificate			
indicating CERT_TLM			

TP Id	SECPKI_TLM_ECTLGEN_06_BV		
Summary	Check that the TLM generates the Delta ECTL when TLM certificate shall be changed		
Reference	ETSI TS 102 941 [1], clause 6.3.1		
Configuration	CFG_CTLGEN_TLM		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the TLM is triggered to add new the TLM certificate (CERT_TLM) in the CTL			
then			
the IUT issue a new	the IUT issue a new CTL of type CtlFormat		
containing isFullO	containing isFullCtl		
indicating FALSE			
and containing ctlCommands			
not containing CtlCommand			
containing add			
containing tlm			
	containing selfSignedTLMCertificate		
indicating CERT_TLM			

TP ld	SECPKI_TLM_ECTLGEN_07_BV		
Summary	Check that the TLM generates the ECTL when CPOC access point has been changed		
Reference	ETSI TS 102 941 [1], clauses 6.3.1 and 6.3.4		
Configuration	CFG_CTLGEN_TLM		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the TLM is triggered	the TLM is triggered to change the CPOC URL in the CTL		
then			
the IUT issue a new	CTL of type CtlFormat		
containing isFull0	Ctl Ctl		
indicating TR	indicating TRUE		
and containing ct	and containing ctlCommands		
not containing CtlCommand			
containing add			
contai	containing tlm		
containing accessPoint			
	indicating URI		

TP Id	SECPKI_TLM_ECTLGEN_08_BV		
Summary	Check that the TLM generates the ECTL when CPOC access point has been changed		
Reference	ETSI TS 102 941 [1], clauses 6.3.1 and 6.3.4		
Configuration	CFG_CTLGEN_TLM		
PICS Selection			
	Expected behaviour		
ensure that			
when	when		
the TLM is triggered	the TLM is triggered to change the CPOC URL in the CTL		
then			
the IUT issue a new	the IUT issue a new CTL of type CtlFormat		
containing isFull(			
indicating FA			
and containing ct	and containing ctlCommands		
not containing CtlCommand			
containing add			
containing tlm			
CO	containing accessPoint		
indicating URL			

TP Id	SECPKI_TLM_ECTLGEN_09_BV		
	Check that the TLM CTL is signed using TLM verification key		
Summary	Check that signing of TLM CTL is allowed by the TLM certificate		
Reference	ETSI TS 102 941 [1], clause 6.3.1		
Configuration			
PICS Selection	GFG_GTLGEN_TLW		
PICS Selection	Expected behaviour		
ensure that	Expedica beliavioui		
when			
*******	ed to issue a new CTL		
then	0 10 10 10 10 10 10 10 10 10 10 10 10 10		
	w CTL of type TlmCertificateTrustListMessage		
containing sign	•		
	signer.digest		
	ng HashedID8 of the TLM certificate (TLM_CERT)		
	containing appPermissions		
co	ntaining an item of type PsidSsp		
	containing psid		
	indicating AID_CTL		
	and containing ssp		
containing opaque[0] (version)			
	indicating 1		
	containing opaque[1] (value)		
	indicating 'TLM entries' (bit 0) set to 1		
	indicating 'RCA entries' (bit 1) set to 1		
	indicating 'EA entries' (bit 2) set to 0		
indicating 'AA entries' (bit 3) set to 0			
indicating 'DC entries' (bit 4) set to 1			
	containing tbsData.payload.data		
	containing OER-encoded EtsiTs103097Data structure		
containing OER-encoder EtsiTs102941Data structure			
containing content.certificateTrustListTlm			
containing ctlCommands			
	containing add		
	containing tim		
containing selfSignedTLMCertificate			
NOTE: The EtsiTs103	indicating TLM_CERT  097Data and EtsiTs102941Data envelopes are not yet removed from the analysing message.		
INOTE. THE EISHS 103	037 Data and Etol 15 10234 IData envelopes are not yet removed normine analysing message.		

