ETSI TS 103 525-2 V2.1.1 (2024-09)

TECHNICAL SPECIFICATION

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

Reference

RTS/ITS-00598

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 the ETSI Search & Browse Standards application.

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 on ETSI deliver.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

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

Contents

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

Foreword

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

The present document is part 2 of a multi-part deliverable. Full details of the entire series can be found in part 1 [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 ETSI Drafting Rules (Verbal forms for the expression of provisions).

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

1 Scope

The present document provides the Test Suite Structure and Test Purposes (TSS & TP) for 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 https://docbox.etsi.org/Reference/.

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

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

[1] ETSI TS 102 941 (V2.2.1): "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2".

[2] ETSI TS 103 097 (V2.1.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats; Release 2".

[3] IEEE Std 1609.2™-2016: "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages", as amended by IEEE Std 1609.2a™-2017: "IEEE Standard for Wireless Access In Vehicular Environments - Security Services for Applications and Management Messages - Amendment 1".

[4] ETSI TS 103 525-1 (V2.1.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 1: Protocol Implementation Conformance Statement (PICS); Release 2".

[5] ETSI TS 103 096-2 (V2.1.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 2: Test Suite Structure and Test Purposes (TSS & TP); Release 2".

[6] ETSI TS 103 601 (V2.1.1): "Intelligent Transport Systems (ITS); Security; Security management messages communication requirements and distribution protocols; Release 2".

[7] European Commission: "Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)" Release 1.1, June 2018.

[8] ETSI TS 102 965 (V2.2.1): "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration; Release 2".

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] Void.

[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 [8], 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_CRL: "CRL service" ITS-AID

AID_CTL: "CTL service" ITS-AID

3.2 Symbols

Void.

3.3 Abbreviations

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

AA	Authorization Authority
AES	Advanced Encryption Standard
AID	Application IDentifier

AT	Authorization Ticket
ATS	Abstract Test Suite
BO	exceptional BehaviOur
BTP	Basic Transport Protocol
BV	Valid Behaviour
CA	Certification Authority
CAM	Co-operative Awareness Messages
CERT	CERTificate
C-ITS	Cooperative Intelligent Transport System
CPOC	C-ITS Point Of Contact
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CTL	Certificate Trust List
DC	Distribution Centre
DENM	Decentralized Environmental Notification Message
EA	Enrolment Authority
EC	Enrolment Credential
ECC	Elliptic Curve Cryptography
ECTL	European Certificate Trust List
GN	GeoNetworking
GN-MGMT	GN Management
GPC	GNSS Positioning Correction
HMAC	keyed-Hash Message Authentication Code
ITS	Intelligent Transportation Systems
ITS-S	Intelligent Transport System - Station
IUT	Implementation Under Test
IVIM	Infrastructure to Vehicle Information Message
MAPEM	MAP (topology) Extended Message
MSG	MesSaGe
OER	Octet Encoding Rules
PCI	Permanent Canonical Identifier
PICS	Protocol Implementation Conformance Statement
PIXIT	Partial Protocol Implementation eXtra Information for Testing
PKI	Public Key Infrastructure
PSID	Provider Service IDentifier
RCA	Root Certificate Authority
SPATEM	Signal Phase And Timing Extended Message
SREM	Signal Request Message
SSEM	Signal Status Extended Message
SSP	Service Specific Permissions
TLM	Trust List Manager
TP	Test Purposes
TS	Test System
TSS	Test Suite Structure
URL	Uniform Resource Locator
UT	Upper Tester

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	Enrollment	Valid
		Authorization	Valid
		CRL handling	Valid
		CTL handling	Valid
	CA	Common Certificate Authority	Valid
	EA	Enrollment	Valid
		Authorization validation	Valid
		Butterfly authorization	Valid
		Butterfly certificate download	Valid
		CA certificate generation	Valid
		CRL handling	Valid
		CTL handling	Valid
	AA	Authorization	Valid
		Authorization validation	Valid
		CA certificate generation	Valid
		Butterfly 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 the 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 the 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 the 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 the 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

This clause introduces the different IUT's configurations required to execute the TPs described in clause 5.

4.3.2 Enrollment

4.3.2.1 Configuration CFG_ENR_ITS-S

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

- IUT is configured to be directly entitled to the initial enrolment, as specified in ETSI TS 102 941 [1], clause 6.1.3.0.
- 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_ITS-S

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 AA.

TS: 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 Authorization using butterfly key expansion mechanism

4.3.5.1 Configuration CFG_BFK_AUTH_ITS-S

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 enrolment certificate issued by the emulated EA;
- the access point URL of the emulated EA.

TS: AA and EA are emulated by the TS.

4.3.5.2 Configuration CFG_BFK_AUTH_EA

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

- the profile information for the emulated ITS-S;
- the certificate of the emulated AA;
- the access point URL of the emulated AA.

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

- the enrolment certificate issued by the IUT;
- the enrolment authority certificate of the IUT.

4.3.5.3 Configuration CFG_BFK_AUTH_AA

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

- the profile information for the emulated ITS-S;
- the certificate of the emulated EA.

TS: EA emulated by the TS and contains following information elements:

- the AA certificate of the IUT.

4.3.6 CA certificate generation

4.3.6.1 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.

4.3.6.2 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.

4.3.6.3 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.

4.3.7 ECTL generation

4.3.7.1 Configuration CFG_CTLGEN_TLM

IUT: TLM in the operational state.

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

4.3.7.2 Configuration CFG_CTLGEN_CPOC

IUT: CPOC in the operational state.

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

4.3.8 Root CTL generation

4.3.8.1 Configuration CFG_CTLGEN_RCA

IUT: RCA in the operational state.

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

4.3.9 CRL generation

4.3.9.1 Configuration CFG_CRLGEN_RCA

IUT: RCA in the operational state.

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

4.3.10 ITS-S CRL/CTL handling

4.3.10.1 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>_[<sgr>_]<sn>_<x>		
	<root> = root	SECPKI	
	<tgt> = target	ITS-S	ITS-Station
		CA	Common Certificate Authority
		AA	Authorization Authority
		EA	Enrolment Authority
		RCA	Root Certification Authority
		DC	Distribution Centre
		CPOC	C-ITS Point of Contact
	<gr> = group	ENR	Enrollment
		AUTH	Authorization
		AUTHVAL	Authorization Validation
		BFK_AUTH	Butterfly authorization request
		BFK_CERTGEN	Butterfly certificate generation
		BFK_CERTDNL	Butterfly certificate download
		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 (optional)	SND	Sending behaviour (default if omitted)
		RCV	Receiving behaviour
		REP	Repetition behaviour
	<sn> = test purpose sequential number		01 to 99
	<x> = category	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_ITS-S	[4] A.2.1
PICS_SECPKI_IUT_EA	[4] A.3.2
PICS_SECPKI_IUT_AA	[4] A.3.3
PICS_SECPKI_IUT_RCA	[4] A.3.4
PICS_SECPKI_IUT_DC	[4] A.3.5
PICS_SECPKI_IUT_TLM	[4] A.3.6
PICS_SECPKI_IUT_CPOC	[4] A.3.7
PICS_SECPKI_ENROLLMENT	[4] A.2.2 or A.4.1
PICS_SECPKI_ENROLLMENT_RETRY	[4] A.2.2.2 or A.4.4
PICS_SECPKI_ENROLLMENT_X509	[4] A.2.2 and A.1.7
PICS_SECPKI_REENROLLMENT	[4] A.2.2.1 or A.4.2
PICS_SECPKI_AUTHORIZATION	[4] A.2.3 or A.5.1
PICS_SECPKI_ AUTHORIZATION _RETRY	[4] A.2.3.3 or A.5.5
PICS_SECPKI_AUTH_PRIVACY	[4] A.2.3.1 or A.5.3
PICS_SECPKI_AUTH_POP	[4] A.2.3.2 or A.5.2
PICS_SECPKI_AUTH_VALIDATION	[4] A.4.3
PICS_SECPKI_AUTH_BFK	[4] A.5.6
PICS_SECPKI_CRL	[4] A.8.5 or A.6.1
PICS_SECPKI_CRL_DOWNLOAD	[4] A.8.6
PICS_SECPKI_CRL_BROADCAST	[4] A.8.9
PICS_SECPKI_CTL	[4] A.8.3 or A.6.2
PICS_SECPKI_CTL_DELTA	[4] A.8.3.1 or A.6.2.1 or A.6.4.1
PICS_SECPKI_CTL_DOWNLOAD	[4] A.8.4
PICS_SECPKI_CTL_BROADCAST	[4] A.8.8
PICS_SECPKI_ECTL	[4] A.8.1 or A.7.1
PICS_SECPKI_ECTL_DELTA	[4] A.8.1.1 or A.7.1.1 or A.7.2.1
PICS_SECPKI_ECTL_DOWNLOAD	[4] A.8.2 or A.7.3
PICS_SECPKI_ECTL_BROADCAST	[4] A.8.7
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 Table 4.

Table 4: Certificates content

AA certificate	Content	To be installed on the IUT
CERT_IUT_A_EA	• signer digest of the CERT_IUT_A_CA; • application permissions: – CRT_REQ with SSP 0x0107; • certificate issuing permissions (SSP value/mask): – CRT_REQ with SSP 0x1C0; • validation time for 3 years; • no region restriction; • assurance level 4; • verification key of type compressed with NIST P256R curve; • encryption key of type compressed with NIST P256R curve; • valid signature of type x-only with NIST P256R curve;	Yes

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 SSP (0x01FFFC / 0xFF0003);
	– DENM with all possible SSP (0x01FFFFFF / 0xFF000000);
	– SPATEM with all possible SSP (0x01E0 / 0xFF1F);
	– MAPEM with all possible SSP (0x01C0 / 0xFF3F);
	– IVIM with all possible SSP (0x01000000FFF8 / 0xFF0000000007);
	– SREM with all possible SSP (0x01FFFFE0 / 0xFF00001F);
	– SSEM with all possible SSP (0x01 / 0xFF);
	– GPC with all possible SSP (0x01 / 0xFF);
	– GN-MGMT without SSP;
	• validation time for 3 years;
	• no region restriction;
	• assurance level 4;
	• verification key of type compressed with NIST P256R curve;
	• encryption key of type compressed with NIST P256R curve;
	• valid signature of type x-only with NIST P256R curve;
		Yes

CERT_IUT_A_CA	• same as CERT_IUT_A_AA;	Yes
CERT_IUT_I_CA	• same as CERT_IUT_A_CA; • type implicit; • not containing signature; • not containing verification key; • containing reconstruction value.	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_ITS-S = 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_ITS-S_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_ITS-S
PICS Selection	
Expected behaviour	

```
with
    the IUT being in the 'initialized' state
ensure that
    when
        the IUT is triggered to request a new Enrolment Credential (EC) certificate
    then
        the IUT sends to EA an EnrolmentRequestMessage
```

TP Id	SECPKI_ITS-S_ENR_02_BV
Summary	If the enrolment request of the IUT is an initial enrolment request, the itsId (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_ITS-S
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 EtsiTs102941Data
                    containing enrolmentRequest
                        containing InnerEcRequest
                            containing itsId
                                indicating the canonical identifier of the ITS-S
                and containing signer
                    declared as self
                and containing signature
                    computed using the canonical private key
```

TP Id	SECPKI_ITS-S_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_ITS-S
PICS Selection	PICS_SECPKI_REENROLMENT

Expected behaviour

```
with
    the IUT being enrolled with certificate CERT_EC
ensure that
    when
        the IUT is requested to send an EnrolmentRequestMessage
    then
        the IUT sends an EtsiTs103097Data-Encrypted
            containing an encrypted EtsiTs103097Data-Signed
                containing EtsiTs102941Data
                    containing enrolmentRequest
                        containing InnerEcRequest
                            containing itsId
                                declared as digest containing the HashedId8 of the CERT_EC
                and containing signer
                    declared as digest containing the HashedId8 of the CERT_EC
                and containing signature
                    computed using the private key corresponding to CERT_EC verification public key
```

TP Id	SECPKI_ITS-S_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_ITS-S
PICS Selection	

Expected behaviour

```
with
    the IUT being in the 'enrolled' state
    and the EC of the IUT expires
ensure that
    when
        the IUT is requested to send an EnrolmentRequestMessage
    then
        the IUT sends an EtsiTs103097Data-Encrypted
            containing an encrypted EtsiTs103097Data-Signed
                containing EtsiTs102941Data
                    containing enrolmentRequest
                        containing InnerEcRequest
                            containing itsId
                                indicating the canonical identifier of the ITS-S
```

TP Id	SECPKI_ITS-S_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 ETSI TS 103 097 [2], clause 7
Configuration	CFG_ENR_ITS-S
PICS Selection	PICS_SECPKI_REENROLMENT
Expected behaviour	

```
with
    the IUT being in the 'initialized' state
ensure that
    when
        the IUT is requested to send multiple EnrolmentRequestMessage
    then
        each EnrolmentRequestMessage
            contains a different and unique verification key pair within the InnerECRequest
```

NOTE: The first EnrolmentRequestMessage should be an initial request, the following EnrolmentRequestMessages should be rekeying requests.

TP Id	SECPKI_ITS-S_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_ITS-S
PICS Selection	
Expected behaviour	

```
with
    the IUT being in the 'initialized' or 'enrolled' 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 EtsiTs102941Data
                    containing enrolmentRequest
                        containing InnerEcRequest
                            containing requestedSubjectAttributes
                                not containing certIssuePermissions
```

TP Id	SECPKI_ITS-S_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 [8] and the generationTime shall be present
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.1
Configuration	CFG_ENR_ITS-S
PICS Selection	
Expected behaviour	

```
with
    the IUT being in the 'initialized' or 'enrolled' 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 EtsiTs102941Data
                    containing enrolmentRequest
                        containing tbsData
                            containing headerInfo
                                containing psid
                                  indicating AID_CERT_REQ
                                and containing generationTime
                                and not containing any other component
```

TP Id	SECPKI_ITS-S_ENR_09_BV
Summary	In the headerInfo of the tbsData of the outer EtsiTs103097Data-Signed 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 [8] and the generationTime shall be present
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.1
Configuration	CFG_ENR_ITS-S
PICS Selection	
Expected behaviour	

```
with
    the IUT being in the 'initialized' or 'enrolled' 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 tbsData
                    containing headerInfo
                        containing psid
                            indicating AID_CERT_REQ
                        and containing generationTime
                        and not containing any other component
```

TP Id	SECPKI_ITS-S_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
Configuration	CFG_ENR_ITS-S
PICS Selection	

Expected behaviour

```
with
    the IUT being in the 'initialized' or 'enrolled' state
ensure that
    when
        the IUT is requested to send an EnrolmentRequestMessage
    then
        the 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 (EKEY)
                    and containing encKey
                      being a symmetric key (SYMKEY) encrypted using the key EKEY
            containing ciphertext
                which is encrypted using the symmetric key SYMKEY contained in encKey
```

TP Id	SECPKI_ITS-S_ENR_11_BV
Summary	In the inner signed data structure (InnerECRequestSignedForPOP), the signature is computed on the tbsData containing the InnerECRequest using the private key corresponding to the verificationKey, containing in InnerECRequest, to prove the possession of the generated verification key pair
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.1
Configuration	CFG_ENR_ITS-S
PICS Selection	

Expected behaviour

```
with
    the IUT being in the 'initialized' or 'enrolled' 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 EtsiTs102941Data
                     containing enrolmentRequest
                         containing tbsData
                             containing InnerEcRequest
                                containing verificationKey (VKEY)
                         containing signature
                              computed on InnerECRequest
                                  using the private key corresponding to VKEY
                                     contained in InnerECRequest
```

TP Id	SECPKI_ITS-S_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, IEEE 1609.2™ [3], clause 6.4.28
Configuration	CFG_ENR_ITS-S
PICS Selection	PICS_SECPKI_REENROLMENT
Expected behaviour	

```
with
  the IUT being in the 'enrolled' 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 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 bitmapSsp [0] (version)
                      indicating 1
                    containing bitmapSsp [1] (value)
                      indicating 'Enrolment Request' (bit 1) set to 1
```

5.2.2.2 Enrolment response handling

TP Id	SECPKI_ITS-S_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_ITS-S
PICS Selection	
Expected behaviour	

```
with
  the IUT being in the X_STATE
  and the IUT has sent the EnrolmentRequestMessage
ensure that
  when
    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_ITS-S_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_ITS-S
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
    then
        the IUT switches to the 'enrolled' state
```

TP Id	SECPKI_ITS-S_ENR_RCV_03_BE
Summary	Check that IUT does not use EC for re-enrolment if this usage is not allowed by EC's application permissions (AID)
Reference	ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1, IEEE 1609.2™ [3], clause 6.4.28
Configuration	CFG_ENR_ITS-S
PICS Selection	PICS_SECPKI_REENROLMENT
Expected behaviour	

```
with
    the IUT being in the 'initialized' state
    and the IUT has sent an EnrolmentRequestMessage
    and the IUT has received an EnrolmentResponsetMessage
        containing certificate
            containing appPermissions
                not containing an item of type PsidSsp
                    containing psid
                        indicating AID_CERT_REQ
ensure that
    when
        the IUT is requested to send an EnrolmentRequestMessage
    then
        the IUT sends an initial enrolment request
```

TP Id	SECPKI_ITS-S_ENR_RCV_04_BE
Summary	Check that IUT does not use EC for re-enrolment if this usage is not allowed by EC's application permissions (SSP)
Reference	ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1, IEEE 1609.2™ [3], clause 6.4.28
Configuration	CFG_ENR_ITS-S
PICS Selection	PICS_SECPKI_REENROLMENT
Expected behaviour	

```
with
    the IUT being in the 'initialized' state
    and the IUT has sent an EnrolmentRequestMessage
    and the IUT has received an EnrolmentResponsetMessage
        containing certificate
            containing appPermissions
                containing an item of type PsidSsp
                    containing psid
                        indicating AID_CERT_REQ
                            and containing ssp
                                containing bitmapSsp[0] (version)
                                    indicating 1
                                and containing bitmapSsp [1] (value)
                                    indicating 'Enrolment Request' (bit 1) set to 0
ensure that
    when
        the IUT is requested to send an EnrolmentRequestMessage
    then
        the IUT sends an initial enrolment request
```

5.2.2.3 Enrolment request repetition

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

- PICS_SECPKI_ENROLMENT_RETRY = TRUE

TP Id	SECPKI_ITS-S_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_ITS-S
PICS Selection	
Expected behaviour	

```
with
    the IUT being in the 'initialized' state
    and the IUT already sent the Enrolment Request at the time T1
    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 to EA an EnrolmentRequestMessage
```

TP Id	SECPKI_ITS-S_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_ITS-S
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_ITS-S_ENR_REP_03_BV
Summary	Check that IUT stops sending the Enrolment Request message if Enrolment Response message has been received
Reference	ETSI TS 103 601 [6], clause 5.1.2
Configuration	CFG_ENR_ITS-S
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 Id	SECPKI_ITS-S_ENR_REP_04_BV
Summary	Check that IUT stops sending the Enrolment Request message if maximum number of retry has been reached
Reference	ETSI TS 103 601 [6], clause 5.1.2
Configuration	CFG_ENR_ITS-S
PICS Selection	
Expected behaviour	
with 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 Id	SECPKI_ITS-S_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_ITS-S
PICS Selection	
Expected behaviour	
with the IUT being in the 'initialized' state and the IUT has started sending the Enrolment Request at the time T1 ensure that when the IUT local time is reached the T1 + PIXIT_ENR_TIMEOUT_TH2 then the IUT stops sending an Enrolment Request messages	

TP Id	SECPKI_ITS-S_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_ITS-S
PICS Selection	
Expected behaviour	

```
with
    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_ITS-S_AUTH_01_BV
Summary	Check that the ITS-S sends the AuthorizationRequestMessage 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_ITS-S
PICS Selection	
Expected behaviour	

```
with
    the IUT in 'enrolled' state
    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-Encrypted to the AA
```

TP Id	SECPKI_ITS-S_AUTH_02_BV
Summary	Check that the AuthorizationRequestMessage is encrypted and sent to only one Authorization Authority
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITS-S
PICS Selection	

Expected behaviour

```
with
    the IUT in 'enrolled' state
    and the AA in 'operational' state
        authorized with CERT_IUT_A_AA certificate
ensure that
    when
        the IUT is triggered to request new Authorization Ticket (AT)
    then
        the IUT sends an 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_ITS-S_AUTH_03_BV
Summary	Check that the AuthorizationRequestMessage 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_ITS-S
PICS Selection	

Expected behaviour

```
with
    the IUT in 'enrolled' state
    and the AA in 'operational' state
        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
                        encrypted using symmetric key
                            been decrypted using AA_ENC_PUB_KEY
```

TP Id	SECPKI_ITS-S_AUTH_04_BV
Summary	Check that the authorization requests never reuses the same encryption key and nonce
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITS-S
PICS Selection	
Expected behaviour	

```
with
    the IUT in 'authorized' state
    and the IUT already sent one or more Authorization Requests
    and the AA in 'operational' state
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.aes128ccm.nonce
                    indicating value not equal to the nonce in N previous messages
                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_ITS-S_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_ITS-S
PICS Selection	
Expected behaviour	

```
with
    the IUT in 'enrolled' state
    and the AA in 'operational' 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 version
                    containing indicating 1
                containing content
                    containing authorizationRequest
```

TP Id	SECPKI_ITS-S_AUTH_06_BV
Summary	Check that for each authorization request the ITS-S generates a new verification key pair 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_ITS-S
PICS Selection	

Expected behaviour

```
with
    the IUT in 'enrolled' state
    and the AA in 'operational' 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 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
```

NOTE: N can be chosen according to implementations recommendations.

TP Id	SECPKI_ITS-S_AUTH_07_BV
Summary	Check that ITS-S sends Authorization request with a keyTag field computed as described in ETSI TS 102 941 [1], clause 6.2.3.3.1
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITS-S
PICS Selection	

Expected behaviour

```
with
    the IUT in 'enrolled' state
    and the AA in 'operational' 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 sharedAtRequest
                        containing keyTag
                            indicating properly calculated value
```

TP Id	SECPKI_ITS-S_AUTH_08_BV
Summary	Check that ITS-S sends Authorization request with eaId of EA certificate
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITS-S
PICS Selection	
Expected behaviour	

```
with
    the IUT is enrolled by the EC, signed with the CERT EA certificate
    and the AA in 'operational' stateensure 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 sharedAtRequest
                        containing eaId
                            indicating HashedId8 of CERT_ EA certificate
```

TP Id	SECPKI_ITS-S_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_ITS-S
PICS Selection	
Expected behaviour	

```
with
    the IUT in 'enrolled' state
    and the AA in 'operational' 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 sharedAtRequest
                        containing certificateFormat
                            indicating 1
```

TP Id	SECPKI_ITS-S_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_ITS-S
PICS Selection	
Expected behaviour	

```
with
    the IUT in 'enrolled' state
    and the AA in 'operational' 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 sharedAtRequest
                        containing requestedSubjectAttributes
                            containing appPermissions
                            and not containing certIssuePermissions
```

TP Id	SECPKI_ITS-S_AUTH_11_BV
Summary	Check that ITS-S sends Authorization request containing EC signature calculated over the sharedATRequest using supported hash algorithm
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITS-S
PICS Selection	
Expected behaviour	

```
with
    the IUT in 'enrolled' state
    and the AA in 'operational' 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
                        containing structure of type EtsiTs103097Data-SignedExternalPayload
                            containing tbsData
                                containing payload
                                    containing extDataHash
                                        indicating supported hash algorithm
                                        and indicating hash of sharedATRequest
```