TP Id	SECPKI_TLM_ECTLGEN_10_BV	
Check that the TLM CTL sequence counter is monotonically increased		
Reference	eference ETSI TS 102 941 [1], clause 6.3.1	
Configuration	CFG_CTLGEN_TLM	
PICS Selection		
Expected behaviour		
with	with	
the TLM already has issued the previous CTL of type CtlFormat		
containing ctlSequence		
indicating N		
ensure that		
when	when	
the TLM is triggered to issue a new CTL		
then		
the IUT issue a new CTL of type CtlFormat		
containing ctlSequence		
indicating N+1		

TP Id	SECPKI TLM ECTLGEN 11 BV	
Summary	Check that the TLM CTL sequence counter is rounded on the value of 256	
Reference		
Configuration	CFG CTLGEN TLM	
PICS Selection		
	Expected behaviour	
with		
	issued the previous CTL of type CtlFormat	
	containing ctlSequence indicating 255	
ensure that	ensure that	
when		
the TLM is trigger	the TLM is triggered to issue a new CTL	
then		
the IUT issue a new CTL of type CtlFormat		
containing ctlSequence		
	indicating 0	

TP ld	SECPKI_TLM_ECTLGEN_12_BV	
Summary	Check that the TLM CTL has an end-validity time	
Reference	ETSI TS 102 941 [1], clause 6.3.1	
Configuration	CFG_CTLGEN_TLM	
PICS Selection		
Expected behaviour		
ensure that		
when		
the TLM is triggered to issue a new CTL at time T1		
then		
the IUT issue a new CTL of type CtlFormat		
containing nextUpdate		
	indicating timestamp greater then T1	

	<del></del>		
TP Id	SECPKI_TLM_ECTLGEN_13_BV		
Summary	ummary Check that the TLM CTL does not have other entries then allowed		
Reference	ETSI TS 102 941 [1], clause 6.3.1		
Configuration	CFG_CTLGEN_TLM		
PICS Selection			
	Expected behaviour		
ensure that			
when	when		
the TLM is triggered to issue a new CTL			
then			
the IUT issue a	the IUT issue a new CTL of type CtlFormat		
containing of	ctlCommands		
not containing any item of type CtlCommand			
containing add			
containing ea			
or containing aa			

TP ld	SECPKI_TLM_ECTLGEN_14_BV		
	Check that the TLM Delta CTL is generated at the same time as FullCTL.		
Summary	Check that the TLM Delta CTL is a difference between correspondent Full CTL and the		
	previous Full CTL		
Reference	ETSI TS 102 941 [1], clause 6.3.1		
Configuration	CFG_CTLGEN_TLM		
PICS Selection			
	Expected behaviour		
with			
the TLM already issued	the previous CTL of type CtlFormat (CTL_FULL_PREV)		
containing isFullCtl			
indicating TRUE			
containing ctlSequer	containing ctlSequence		
indicating N			
ensure that			
when			
the TLM is triggered to issue a new CTL			
then			
	CTL of type CtlFormat (CTL_FULL)		
containing isFullCtl			
	indicating TRUE		
and containing ctlSequence			
indicating N+1			
and the IUT issue a new CTL of type CtlFormat (CTL_DELTA)			
containing is Full Ctl			
indicating FALSE			
and containing ctlSequence			
indicating N+			
containing ctlCommands			
indicating difference between CTL_FULL and CTL_FULL_PREV			

TP Id	SECPKI_TLM_ECTLGEN_15_BV		
Summary	Check that the TLM CTL version is set to 1		
Reference	ETSI TS 102 941 [1], clause 6.3.4		
Configuration	CFG_CTLGEN_TLM		
PICS Selection			
	Expected behaviour		
ensure that	ensure that		
when	when		
the IUT is triggered to issue a new CTL			
then			
the IUT issue a new CTL of type CtlFormat			
containing version			
indicating 1			

TP Id	SECPKI TLM ECTLGEN 16 BV		
Summary			
, , , , , , , , , , , , , , , , , , ,	* '		
Reference	ETSI TS 102 941 [1], clause 6.3.1		
Configuration	CFG_CTLGEN_TLM		
PICS Selection			
	Expected behaviour		
ensure that			
when	when		
the IUT is triggered t	o delete the CA from the CTL		
then			
the IUT issue a new	CTL of type CtlFormat		
containing isFullO	Ctl		
	indicating TRUE		
and containing ctlCommands			
NOT containing any item of type CtlCommand			
containing delete			

## 5.9 CPOC behaviour

TP ld	SECPKI_CPOC_LISTDIST_01_BV	
Summary	Check that the TLM CTL is published and accessible when issued	
Reference	ETSI TS 102 941 [1], clauses 6.3.2 and 6.3.3	
Configuration	ion CFG_CPOC	
PICS Selection		
Expected behaviour		
with		
the TLM issued a new CTL		
ensure that		
when		
the ITS-S asked the IUT for the newly issued CTL		
then		
the IUT is answered	the IUT is answered with this CTL	

# History

Document history		
V1.1.1	March 2019	Publication
V1.2.1	January 2022	Publication