TP Id	SECPKI_ITS-S_AUTH_12_BV
Summary	Check that the ecSignature psid is set to the proper ITS_AID Check that the ecSignature generation time is present
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITS-S
PICS Selection	
Expected behaviour	

```
with
    the IUT in 'enrolled' state
    and the AA in 'operational' 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
                        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_ITS-S_AUTH_13_BV
Summary	Check that ITS-S sends Authorization request containing EC signature with supported hash algorithm
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITS-S
PICS Selection	
Expected behaviour	

with
    the IUT in 'enrolled' state
    and the AA in 'operational' 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
                        containing structure of type EtsiTs103097Data-SignedExternalPayload
                            containing hashId
                                indicating supported hash algorithm	

TP Id	SECPKI_ITS-S_AUTH_14_BV
Summary	Check that the ecSignature of the Authorization request is signed with EC certificate 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_ITS-S
PICS Selection	
Expected behaviour	

with
    the IUT is enrolled with CERT_EC certificate
    and the AA in 'operational' 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
                        containing structure of type EtsiTs103097Data-SignedExternalPayload
                            containing signer
                                indicating HashedId8 of the CERT_EC certificate
                            containing signature
                                indicating signature over sharedATRequest calculated with CERT_EC verificationKey	

TP Id	SECPKI_ITS-S_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_ITS-S
PICS Selection	PICS_PKI_AUTH_PRIVACY

Expected behaviour

```
with
    the IUT in 'enrolled' state
    and the AA in 'operational' state
    and the EA in 'operational' state
        authorized with CERT_EA certificate
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
                        containing encryptedEcSignature
                            containing 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 containing cyphertext
                                containing encrypted representation
                                        of structure EtsiTs103097Data-SignedExternalPayload
```

=

TP Id	SECPKI_ITS-S_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_ITS-S
PICS Selection	NOT PICS_PKI_AUTH_PRIVACY

Expected behaviour

```
with
    the IUT in 'enrolled' state
    and the AA in 'operational' 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
                        containing ecSignature
```

TP Id	SECPKI_ITS-S_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_ITS-S
PICS Selection	NOT PICS_PKI_AUTH_POP

Expected behaviour

```
with
    the IUT in 'enrolled' state
    and the AA in 'operational' state
ensure that
    when
        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 Ieee1609Dot2Data
                containing content.unsecuredData
```

TP Id	SECPKI_ITS-S_AUTH_18_BV
Summary	Check that the Authorization request is signed when Prove of Possession is used 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_ITS-S
PICS Selection	PICS_PKI_AUTH_POP

Expected behaviour

```
with
    the IUT in 'enrolled' state
    and the AA in 'operational' state
ensure that
    when
        the IUT is triggered to request new Authorization Ticket (AT)
    then
        the IUT sends a EtsiTs103097Data-Encrypted to the AA
            containing cyphertext
                containing encrypted representation of the EtsiTs103097Data-Signed
                    containing content.signedData
                        containing hashId
                            indicating valid hash algorithm
                        and containing tbsData
                            containing headerInfo
                                containing psid
                                    indicating AID_PKI_CERT_REQUEST
                                and containing generationTime
                                and not containing any other headers
                        and containing signer
                            containing self
                        and containing signature
                            indicating value calculated over tbsData with the private key
                                correspondent to the verificationKey from this message
```

TP Id	SECPKI_ITS-S_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_ITS-S
PICS Selection	
Expected behaviour	

```
with
    the IUT in 'enrolled' state
    and the AA in 'operational' 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
                        containing structure of type EtsiTs103097Data-SignedExternalPayload
                            containing signer
                                indicating HashedId8 of EC certificate
                                  containing appPermissions
                                     containing an item of type PsidSsp
                                         containing psid
                                             indicating AID_CERT_REQ
                                         and containing ssp
                                             containing bitmapSsp[0] (version)
                                                 indicating 1
                                             containing bitmapSsp[1] (value)
                                                 indicating 'Enrolment Request' (bit 1) set to 1
```

5.2.3.2 Authorization response handling

Void.

5.2.3.3 Authorization request repetition

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

PICS_SECPKI_ AUTHORIZATION _RETRY = TRUE

TP Id	SECPKI_ITS-S_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_ITS-S
PICS Selection	
Expected behaviour	

```
with
    the IUT being in the 'enrolled' state
    and the IUT already sent the Authorization Request at the time T1
    and the IUT has not yet received the Authorization Response
ensure that
    when
        the IUT local time is reached the T1 + PIXIT_AUTH_TIMEOUT_TH1
    then
        the IUT sends to EA an AuthorizationRequestMessage
```

TP Id	SECPKI_ITS-S_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_AUTH_ITS-S
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_ITS-S_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_AUTH_ITS-S
PICS Selection	

Expected behaviour

```
with
    the IUT being in the 'enrolled' state
    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 Id	SECPKI_ITS-S_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_AUTH_ITS-S
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 sending Authorization Requests
```

TP Id	SECPKI_ITS-S_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_AUTH_ITS-S
PICS Selection	

Expected behaviour

```
with
    the IUT being in the 'enrolled' state
    and the IUT has started sending the Authorization Request at the time T1
ensure that
    when
        the IUT local time is reached the T1 + PIXIT_AUTH_TIMEOUT_TH2
    then
        the IUT stops sending an Authorization Request messages
```

5.2.3.4 Authorization using butterfly key expansion mechanism

5.2.3.4.1 Overview

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

PICS_SECPKI_ AUTH_BFK = TRUE

5.2.3.4.2 Butterfly authorization request

<table>
<tr><td><b>TP Id</b></td><td>SECPKI_ITS-S_ BFK_AUTH_01_BV</td></tr>
<tr><td><b>Summary</b></td><td>Check that the ITS-S sends the EtsiTs103097Data to the Enrolment Authority (EA) to request a batch of authorization tickets
Check that this message is encrypted and addressed to a single recipient.</td></tr>
<tr><td><b>Reference</b></td><td>ETSI TS 102 941 [1], clause 6.2.3.5.1</td></tr>
<tr><td><b>Configuration</b></td><td>CFG_BFK_AUTH_ITS-S</td></tr>
<tr><td><b>PICS Selection</b></td><td></td></tr>
<tr><td colspan="2"><b>Expected behaviour</b></td></tr>
<tr><td colspan="2">with
    the IUT in 'enrolled' state
    and the EA in 'operational' state
        authorized with enrolment certificate CERT_IUT_A_EA
ensure that
    when
        the IUT is triggered to request a new batch of authorization tickets
    then
        the IUT sends a EtsiTs103097Data to the EA
            containing content.encryptedData
                containing recipients
                    indicating size 1
                    and containing the instance of RecipientInfo
                        containing certRecipInfo
                            containing recipientId
                                indicating HashedId8 of the CERT_IUT_A_EA</td></tr>
</table>

TP Id	SECPKI_ITS-S_ BFK_AUTH_02_BV
Summary	Check that the ButterflyAuthorizationRequestMessage is signed using the EC certificate
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.2
Configuration	CFG_BFK_AUTH_ITS-S
PICS Selection	NOT PICS_SECPKI_ENROLMENT_X509

Expected behaviour

```
with
    the IUT in 'enrolled' state
        with certificate CERT_EC
            issued by CA authorized with CERT_IUT_A_EA
    and the EA in 'operational' state
        authorized with enrolment certificate CERT_IUT_A_EA
ensure that
    when
        the IUT is triggered to request a new batch of authorization tickets
    then
        the IUT sends a EtsiTs103097Data to the EA
            containing content.encryptedData.cipherText
                    containing encrypted representation of EtsiTs103097Data
                        containing signedData
                            containing tbsData
                                containing headerInfo
                                    containing psid
                                        indicating AID_PKI_CERT_REQUEST
                                    and containing generationTime
                                    and not containing any other field
                                and containing payload.data
                                    indicating EtsiTs102941Data
                                        containing version
                                            indicating '1'
                                        and containing content
                                            containing butterflyAuthorizationRequest
                                                indicating EeRaCertRequest
                                and containing signer
                                    containing digest
                                        indicating HashedId8 of the CERT_EC
```

TP Id	SECPKI_ITS-S_BFK_AUTH_02a_BV
Summary	Check that the ButterflyAuthorizationRequestMessage is signed using the X.509 EC certificate
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.2
Configuration	CFG_BFK_AUTH_ITS-S
PICS Selection	PICS_SECPKI_ENROLMENT_X509

Expected behaviour

```
with
    the IUT in 'enrolled' state
        with certificate CERT_ENR of form X.509
    and the EA in 'operational' state
        authorized with enrolment certificate CERT_IUT_A_EA
ensure that
    when
        the IUT is triggered to request a new batch of authorization tickets
    then
        the IUT sends a EtsiTs103097Data to the EA
            containing content.encryptedData.cipherText
                    containing encrypted representation of EtsiTs103097Data
                        containing signedX509CertificateRequest
                            containing encoded representation of the SignedX509CertificateRequest
                                containing tbsRequest
                                    indicating the EeRaCertRequest
                                containing signer
                                    containing the DER representation of the CERT_ENR
                                and containing signature
                                    calculated over the hashes of tbsRequest and signer
                                        using the private key correspondent to the CERT_ENR
```

TP Id	SECPKI_ITS-S_ BFK_ AUTH_03_BV
Summary	Check that the ButterflyAuthorizationRequestMessage contains all required elements
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.2
Configuration	CFG_BFK_AUTH_ITS-S
PICS Selection	
Expected behaviour	

with
    the IUT in 'enrolled' state
    and the EA is in 'operational' state
ensure that
    when
        the IUT is triggered to request a new batch of Authorization Tickets (AT)
    then
        the IUT sends to the EA a EtsiTs103097Data
            containing the EeRaCertRequest
                containing version
                    indicating '2'
                and containing generationTime
                    indicating current ITS timestamp
                and containing certificateType
                    indicating 'explicit"
                and containing tbsCert
                    containing id
                        indicating 'none'
                    and containing cracaId
                        indicating '000000'H
                    and containing crlSeries
                        indicating '0'
                and containing additionalParams
                    containing original
                    or containing unified	

NOTE: The EeRaCertRequest can be sent by IUT using approaches presented in SECPKI_ITS-S_AUTH_BFK_02_BV and SECPKI_ITS-S_AUTH_BFK_02a_BV.	

TP Id	SECPKI_ITS-S_ BFK_ AUTH_04_BV
Summary	Check that the ButterflyAuthorizationRequestMessage contains newlly generated caterpillar public key
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.2
Configuration	CFG_BFK_AUTH_ITS-S
PICS Selection	
Expected behaviour	
with the IUT in 'authorized' state and the IUT already sent one or more Butterfly Authorization Requests and the EA is in 'operational' state ensure that when the IUT is triggered to request a new batch of Authorization Tickets (AT) then the IUT sends to the EA an EtsiTs103097Data message containing the EeRaCertRequest containing tbsCert containing verifyKeyIndicator containing verificationKey containing public key not equal to the key was used in a previously sent Butterfly Authorization Requests and containing additionalParams containing original containing signingExpansion containing 16 byte string not equal to the value was used in a previously sent Butterfly Authorization Requests and containing encryptionKey containing public key not equal to the key was used in a previously sent Butterfly Authorization Requests containing encryptionExpansion containing 16 byte string not equal to the value was used in a previously sent Butterfly Authorization Requests or containing unified containing 16 byte string not equal to the value was used in a previously sent Butterfly Authorization Requests	
NOTE: The EeRaCertRequest can be sent by IUT using approaches presented in SECPKI_ITS-S_AUTH_BFK_02_BV and SECPKI_ITS-S_AUTH_BFK_02a_BV.	

5.2.3.4.3 Butterfly AT download request

TP Id	SECPKI_ITS-S_BFK_CERTDNL_01_BV
Summary	Check that IUT downloads the AT certificates batch after receiving of positive ButterflyAuthorizationResponse message
Reference	ETSI TS 102 941 [1], clauses 6.2.3.5.3 and 6.2.3.5.6
Configuration	CFG_BFK_AUTH_ITS-S
PICS Selection	

Expected behaviour

```
with
    the IUT being in the 'enrolled' state
    and the EA is in 'operational' state
    and the IUT has sent the ButterflyAuthorizationRequestMessage
ensure that
    when
        the IUT receives an EtsiTs102941Data as an answer of the EA
            containing butterflyAuthorizationResponse
                indicating RaEeCertInfo
                    containing generationTime
                        indicating GEN_TIME
                    and containing currentI
                        indicating VALUE_I
                    and containing requestHash
                        indicating REQ_HASH
                    and containing nextDlTime
                        indicating time between GEN_TIME and current time
    then
        the IUT sends the ButterflyAtDownloadRequestMessage
            containing butterflyAtDownloadRequest
                indicating EeRaDownloadRequest
                    containing generationTime
                        indicating value more than GEN_TIME
                    and containing filename
                        indicating string REQ_HASH + "_" + VALUE_I + ".zip"
```

5.2.4 CTL handling

TP Id	SECPKI_ITS-S_CTL_01_BV
Summary	Check that the IUT trusts 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 does not trust the CERT_RCA_NEW
    and the IUT has received the TLM CTL
        containing the CERT_RCA_NEW
ensure that
    when
        the IUT received a CAM
            signed with AT certificate
                signed with AA certificate
                    signed with CERT_RCA_NEW
    then
        the IUT accepts this CAM
```

TP Id	SECPKI_ITS-S_CTL_02_BV
Summary	Check that the IUT distrusts 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 CERT_RCA
    and the IUT has received the TLM CTL
        not containing the CERT_RCA
ensure that
    when
        the IUT received a CAM
            signed with AT certificate
                signed with AA certificate
                    signed with CERT_RCA
    then
        the IUT rejects this CAM
```

TP Id	SECPKI_ITS-S_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 trusting the CERT_RCA
    and the IUT does not have the CERT_AA_NEW
    and the IUT has received the RCA CTL
        containing the CERT_AA_NEW
        and issued 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 this CAM
```

TP Id	SECPKI_ITS-S_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 the TLM CTL
        containing nextUpdate
            indicating timestamp T1
        and containing CPOC URL
ensure that
    when
        the T1 < CURRENT TIME
    then
        the IUT sends a request to the CPOC for a new CTL
```

TP Id	SECPKI_ITS-S_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 this clause 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_ITS-S_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 Id	SECPKI_ITS-S_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.

<table>
<tr><td><b>TP Id</b></td><td colspan="3">SECPKI_ITS-S_CTLDIST_03_BV</td></tr>
<tr><td><b>Summary</b></td><td colspan="3">Check that the IUT is using the proper BTP port to broadcast the Delta CTL</td></tr>
<tr><td><b>Reference</b></td><td colspan="3">ETSI TS 103 601 [6], clause 5.4.4</td></tr>
<tr><td><b>Configuration</b></td><td colspan="3">CFG_CXL_P2P</td></tr>
<tr><td><b>PICS Selection</b></td><td colspan="3">UC-SEC-05.2, <b><i>X_PICS</i></b></td></tr>
<tr><td colspan="4" align="center"><b>Expected behaviour</b></td></tr>
<tr><td colspan="4">with
    the IUT is configured to support P2P <b><i>X_DISTRIBUTION</i></b> distribution
    and the IUT has received the Delta <b><i>X_DISTRIBUTION</i></b> message
ensure that
    when
        the IUT is triggered to broadcast the Delta <b><i>X_DISTRIBUTION</i></b> message
    then
        the IUT sends the <b><i>X_MESSAGE</i></b>
            using the BTP port 2014</td></tr>
<tr><td colspan="4" align="center"><b>Permutation table</b></td></tr>
<tr><td><b>X</b></td><td><b><i>X_DISTRIBUTION</i></b></td><td><b><i>X_MESSAGE</i></b></td><td><b><i>X_PICS</i></b></td></tr>
<tr><td>A</td><td>ECTL</td><td>TlmCertificateTrustListMessage</td><td>PICS_SECPKI_ECTL_BROADCAST</td></tr>
<tr><td>B</td><td>RootCA CTL</td><td>RcaCertificateTrustListMessage</td><td>PICS_SECPKI_CTL_BROADCAST</td></tr>
</table>

<table>
<tr><td><b>TP Id</b></td><td colspan="3">SECPKI_ITS-S_CTLDIST_04_BV</td></tr>
<tr><td><b>Summary</b></td><td colspan="3">Check that the IUT stops to redistribute the Delta CTL if another node is also sending it</td></tr>
<tr><td><b>Reference</b></td><td colspan="3">ETSI TS 103 601 [6], clause 5.3.1</td></tr>
<tr><td><b>Configuration</b></td><td colspan="3">CFG_CXL_P2P</td></tr>
<tr><td><b>PICS Selection</b></td><td colspan="3">UC-SEC-05.2</td></tr>
<tr><td colspan="4" align="center"><b>Expected behaviour</b></td></tr>
<tr><td colspan="4">with
    the IUT is configured to support P2P Delta <b><i>X_DISTRIBUTION</i></b> distribution
    and the IUT has started broadcasting the Delta <b><i>X_DISTRIBUTION</i></b> message
        signed with <b><i>X_CERTIFICATE</i></b>
        and containing ctlSequence (<b><i>SN</i></b>)
ensure that
    when
        the IUT has received the Delta <b><i>X_DISTRIBUTION</i></b>
            signed with <b><i>X_CERTIFICATE</i></b>
            and containing ctlSequence
                indicating value equal or higher than <b><i>SN</i></b>
    then
        the IUT stops broadfcasting the Delta <b><i>X_DISTRIBUTION</i></b>
            signed with <b><i>X_CERTIFICATE</i></b>
            and containing ctlSequence (<b><i>SN</i></b>)</td></tr>
<tr><td colspan="4" align="center"><b>Permutation table</b></td></tr>
<tr><td><b>X</b></td><td><b><i>X_DISTRIBUTION</i></b></td><td><b><i>X_CERTIFICATE</i></b></td><td><b><i>X_PICS</i></b></td></tr>
<tr><td>A</td><td>ECTL</td><td>CERT_TLM</td><td>PICS_SECPKI_ECTL_BROADCAST</td></tr>
<tr><td>B</td><td>RootCA CTL</td><td>CERT_IUT_A_RCA</td><td>PICS_SECPKI_CTL_BROADCAST</td></tr>
</table>

TP Id	SECPKI_ITS-S_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

```
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 ContributedExtensionBlock
                    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 Id	SECPKI_ITS-S_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 valid TLM or/and RootCA certificate (CERT)
    and the IUT contain the CERT CTL information
        containing ctlSequence
            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
            containing contributedExtensions
                containing an item of type ContributedExtensionBlock
                    containing  contributorId
                        indicating etsiHeaderInfoContributorId (2)
                    containing an item of type EtsiTs102941CtlRequest
                        containing issuerId
                            indicating HashedID8 of the CERT
                        and containing lastKnownCtlSequence
                            indicating SN
```

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

TP Id	SECPKI_ITS-S_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
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 contains the ***CERT*** CTL information
        containing ctlSequence
            indicating (***SN***)
ensure that
    when
        the IUT receives the Secured GN Message
            containing `contributedExtensions`
                containing an item of type `ContributedExtensionBlock`
                    containing `contributorId`
                        indicating `etsiHeaderInfoContributorId (2)`
                    containing an item of type `EtsiTs102941CtlRequest`
                        containing `issuerId`
                            indicating `HashedID8` of the ***CERT***
                        and containing `lastKnownCtlSequence`
                            indicating value higher than ***SN***
    then
        the IUT starts sending Secured GN messages
            containing `contributedExtensions`
                containing an item of type `ContributedExtensionBlock`
                    containing `contributorId`
                        indicating `etsiHeaderInfoContributorId (2)`
                    containing an item of type `EtsiTs102941CtlRequest`
                        containing `issuerId`
                            indicating `HashedID8` of the ***CERT***
                        and containing `lastKnownCtlSequence`
                            indicating ***SN***	

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

TP Id	SECPKI_ITS-S_CTLDIST_08_BV
Summary	Check that the IUT starts broadcasting the Delta CTL when request is received using P2P protocol
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 `ctlSequence`
            indicating (***SN***)
ensure that
    when
        the IUT receives 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***)	

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

TP Id	SECPKI_ITS-S_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 ***D1*** time and the IUT has started to broadcast a Delta CTL message at the time ***T*** 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 shall be provided as a PIXIT.	

<table>
<tr><td><b>TP Id</b></td><td>SECPKI_ITS-S_CTLDIST_10_BV</td></tr>
<tr><td><b>Summary</b></td><td>Check that the IUT stops broadcasting the requested Delta CTL when broadcasting period is expired</td></tr>
<tr><td><b>Reference</b></td><td>ETSI TS 103 601 [6], clause 5.3.6</td></tr>
<tr><td><b>Configuration</b></td><td>CFG_CXL_P2P</td></tr>
<tr><td><b>PICS Selection</b></td><td>UC-SEC-06.2</td></tr>
<tr><td colspan="2"><b>Expected behaviour</b></td></tr>
<tr><td colspan="2">with
 the IUT is configured to support P2P Delta CTL distribution
 and the IUT is configured to broadcast the requested Delta CTL during <b><i>D2</i></b> time
 and the IUT has started to broadcast a Delta CTL message
  at the time <b><i>T</i></b>
ensure that
 when
  the IUT local time is reached the <b><i>T + D2</i></b>
 then
  the IUT stops broadcasting the Delta CTL</td></tr>
<tr><td colspan="2">NOTE 1: This TP is applied for both: ECTL and RootCA CTL handling behaviour.
NOTE 2: The <b><i>D2</i></b> value shall be provided as a PIXIT.</td></tr>
</table>

5.2.6 CRL handling

<table>
<tr><td><b>TP Id</b></td><td>SECPKI_ITS-S_CRL_01_BV</td></tr>
<tr><td><b>Summary</b></td><td>Check that the IUT accept the received CRL information</td></tr>
<tr><td><b>Reference</b></td><td>ETSI TS 102 941 [1], clause 5.4.2</td></tr>
<tr><td><b>Configuration</b></td><td>CFG_CXL_P2P</td></tr>
<tr><td><b>PICS Selection</b></td><td></td></tr>
<tr><td colspan="2"><b>Expected behaviour</b></td></tr>
<tr><td colspan="2">with
 the IUT contains valid RootCA certificate (CERT_IUT_A_RCA)
 and the IUT has not received yet the CRL information issued by the RootCA
ensure that
 when
  the IUT received the CRL information from the DC
 then
  the IUT accepts the received CRL</td></tr>
</table>

<table>
<tr><td><b>TP Id</b></td><td>SECPKI_ITS-S_CRL_02_BV</td></tr>
<tr><td><b>Summary</b></td><td>Check that the IUT can handle the revocation of its own AA</td></tr>
<tr><td><b>Reference</b></td><td>ETSI TS 102 941 [1], clause 5.4.2</td></tr>
<tr><td><b>Configuration</b></td><td>CFG_CXL_P2P</td></tr>
<tr><td><b>PICS Selection</b></td><td></td></tr>
<tr><td colspan="2"><b>Expected behaviour</b></td></tr>
<tr><td colspan="2">With
 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</td></tr>
</table>

TP Id	SECPKI_ITS-S_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	

```
with
    the IUT is in 'authorized' state
    and the IUT contains valid RootCA certificate (CERT_IUT_A_RCA)
    and the IUT been enrolled with EC certificate
        signed with CERT_IUT_A_EA certificate
ensure that
    when
        the IUT the IUT received the CRL information from the DC
            containing revocation of CERT_IUT_A_EA
    then
        the IUT switches to the 'initial' state
```

TP Id	SECPKI_ITS-S_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 valid RootCA certificate (CERT_IUT_A_RCA)
    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 the 'initial' state
```

TP Id	SECPKI_ITS-S_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 contains valid RootCA certificate (CERT_IUT_A_RCA)
    and the IUT has not received yet the CRL information issued by the RootCA
    and the IUT is authorized using AT certificate
        signed with CERT_IUT_A_AA
    and the IUT contains another AA certificate (CERT_IUT_A_B_AA)
    and the IUT has already accepted messages signed with AT certificate
        signed with CERT_IUT_A_B_AA
    and the IUT received the CRL information from the DC
        containing revocation of CERT_IUT_A_B_AA
ensure that
    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 Id	SECPKI_ITS-S_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
    the IUT is configured to support P2P CRL distribution
    and the IUT contains valid RootCA certificate (CERT_IUT_A_RCA)
    and the IUT has not 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 Id	SECPKI_ITS-S_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	

with
    the IUT is configured to support P2P CRL distribution
    and the IUT contains valid RootCA certificate (CERT_IUT_A_RCA)
    and the IUT has not received yet the CRL information issued by the RootCA
ensure that
    when
        the IUT is triggered to broadcast the CRL
    then
        the IUT sends the `CertificateRevocationListMessage`
            using the BTP port 2015	

TP Id	SECPKI_ITS-S_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 valid RootCA certificate (CERT_IUT_A_RCA) and the IUT has already received the CRL information from DC at the time ***T*** and the IUT has started broadcasting the received CRL and the IUT is configured to limit the broadcasting time to ***D1*** ensure that when the IUT current time is equal or more than ***T + D1*** then the IUT stops broadcasting the CRL	
NOTE: The ***D1*** value shall be provided as a PIXIT.	

<table>
<tr><td><b>TP Id</b></td><td>SECPKI_ITS-S_CRLDIST_03_BV</td></tr>
<tr><td><b>Summary</b></td><td>Check that the IUT stops broadcasting the CRL when the CRL became outdated because of the nextUpdate value</td></tr>
<tr><td><b>Reference</b></td><td>ETSI TS 103 601 [6], clause 5.4.3</td></tr>
<tr><td><b>Configuration</b></td><td>CFG_CXL_P2P</td></tr>
<tr><td><b>PICS Selection</b></td><td>UC-SEC-07.2</td></tr>
<tr><td colspan="2" align="center"><b>Expected behaviour</b></td></tr>
<tr><td colspan="2">with
    the IUT is configured to support P2P CRL distribution
    and the IUT contains valid RootCA certificate (CERT_IUT_A_RCA)
    and the IUT has already received the CRL information from DC
        containing nextUpdate (<b><i>N</i></b>)
    and the IUT has started broadcasting the received CRL
ensure that
    when
        the IUT current time is equal or more than <b><i>N</i></b>
    then
        the IUT stops broadcasting the CRL</td></tr>
</table>

<table>
<tr><td><b>TP Id</b></td><td>SECPKI_ITS-S_CRLDIST_04_BV</td></tr>
<tr><td><b>Summary</b></td><td>Check that the IUT stops broadcasting the CRL when another station starts to broadcast the same or more recent CRL</td></tr>
<tr><td><b>Reference</b></td><td>ETSI TS 103 601 [6], clause 5.4.3</td></tr>
<tr><td><b>Configuration</b></td><td>CFG_CXL_P2P</td></tr>
<tr><td><b>PICS Selection</b></td><td>UC-SEC-07.2</td></tr>
<tr><td colspan="2" align="center"><b>Expected behaviour</b></td></tr>
<tr><td colspan="2">with
    the IUT is configured to support P2P CRL distribution
    and the IUT contains valid RootCA certificate (CERT_IUT_A_RCA)
    and the IUT has already received the CRL
        containing thisUpdate (<b><i>T</i></b>)
    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 greater than <b><i>T</i></b>
    then
        the IUT stops broadcasting the CRL</td></tr>
</table>

TP Id	SECPKI_ITS-S_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 valid RootCA certificate (CERT_IUT_A_RCA)
    and the IUT has never received 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
            containing contributedExtensions
                containing an item of type ContributedExtensionBlock
                    containing  contributorId
                        indicating etsiHeaderInfoContributorId (2)
                    containing an item of type EtsiTs102941CrlRequest
                        containing issuerId
                            indicating HashedID8 of the CERT_IUT_A_RCA
                        and not containing lastKnownUpdate
```

TP Id	SECPKI_ITS-S_CRLDIST_05_BV
Summary	Check that the IUT includes the lastKnownUpdate information in the P2P CRL request if 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
    the IUT is configured to support P2P CRL distribution
    and the IUT contains valid RootCA certificate (CERT_IUT_A_RCA)
    and the IUT has already received the CRL information issued by the RootCA
        containing thisUpdate (T)
ensure that
    when
        the IUT is triggered to request the CRL
    then
        the IUT starts sending Secured GN messages
            containing contributedExtensions
                containing an item of type ContributedExtensionBlock
                    containing  contributorId
                        indicating etsiHeaderInfoContributorId (2)
                    containing an item of type EtsiTs102941CrlRequest
                        containing issuerId
                            indicating HashedID8 of the CERT_IUT_A_RCA
                        and containing lastKnownUpdate
                            indicating T
```

<table>
<tr><td><b>TP Id</b></td><td>SECPKI_ITS-S_CRLDIST_06_BV</td></tr>
<tr><td><b>Summary</b></td><td>Check that the IUT starts broadcasting the CRL using P2P protocol when CRL information has been requested by another ITS station</td></tr>
<tr><td><b>Reference</b></td><td>ETSI TS 103 601 [6], clause 5.4.2</td></tr>
<tr><td><b>Configuration</b></td><td>CFG_CXL_P2P</td></tr>
<tr><td><b>PICS Selection</b></td><td>UC-SEC-08.2</td></tr>
<tr><td colspan="2"><b>Expected behaviour</b></td></tr>
<tr><td colspan="2">with
    the IUT is configured to support P2P CRL distribution
    and the IUT contains valid RootCA certificate (CERT_IUT_A_RCA)
    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 broadcasting the received CRL</td></tr>
</table>

<table>
<tr><td><b>TP Id</b></td><td>SECPKI_ITS-S_CRLDIST_06_BV</td></tr>
<tr><td><b>Summary</b></td><td>Check that the IUT stops broadcasting the CRL when distribution time (d2) has been expired after receiving of CRL request</td></tr>
<tr><td><b>Reference</b></td><td>ETSI TS 103 601 [6], clause 5.4.2</td></tr>
<tr><td><b>Configuration</b></td><td>CFG_CXL_P2P</td></tr>
<tr><td><b>PICS Selection</b></td><td>UC-SEC-08.2</td></tr>
<tr><td colspan="2"><b>Expected behaviour</b></td></tr>
<tr><td colspan="2">with
    the IUT is configured to support P2P CRL distribution
    and the IUT contains valid RootCA certificate (CERT_IUT_A_RCA)
    and the IUT has already received the CRL information request
        at the time <b><i>T</i></b>
    and the IUT has started broadcasting the CRL
    and the IUT is configured to limit the broadcasting time to <b><i>D2</i></b>
ensure that
    when
        the IUT current time is equal or more than <b><i>T+D1</i></b>
    then
        the IUT stops broadcasting the CRL</td></tr>
<tr><td colspan="2">NOTE: The <b><i>D1</i></b> value shall be provided as a PIXIT.</td></tr>
</table>

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 Id	SECPKI_CA_CERTGEN_01_BV
Summary	Check that the issuing certificate has version 3
Reference	ETSI TS 103 097 [2], clause 6 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 Id	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	PICS_GN_SECURITY AND 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 certificate
    then
        this certificate is of type EtsiTs103097Certificate
            containing version
                indicating 3
            and containing type
                indicating 'explicit'
            and containing toBeSigned
                containing verifyKeyIndicator
                    containing verificationKey
            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_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 AT certificate
                using the butterfly key expansion mechanism
    then
        this certificate is of type EtsiTs103097Certificate
            containing version
                indicating 3
            containing type
                indicating 'implicit'
            and containing toBeSigned
                containing verifyKeyIndicator
                    containing reconstructionValue
            and not containing signature
```

TP Id	SECPKI_CA_CERTGEN_02_BV_03
Summary	Check that the CA, been authorized using implicit 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' state
    CA is initialized with the implicit certificate (CERT_IUT_I_CA)
ensure that
    when
        the CA is requested to issue the AT certificate
                using the butterfly key expansion mechanism
    then
        this certificate is of type EtsiTs103097Certificate
            containing version
                indicating 3
            containing type
                indicating 'implicit'
            and containing toBeSigned
                containing verifyKeyIndicator
                    containing reconstructionValue
            and not containing signature
```

TP Id	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 IEEE Std 1609.2™ [3], clause 6.4.3
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_IMPLICIT_CERTIFICATES AND PICS_SEC_EXPLICIT_CERTIFICATES

Expected behaviour

```
with
    CA is in 'operational' 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 issue the certificate
```

TP Id	SECPKI_CA_CERTGEN_03_BV
Summary	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' state
ensure that
    when
        the CA is issuing the certificate
    then
        this certificate is of type EtsiTs103097Certificate
            containing toBeSigned
                containing id
                    indicating 'none' or 'name'
                and containing cracaId
                    indicating '000000'H
                and containing crlSeries
                    indicating '0'D
                and not containing certRequestPermissions
                and not containing canRequestRollover
```

TP Id	SECPKI_CA_CERTGEN_04_BV_X
Summary	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

```
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 X_ALGORITHM
                        referenced to certificate C_ISSUER
            and containing toBeSigned
                containing verifyKeyIndicator
                    containing verificationKey
                        containing X_KEY
```

Permutation table

X	***X_DIGEST***	***X_ALGORITHM***	***X_KEY***	***X_PICS***
A	sha256AndDigest	SHA-256	ecdsaNistP256 or ecdsaBrainpoolP256r1	PICS_SEC_SHA256 AND PICS_SEC_BRAINPOOL_P256R1
B	sha384AndDigest	SHA-384	ecdsaBrainpoolP384r1	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1

5.3.1.2 Check certificate region validity restriction

TP Id	SECPKI_CA_CERTGEN_05_BV
Summary	Check that the CA is able to issue the certificate with the well-formed circular region 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' state
    the CA is authorized with CA certificate
        containing toBeSigned
            containing region
                indicating REGION
ensure that
    when
        the CA is requested to issue the certificate
            containing circular region restriction
    then
        the CA issues the certificate of type EtsiTs103097Certificate
            containing toBeSigned
                containing region
                    containing circularRegion
                        containing centre
                            indicating a point inside the REGION
                        and containing radius
                            indicating a value when all points of the circle are inside the REGION
```

TP Id	SECPKI_CA_CERTGEN_06_BV
Summary	Check that the CA is able to issue the certificate with the well-formed rectangular region 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' state
    the CA is authorized with CA certificate
        containing toBeSigned
            containing region
                indicating REGION
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 containing southeast
                                indicating a point on the south and east from northwest
                                and inside the REGION
```

TP Id	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	

```
with
    CA is in 'operational' state
    the CA is authorized with CA certificate
        containing toBeSigned
            containing region
                indicating REGION
ensure that
    when
        the CA is requested to issue the certificate
            containing polygonal region validity restriction
    then
        the CA issues the certificate of type EtsiTs103097Certificate
            containing toBeSigned
                containing region
                    containing polygonalRegion
                        containing more than 2 items of type TwoDLocation
                            indicating points inside the REGION
                            and indicating unintercepting segments
```

TP Id	SECPKI_CA_CERTGEN_08_BV
Summary	Check that the CA is able to issue the certificate with identified region validity restriction 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 'operational' state
    the CA is authorized with CA certificate
        containing toBeSigned
            containing region
                indicating REGION
ensure that
    when
        the CA is requested to issue the certificate
            containing identified region validity restriction
                indicating country or area COUNTRY
    then
        the CA issued the certificate of type EtsiTs103097Certificate
            containing toBeSigned
                containing region
                    containing identifiedRegion
                        containing 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
                                containing country
                                    indicating integer representation of the identifier of country or area COUNTRY
```

TP Id	SECPKI_CA_CERTGEN_09_BV
Summary	Check that the identified region validity restriction of the subordinate certificate is included in the identified region validity restriction of the issuing certificate
Reference	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
    the CA is in 'operational' state
    and the CA is authorized with CA certificate
        containing toBeSigned
            containing region
                containing identifiedRegion
                    containing countryOnly
                        indicating COUNTRY
                    or containing countryAndRegions
                        containing countryOnly
                            indicating COUNTRY
                        and containing regions
                            indicating REGIONS
                    or containing countryAndSubregions
                        containing country
                            indicating COUNTRY
                        and containing regionAndSubregions
                            indicating REGIONS and SUBREGIONS
ensure that
    when
        the CA issued the certificate
            containing toBeSigned
                containing region
                    containing identifiedRegion
    then
        this certificate is of type EtsiTs103097Certificate
            containing toBeSigned
                containing region
                    containing identifiedRegion
                        containing countryOnly
                            indicating value = COUNTRY
                        or containing countryAndRegions
                            containing countryOnly
                                indicating value = COUNTRY
                            and containing regions
                                containing region identifiers contained in REGIONS
                        or containing countryAndSubregions
                            containing country
                                indicating value = COUNTRY
                            and containing regionAndSubregions
                                containing region identifiers contained in REGIONS
                                and containing subRegion identifiers contained in SUBREGIONS for every region
```

5.3.1.3 Check ECC point type of the certificate signature

TP Id	SECPKI_CA_ CERTGEN_10_BV_***XX***
Summary	Check that the certificate signature contains ECC point of type set to either compressed_lsb_y_0, compressed_lsb_y_1 or x_coordinate_only
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 explicit certificate
    then
        this certificate is of type EtsiTs103097Certificate
            containing signature
                containing X_SIGNATURE
                    containing rSig
                      containing x-only
                      or containing compressed-y-0
                      or containing compressed-y-1
```

Permutation table

XX	***X_SIGNATURE***	***X_PICS***
A	ecdsaNistP256Signature	
B	ecdsaBrainpoolP256r1Signature	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 Id	SECPKI_CA_CERTGEN_11_BV
Summary	Check that the certificate verification key contains ECC point of type set to either 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 AND PICS_SEC_EXPLICIT_CERTIFICATES AND ***X_PICS***

Expected behaviour

```
with
    the CA is in 'operational' state
ensure that
    when
        the CA issued the explicit certificate
    then
        this certificate is of type EtsiTs103097Certificate
            containing toBeSigned
                containing verifyKeyIndicator
                    containing verificationKey
                        containing X_KEY
                          containing uncompressed
                          or containing compressed-y-0
                          or containing compressed-y-1
```

Permutation table

XX	***X_KEY***	***X_PICS***
A	ecdsaNistP256	
B	ecdsaBrainpoolP256r1	PICS_SEC_BRAINPOOL_P256R1
C	ecdsaBrainpoolP384r1	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1

TP Id	SECPKI_CA_CERTGEN_12_BV
Summary	Check that the certificate encryption key contains ECC point of type set to either compressed_lsb_y_0, compressed_lsb_y_1 or uncompressed
Reference	IEEE Std 1609.2™ [3], clause 6.4.38
PICS Selection	PICS_GN_SECURITY

Expected behaviour

```
with
    the CA is in 'operational' 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	eciesBrainpoolP256r1	PICS_SEC_BRAINPOOL_P256R1

5.3.1.5 Verify certificate signatures

TP Id	SECPKI_CA_CERTGEN_13_BV_01
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 'operational' state
    and the CA is authorized with explicit certificate
        containing toBeSigned
            containing verifyKeyIndicator
                containing verificationKey
                    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 X_KEY
                                    indicating KEY
            and containing signature
                containing X_SIGNATURE
                    verifiable using KEY
```

Permutation table

XX	***X_KEY***	***X_SIGNATURE***	***X_PICS***
A	ecdsaNistP256	ecdsaNistP256Signature	
B	ecdsaBrainpoolP256r1	ecdsaBrainpoolP256r1Signature	PICS_SEC_BRAINPOOL_P256R1
C	ecdsaBrainpoolP384r1	ecdsaBrainpoolP384r1Signature	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1

TP Id	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 'operational' state
    and the CA is authorized with explicit certificate
        containing toBeSigned
            containing verifyKeyIndicator
                containing verificationKey
                    containing X_KEY
                        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
                            indicating VALUE
ensure that
    when
        the CA is calculated the digital signature
            using the private key associated with the CERT
    then
        this signature can be verified using public key
            reconstructed using VALUE and KEY
```

Permutation table

XX	***X_KEY***	***X_PICS***
A	ecdsaNistP256	
B	ecdsaBrainpoolP256r1	PICS_SEC_BRAINPOOL_P256R1
C	ecdsaBrainpoolP384r1	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1

5.3.1.6 Verify certificate permissions

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 certificate
            containing toBeSigned
                containing appPermissions
    then
        this certificate is of type EtsiTs103097Certificate
            containing toBeSigned
                containing appPermissions
                    containing items of type PsidSsp
                        containing psid
                            indicating unique values in this sequence
```

TP Id	SECPKI_CA_CERTGEN_15_BV
Summary	Check that all PSID entries of the appPermissions component of the certificate are also 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 certificate
            containing toBeSigned
                containing appPermissions
    then
        this certificate is of type EtsiTs103097Certificate
            containing issuer
                referenced to the certificate
                    containing toBeSigned
                        containing certIssuePermissions
                            containing items of type PsidGroupPermissions
                                containing eeType
                                    indicating app(0)
                                and containing subjectPermissions
                                    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
                        containing psid
                            contained 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 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 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 certificate
      containing toBeSigned
        containing appPermissions
  then
    this certificate is of type EtsiTs103097Certificate
      containing issuer
        referenced to the certificate
          containing toBeSigned
            containing certIssuePermissions
              containing items of type PsidGroupPermissions
                containing eeType
                  indicating app(0)
                and containing subjectPermissions
                  containing explicit
                    containing items of type PsidSspRange
                      containing psid
                        indicating X_PSID_AA
                      containing sspRange
                        indicating X_SSP_AA [X_PSID_AA]
                  or containing all
      containing toBeSigned
        containing appPermissions
          containing items of type PsidSsp
            containing psid
              indicating value equal to X_PSID_AA
            containing ssp
              indicating value permitted by X_SSP_AA [X_PSID_AA]
```

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' state
   and the CA is authorized with CA certificate
      containing toBeSigned
         containing validityPeriod
            containing start
               indicating X_START_VALIDITY_CA
            containing duration
               indicating X_DURATION_CA
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 EnrollmentResponse message shall be sent by the EA to the ITS-S across the interface at reference point S3 in response to a received EnrollmentRequest 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' state
ensure that
    when
        the IUT receives an EnrollmentRequestMessage
    then
        the IUT answers with an EnrollmentResponseMessage
        across the interface at reference point S3
```

TP Id	SECPKI_EA_ENR_RCV_02_BI
Summary	Check that EA does not accept Enrolment rekeying request when enrolment is not permitted by signing certificate
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 EnrollmentRequestMessage
            containing an encrypted EtsiTs103097Data-Signed
                containing signer
                  containing digest
                     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
        the IUT answers with an EnrollmentResponseMessage
          containing InnerECResponse
             containing responseCode
                indicating 'deniedpermissions'
```

TP Id	SECPKI_EA_ENR_RCV_04_BI
Summary	Enroll an ITS-Station, but the outer signature, created with the canonical private key, cannot 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 'operational' state
ensure that
    when
        the IUT receives an EnrollmentRequestMessage
            containing an outer signature
                signed with an unknown canonical private key
    then
        the IUT answers with an EnrollmentResponseMessage
          containing InnerECResponse
             containing responseCode
                indicating 'invalidsignature'
             and not containing a certificate
```

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 EnrollmentRequestMessage
            containing an InnerEcRequest
                containing Hostname
                    indicating an unknown canonical-ID
    then
        the IUT answers with an EnrollmentResponseMessage
          containing InnerECResponse
              containing responseCode
                  indicating unknownits'
              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 'operational' state
ensure that
    when
        the IUT receives an EnrollmentRequestMessage
            containing an InnerEcRequest
                containing SSP
                    indicating more permissions than EA allows
    then
        the IUT answers with an EnrollmentResponseMessage
          containing InnerECResponse
              containing responseCode
                  indicating 'deniedpermissions'
              and not containing a certificate
```

TP Id	SECPKI_EA_ENR_RCV_07_BI
Summary	Enroll the ITS-Station, but the CSR requests an 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
    when
        the IUT receives an EnrollmentRequestMessage
            containing an InnerEcRequest
                containing SSP
                    containing an AID permission not authorized by EA
    then
        the IUT answers with an EnrollmentResponseMessage
          containing InnerECResponse
              containing responseCode
                  indicating 'deniedpermissions'
              and not containing a certificate
```

TP Id	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 EnrollmentRequestMessage
            containing an InnerEcRequest
                containing ValidityPeriod
                    indicating end validity time
                        less than the start date of the EA
    then
        the IUT answers with an EnrollmentResponseMessage
          containing InnerECResponse
              containing responseCode
                  indicating 'deniedpermissions'
              and not containing a certificate
```

TP Id	SECPKI_EA_ENR_RCV_09_BI
Summary	Enroll the ITS-Station, but the start date of the CSR is before the start date of the EA
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 EnrollmentRequestMessage
            containing an InnerEcRequest
                containing ValidityPeriod
                    containing start date
                        indicating a value less than the start date of the EA
    then
        the IUT answers with an EnrollmentResponseMessage
          containing InnerECResponse
              containing responseCode
                  indicating 'deniedpermissions'
              and not containing 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 EnrollmentRequestMessage
            containing an InnerEcRequest
                containing ValidityPeriod
                    indicating a value greater than the ValidityPeriod of the EA
    then
        the IUT answers with an EnrollmentResponseMessage
          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 EnrollmentRequestMessage
            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 EnrollmentResponseMessage
          containing InnerECResponse
              containing responseCode
                  indicating 'deniedpermissions'
              and not containing a certificate
```

TP Id	SECPKI_EA_ENR_RCV_12_BI
Summary	Enroll the ITS-Station, but the lifetime of the EC would be greater than allowed (considering values in C-ITS CP [7])
Reference	ETSI TS 102 941 [1] and C-ITS CP [7], clause 7.2
Configuration	CFG_ENR_EA
PICS Selection	
Expected behaviour	

```
with
    the EA is in 'operational' state
ensure that
    when
        the IUT receives an EnrollmentRequestMessage
            containing an InnerEcRequest
                containing ValidityPeriod
                    indicating a value greater than 3 years
    then
        the IUT answers with an EnrollmentResponseMessage
          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, cannot be verified with the provided public key
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.1
Configuration	CFG_ENR_EA
PICS Selection	
Expected behaviour	

```
with
    the EA is in 'operational' state
ensure that
    when
        the IUT receives an EnrollmentRequestMessage
            containing an InnerEcRequest
                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 EnrollmentResponseMessage
          containing InnerECResponse
             containing responseCode
                indicating 'invalidsignature'
             and not containing a certificate
```

TP Id	SECPKI_EA_ENR_RCV_14_BV
Summary	Check that EA sends 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_ENROLLMENT_RETRY
Expected behaviour	

```
with
    the EA is in 'operational' state
    and the EA already received EnrollmentRequestMessage (REQ)
        having checksum (CS)
    and the EA has sent the EnrollmentResponseMessage (RES)
            containing responseCode
                indicating OK
ensure that
    when
        the IUT receives an EnrollmentRequestMessage
            having checksum
                indicating value equal to CS
    then
        the IUT answers with an EnrollmentResponseMessage
            indicating RES
```

TP Id	SECPKI_EA_ENR_RCV_15_BV
Summary	Check that EA does not accept enrolment when message generation time is too far in the past
Reference	ETSI TS 103 601 [6], clause 5.1.4
Configuration	CFG_ENR_EA
PICS Selection	PICS_SECPKI_ENROLLMENT_RETRY
Expected behaviour	

with
    the EA is in 'operational' state
    and the EA already received the EnrollmentRequestMessage (***REQ***)
        containing generationTime ***TG***
        and having checksum (**CS)**
ensure that
    when
        the IUT receives an EnrollmentRequestMessage
            at the moment ***TR2***
                indicating ***TR2*** > ***TG*** + ***PIXIT_EA_ENROLLMENT_TIMEOUT***
            and having checksum
                indicating value equal to ***CS***
    then
        the IUT answers with an EnrollmentResponseMessage
            containing responseCode
                indicating `deniedrequest`	

NOTE: PIXIT_EA_ENROLLMENT_TIMEOUT shall be set as a TP parameter.	

5.4.2 Enrolment response

TP Id	SECPKI_EA_ENR_01_BV
Summary	The EnrollmentResponse 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 EnrollmentRequest 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 EnrollmentRequestMessage
          containing encKey
              containing an encrypted AES key (SYMKEY)
    then
        the IUT answers with an EnrollmentResponseMessage
          containing cipherText
              being encrypted using SYMKEY
            and using an ETSI TS 103 097 [2] approved algorithm	

TP Id	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 EnrollmentRequest 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

```
ensure that
    when
        the IUT receives an EnrollmentRequestMessage
        and triggered to send the enrolment response
    then
        the IUT sends an EtsiTs103097Data-Encrypted structure
          containing recipients
              containing one instance of RecipientInfo of choice pskRecipInfo
                  containing the HashedId8 of the symmetric key used to encrypt the EnrollmentRequestMessage
          and containing cipherText
              being an encrypted EtsiTs103097Data-Signed structure
```

TP Id	SECPKI_EA_ENR_04_BV
Summary	The decrypted 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 EnrollmentResponseMessage as an answer for an EnrollmentRequestMessage
    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 publicVerificationKey found in the referenced EA certificate
```

TP Id	SECPKI_EA_ENR_05_BV
Summary	Within the headerInfo of the tbsData, the tbsData field of the decrypted EtsiTs103097Data-Signed structure shall contain the psid set to "secured certificate request" as assigned in ETSI TS 102 965 [8] and the generationTime
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 EnrollmentResponseMessage as an answer for an EnrollmentRequestMessage
    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
                   and not containing any other component of tbsData.headerInfo
```

TP Id	SECPKI_EA_ENR_07_BV
Summary	The EtsiTS102941Data shall contain the version set to v1 (integer value set to 1) and the 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 EnrollmentResponseMessage as an answer for an EnrollmentRequestMessage
    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)
```

TP Id	SECPKI_EA_ENR_08_BV
Summary	The InnerECResponse shall contain the requestHash, which is the left-most 16 octets of the SHA256 digest of the EtsiTs103097Data-Encrypted 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 EnrollmentResponseMessage as an answer for an EnrollmentRequestMessage
    then
        the IUT sends an EtsiTs103097Data-Encrypted structure
          containing an encrypted EtsiTs103097Data-Signed structure
              containing tbsData
                  containing EtsiTS102941Data
                    containing InnerECResponse
                        containing requestHash
                            indicating the left-most 16 octets of the SHA256 digest
                                of the topmost EtsiTs103097Data-Encrypted structure received in the request
                        and containing responseCode
```

TP Id	SECPKI_EA_ENR_09_BV
Summary	If the responseCode is 0, the InnerECResponse shall also contain an (enrollment) 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 EnrollmentResponseMessage
          containing a responseCode
             indicating 0
    then
        the IUT sends an EtsiTs103097Data-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 requested to send an EnrollmentResponseMessage
          containing a responseCode
             indicating a value different than 0
    then
        the IUT sends an EtsiTs103097Data-Encrypted structure
          containing an encrypted EtsiTs103097Data-Signed structure
             containing tbsData
                containing EtsiTS102941Data
                  containing InnerECResponse
                     not containing a certificate
```

TP Id	SECPKI_EA_ENR_11_BV
Summary	Check that signing of enrolment response 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 EnrollmentResponseMessage as an answer for an EnrollmentRequestMessage
    then
        the IUT sends an EtsiTs103097Data-Encrypted structure
          containing an encrypted EtsiTs103097Data-Signed structure
             containing signer
                declared as a digest
                  containing the HashedId8 of the EA 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 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
        the IUT is requested to send an EnrollmentResponseMessage
          containing a certificate (EC_CERT)
    then
        the EC_CERT
            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 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 containing an item of type PsidSsp
                    containing psid
                        indicating AID_CRL
```

5.4.3 Authorization validation request handling

TP Id	SECPKI_EA_AUTHVAL_RCV_01_BV
Summary	The authorization validation response shall be sent by the EA to the AA across the interface at reference point S4 in response to a received AuthorizationValidationRequestMessage
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 an AuthorizationValidationRequestMessage
    then
        the IUT sends a AuthorizationValidationResponseMessage
            across the reference point S4 to the AA
```

TP Id	SECPKI_EA_AUTHVAL_RCV_02_BI
Summary	Check that EA does not accept the 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 receives an AuthorizationValidationRequestMessage
            containing EtsiTs102941Data
              containing ecSignature
                  containing signer
                     containing 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
        the IUT answers with an AuthorizationValidationResponseMessage
          containing responseCode
             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 authorization request 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 ETSI TS 103 097 [2], clause 7
Configuration	CFG_AVALID_EA
PICS Selection	
Expected behaviour	

```
ensure that
    when
        the IUT receives a AuthorizationValidationRequestMessage
        containing encKey
          containing the encrypted symmetric data encryption key (SYMKEY)
    then
        the IUT sends a AuthorizationValidationResponseMessage
          containing EtsiTs103097Data-Encrypted
             containing recipients
                containing one instance of RecipientInfo of choice pskRecipInfo
                   indicating the HashedId8 of SYMKEY
             and containing ciphertext
                containing EtsiTs103097Data-Signed
                   being encrypted using SYMKEY and an ETSI TS 103 097 [2] approved algorithm
```

TP Id	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
        the IUT receives a AuthorizationValidationRequestMessage
    then
        the IUT sends a AuthorizationValidationResponseMessage
          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	

```
ensure that
    when
        the IUT receives a AuthorizationValidationRequestMessage
         containing EtsiTs103097Data-Signed structure (REQDSS)
    then
        the IUT sends a AuthorizationValidationResponseMessage
          containing EtsiTs103097Data-Signed
             containing EtsiTs102941Data
                containing authorizationValidationResponse
                   containing requestHash
                     indicating the left-most 16 octets of the SHA256 digest of REQDSS
                   and containing responseCode
```

TP Id	SECPKI_EA_AUTHVAL_04_BV
Summary	If the responseCode is 0, the AuthorizationValidationResponse structure contains the 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 receives a AuthorizationValidationRequestMessage
        and the IUT responds with a AuthorizationValidationResponseMessage
          containing authorizationValidationResponse
             containing responseCode
                indicating 0
    then
        the sent AuthorizationValidationResponseMessage
          contains an authorizationValidationResponse
             containing confirmedSubjectAttributes
                not containing certIssuePermissions
```

TP Id	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 AuthorizationValidationRequestMessage
        and the IUT responds with a AuthorizationValidationResponseMessage
          containing authorizationValidationResponse
              containing responseCode
                  indicating a value different than 0
    then
        the sent AuthorizationValidationResponseMessage
          contains an authorizationValidationResponse
              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 a AuthorizationValidationRequestMessage
    then
        the IUT sends a AuthorizationValidationResponseMessage
          containing EtsiTs103097Data-Signed
              containing EtsiTs102941Data
                  containing version
                      indicating v1 (integer value set to 1)
```

TP Id	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 [8] 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 AuthorizationValidationRequestMessage
    then
        the IUT sends a AuthorizationValidationResponseMessage
          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
Summary	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 6.2.3.4.2
Configuration	CFG_AVALID_EA
PICS Selection	
Expected behaviour	

```
ensure that
    when
        the IUT receives a AuthorizationValidationRequestMessage
    then
        the IUT sends a AuthorizationValidationResponseMessage
          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
                        corresponding to the publicVerificationKey found in the referenced EA certificate
```

TP Id	SECPKI_EA_AUTHVAL_09_BV
Summary	Check that signing of authorization validation response 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
        the IUT sends an EtsiTs103097Data-Encrypted structure
          containing an encrypted EtsiTs103097Data-Signed structure
              containing signer
                  containing digest
                    indicating HashedId8 of the EA 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
```

5.4.5 CA Certificate Request

TP Id	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 requested to send a CACertificateRequestMessage then the IUT sends a CACertificateRequestMessage across the reference point S10 to the RCA	

TP Id	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 ETSI TS 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 '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	

TP Id	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	

```
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
      being an EtsiTs103097Data-Signed structure
        containing hashId
          indicating the hash algorithm to be used
        and containing signer
          indicating 'self'
        and containing tbsData
          containing the EtsiTs102941Data structure
            containing caCertificateRequest
              containing publicKeys
                containing verification_key (VKEY)
        and containing signature
          computed over tbsData using the private key corresponding to the verificationKey (VKEY)
```

TP Id	SECPKI_EA_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 'initial' state
ensure that
  when
    the IUT is requested to send a CACertificateRequestMessage
  then
    the IUT sends a CACertificateRequestMessage
      containing caCertificateRequest
        containing publicKeys
          containing verification_key
          and containing 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 'initial' state
ensure that
    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 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 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
                containing requestedSubjectAttributes
                    as specified in ETSI TS 103 097 [2], clause 7.2.4.
```

TP Id	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 [8] 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 Id	SECPKI_EA_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 the 'operational' state
ensure that
    when
        the IUT is requested to perform a CA certificate rekeying procedure
        and SubCA certificate is no longer valid (due to end of validity or revocation)
    then
        the IUT switches to the ''initial' state
        and sends a CACertificateRequestMessage
```

TP Id	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 'operational' state
ensure that
    when
        the IUT is requested to perform a CA certificate rekeying procedure
    then
        the IUT sends a CACertificateRekeyingMessage
          being an EtsiTs103097Data-Signed structure
            containing hashId
                indicating the hash algorithm to be used
            and containing tbsData
            and containing signer
                containing digest
                  indicating HashedId8 of the SubCA certificate (CERT)
            and containing signature
                computed over tbsData
                  using the private key corresponding to CERT
```

TP Id	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 the 'operational' state
ensure that
    when
        the IUT is requested to perform a CA certificate rekeying procedure
    then
        the sends a CACertificateRekeyingMessage
          containing tbsData
            containing CaCertificateRequestMessage
```

TP Id	SECPKI_EA_CERTGEN_11_BV
Summary	The (outer) tbsData of the CACertificateRekeyingMessage shall contain a headerInfo containing psid and generationTime. The psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [8] 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 'operational' state
ensure that
  when
    the IUT is requested to perform a CA certificate rekeying procedure
  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
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_REKEY
PICS Selection	
Expected behaviour	

```
with
  the IUT being in the 'operational' state
ensure that
  when
    the IUT is requested to perform a CA certificate rekeying procedure
  then
    the sends a CACertificateRekeyingMessage
      being an EtsiTs103097Data-Signed structure
        and containing tbsData
          and containing signer
          containing digest
            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
                    containing opaque[1] (value)
                      indicating 'CA Certificate Response' (bit 6) set to 1
```

5.4.6 Authorization using butterfly key expansion mechanism

5.4.6.1 Butterfly authorization response

TP Id	SECPKI_EA_BFK_AUTH_01_BV
Summary	Check that the EA sends the butterfly authorization respond message after receiving of the butterfly authorization request Check that this message is signed with EA certificate
Reference	ETSI TS 102 941 [1], clauses 6.2.3.5.1 and 6.2.3.5.3
Configuration	CFG_BFK_AUTH_EA
PICS Selection	
Expected behaviour	

```
with
    the EA in 'operational' state
        authorized with CERT_EA certificate
    and the ITS-S in 'enrolled' state
ensure that
    when
        the IUT received the ButterflyAuthorizationRequestMessage
    then
        the IUT sends an EtsiTs103097Data to the ITS-S
            containing content.signedData
                containing tbsData
                    containing headerInfo
                        containing psid
                            indicating AID_PKI_CERT_REQUEST
                        and containing generationTime
                        and not containing any other field
                    and containing payload.data
                        indicating EtsiTs102941Data
                            containing version
                                indicating '1'
                            and containing content
                                containing butterflyCertificateResponse
                    and containing signer
                        containing digest
                            indicating HashedId8 of the CERT_EA
                and containing signature
                    validated using CERT_EA verification public key
```

TP Id	SECPKI_EA_BFK_AUTH_02_BV
Summary	Check that the butterfly authorization respond message, sent by EA, contains all necessary fields
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.3
Configuration	CFG_BFK_AUTH_EA
PICS Selection	
Expected behaviour	

```
with
    the EA in 'operational' state
        authorized with CERT_EA certificate
    and the ITS-S in 'enrolled' state
ensure that
    when
        the IUT received the ButterflyAuthorizationRequestMessage (REQ)
    then
        the IUT sends to the ITS-S a ButterflyAuthorizationResponseMessage
            containing butterflyCertificateResponse
                        indicating RaEeCertInfo
                            containing version
                                indicating 2
                            and containing generationTime
                                indicating value between REQ_TIME and the current time
                            and containing currentI
                            and containing requestHash
                                indicating the left-most 16 octets of the SHA256 digest of the REQ
                            and containing nextDlTime
                            and not containing acpcTreeId
```

5.4.6.2 Butterfly certificate request

TP Id	SECPKI_EA_BFK_AUTH _03_BV
Summary	Check that the EA sends butterfly certificate request message after receiving of the butterfly authorization request Check that this message is encrypted for the AA Check that this message is signed with the EA certificate
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.4
Configuration	CFG_BFK_AUTH_EA
PICS Selection	
Expected behaviour	

```
with
    the EA in 'operational' state
        authorized with CERT_EA certificate
    and the AA is emulated by TS and
        authorized with CERT_AA certificate
    and EA is configured to use emulated AA to generate certificates
ensure that
    when
        the IUT received the ButterflyAuthorizationRequestMessage
            containing EtsiTs102941Data
                containing content.butterflyAuthorizationRequest
    then
        the IUT sends a EtsiTs103097Data to the AA
            containing content.encryptedData
                containing recipients
                    indicating size 1
                    and containing the instance of RecipientInfo
                        containing certRecipInfo
                            containing recipientId
                                indicating HashedId8 of the CERT_AA
                containing encrypted representation of EtsiTs103097Data
                    containing signedData
                        containing tbsData
                            containing headerInfo
                                containing psid
                                    indicating AID_PKI_CERT_REQUEST
                                and containing payload.data
                                    indicating EtsiTs102941Data
                                        containing version
                                            indicating '1'
                                        and containing content
                                            containing butterflyCertificateRequest
                                and containing signer
                                    containing digest
                                        indicating HashedId8 of the CERT_EA
```

TP Id	SECPKI_EA_ BFK_ AUTH_04_BV
Summary	Check that the butterfly certificate request message sent by EA to AA contains all required elements
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.4
Configuration	CFG_BFK_AUTH_EA
PICS Selection	
Expected behaviour	

```
with
    the EA in 'operational' state
        authorized with CERT_EA certificate
    and the EA already received the ButterflyAuthorizationRequestMessage
        indicating the sha256 message hash MSG_HASH
    and the EA already responded with ButterflyAuthorizationResponseMessage
        containing EtsiTs102941Data
            containing butterflyAuthorizationResponse
                containing nextDlTime
                    indicating DNL_TIME
ensure that
    when
        the IUT received the ButterflyAtDownloadRequestMessage
            containing EtsiTs102941Data
                containing butterflyAtDownloadRequest
                    indicating EeRaCertRequest
                        containing generationTime
                            indicating REQ_TIME
    then
        the IUT sends to the AA the ButterflyCertRequestMessage
            containing EtsiTs102941Data
                containing content
                    containing butterflyCertificateRequest
                        indicating RaAcaCertRequest
                            containing version
                                indicating 2
                            and containing generationTime
                                indicating value between REQ_TIME and the current time
                            and containing flags
                                indicating empty bit string
                            and containing certEncKey
                            and containing tbsCert
                            and not containing linkageInfo
```

TP Id	SECPKI_EA_BFK_AUTH_05_BV
Summary	Check that the butterfly certificate request message contains expanded cocoon key
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.4
Configuration	CFG_BFK_AUTH_EA
PICS Selection	
Expected behaviour	

```
with
    the EA in 'operational' state
        authorized with CERT_EA certificate
    and the AA in 'operational' state
        authorized with CERT_AA certificate
    and EA is configured to use AA of the current configuration to generate certificates
ensure that
    when
        the IUT received the ButterflyAuthorizationRequestMessage
            containing EtsiTs102941Data
                containing content.butterflyAuthorizationRequest
                    indicating EeRaCertRequest
                        containing tbsCert (TBS_CERT)
                            containing verification key (CATERPILLAR_KEY)
    then
        the IUT sends to the AA the ButterflyCertRequestMessage
            containing EtsiTs102941Data
                containing content
                    containing butterflyCertificateRequest
                        indicating RaAcaCertRequest
                            and containing tbsCert
                                containing verificationKey
                                    containing "cocoon" key
                                        derived from the CATERPILLAR_KEY
```

5.4.6.3 Authorization certificate download

TP Id	SECPKI_EA_BFK_AUTH_06_BV
Summary	Check that the butterfly certificate request message sent by EA to AA contains all required elements
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.4
Configuration	CFG_BFK_AUTH_EA
PICS Selection	
Expected behaviour	

```
with
    the EA in 'operational' state
        authorized with CERT_EA certificate
    and the EA already responded with ButterflyAuthorizationResponseMessage (MSG_RESPONSE)
        containing EtsiTs102941Data
            containing butterflyAuthorizationResponse
                containing nextDlTime
                    indicating DNL_TIME
                and containing currentI
                    indicating I_VALUE
                and containing requestHash
                    indicating MSG_HASH
    and the EA already received from emullated AA one or more ButterflyCertResponse messages
        containing AcaEeCertResponsePrivateSpdu (CERT_RESPONSE)
ensure that
    when
        the IUT received the ButterflyAtDownloadRequestMessage
            containing EtsiTs102941Data
                containing butterflyAtDownloadRequest
                    indicating EeRaDownloadRequest
                        containing generationTime
                            indicating DNL_TIME + 1
                        and containing filename
                            indicating MSG_HASH + "_" + hex(I_VALUE) + ".zip"
    then
        the IUT sends the requested batch of certificates
            containing file hex(I_VALUE) + ".info"
                indicating COER encoding of MSG_RESPONSE
            and containing a set of files hex(I_VALUE) + "_" + (0..N)
                indicating COER encoding of AcaEeCertResponsePrivateSpdu (CERT_RESPONSE)
```

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
Summary	Check that the AA is able to decrypt the AuthorizationRequestMessage using the encryption private key corresponding to the recipient certificate Check that the AA is able to verify the inner signature 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

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 receives the EtsiTs103097Data-Encrypted message
            containing content.encryptedData
                containing recipients
                    containing the instance of RecipientInfo
                        containing 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 encrypted representation of the EtsiTs103097Data-Signed
                        containing content.signedData
                            containing hashId
                                indicating valid hash algorithm
                        and containing signer
                            containing self
                        and containing tbsData (SIGNED_DATA)
                            containing payload
                                containing EtsiTs102941Data
                                    containing content.authorizationRequest
                                        containing publicKeys.verificationKey (V_KEY)
                                        and containing hmacKey (HMAC)
                                        and containing sharedAtRequest
                                            containing keyTag (KEY_TAG)
                                            and containing eaId (EA_ID)
                                                indicating HashedId8 of the known EA certificate
                        and containing signature (SIGNATURE)
    then
        the IUT is able to decrypt the S_KEY
            using the private key
                corresponding to the AA_ENC_PUB_KEY
        and the IUT is able to decrypt the cyphertext ENC_DATA
            using the S_KEY
        and the IUT is able to verify the signature over the SIGNED_DATA
            using the V_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 EA_ID
```

TP Id	SECPKI_AA_AUTH_RCV_02_BV
Summary	Check that the AA is able to decrypt the AuthorizationRequestMessage using the encryption private key corresponding to the recipient certificate 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	NOT PICS_PKI_AUTH_POP
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 receives the EtsiTs103097Data-Encrypted message
            containing content.encryptedData
                containing recipients
                    containing the instance of RecipientInfo
                        containing 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 eaId (EA_ID)
                                    indicating HashedId8 of the known EA certificate
    then
        the IUT is able to decrypt the S_KEY
            using the private key
                corresponding to the AA_ENC_PUB_KEY
        and the IUT is able to decrypt the cyphertext ENC_DATA
            using the S_KEY
        and the IUT is able to verify integrity of HMAC and KEY_TAG
        and the IUT sends the AuthorizationValidationRequestMessage to the EA
            identified by the EA_ID
```

TP Id	SECPKI_AA_AUTH_RCV_03_BI
Summary	Check that the AA skips the authorization request 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' state
        authorized with the certificate CERT_AA
            containing encryptionKey (AA_ENC_PUB_KEY)
ensure that
    when
        the IUT receives the EtsiTs103097Data message
            containing content.encryptedData
                containing recipients
                    containing only one instance of RecipientInfo
                        containing certRecipInfo
                            containing recipientId
                                indicating value
                                    NOT equal to the 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
    then
        the IUT does not send the AuthorizationValidationRequestMessage
```

TP Id	SECPKI_AA_AUTH_RCV_04_BI
Summary	Check that the AA skips the authorization request if it is unable to decrypt the encKey
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' state
        authorized with the certificate CERT_AA
            containing encryptionKey (AA_ENC_PUB_KEY)
ensure that
    when
        the IUT receives the EtsiTs103097Data message
            containing content.encryptedData
                containing recipients
                    containing the instance of RecipientInfo
                        containing 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 send the AuthorizationValidationRequestMessage
```

TP Id	SECPKI_AA_AUTH_RCV_05_BI
Summary	Check that the AA skips the authorization request if it is 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' state
        authorized with the certificate CERT_AA
            containing encryptionKey (AA_ENC_PUB_KEY)
ensure that
    when
        the IUT receives the EtsiTs103097Data message
            containing content.encryptedData
                containing recipients[0].encKey
                    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 AuthorizationValidationRequestMessage to the correspondent EA
```

TP Id	SECPKI_AA_AUTH_RCV_06_BI
Summary	Check that the AA rejects the authorization request if it is unable to verify the POP signature
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS_PKI_AUTH_POP

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 receives the EtsiTs103097Data message
            containing content.encryptedData.cyphertext
                containing encrypted representation of the EtsiTs103097Data-Signed (SIGNED_DATA)
                    containing content.signedData
                        containing tbsData
                            containing payload
                                containing EtsiTs102941Data
                                    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 not send the AuthorizationValidationRequestMessage
        and the IUT sends to the TS the AuthorizationResponseMessage
            containing authorizationResponse
                containing requestHash
                    indicating the leftmost 16 bits of the SHA256 value
                        calculated over the SIGNED_DATA
                and containing responseCode
                    indicating the value NOT EQUAL to 0
                and not containing certificate
```

TP Id	SECPKI_AA_AUTH_RCV_07_BI
Summary	Check that the AA rejects the authorization request if it is 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 receives 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 AuthorizationResponseMessage
            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	EtsiTs103097Data-Signed
2	NOT PICS_PKI_AUTH_POP	EtsiTs102941Data

TP Id	SECPKI_AA_AUTH_RCV_08_BI
Summary	Send a correctly encoded AT request, but the ITS-Station is not enrolled at the EA
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS_PKI_AUTH_POP

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 receives the AuthorizationRequestMessage
            containing ecSignature
                containing Signer
                    indicating an unknown EC hashedId8 value
    then
        and the IUT does not send the AuthorizationValidationRequestMessage
        and the IUT sends to the TS the AuthorizationResponseMessage
            containing authorizationResponse
                containing responseCode
                    indicating the value 'unknownits'
                and not containing certificate
```

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
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 receives the AuthorizationRequestMessage
            containing SharedAtRequest
                containing eaId
                    indicating an unknown value
    then
        and the IUT does not send the AuthorizationValidationRequestMessage
        and the IUT sends to the TS the AuthorizationResponseMessage
            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 later then preloading period of AT certificates
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1, C-ITS CP [7], clause 7.2.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS_PKI_AUTH_POP
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 receives the AuthorizationRequestMessage
            containing POP signature
                containing tbsData
                    containing generationTime
                        indicating a value later then PIXIT_AT_PRELOADING_PERIOD in the past
    then
        and the IUT does not send the AuthorizationValidationRequestMessage
        and the IUT sends to the TS the AuthorizationResponseMessage
            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

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 receives the AuthorizationRequestMessage
            containing POP signature
                containing tbsData
                    containing generationTime
                        indicating a value in the future
    then
        and the IUT does not send the AuthorizationValidationRequestMessage
        and the IUT sends to the TS the AuthorizationResponseMessage
            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

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 receives the AuthorizationRequestMessage
            containing SharedAtRequest
                containing requestedSubjecAttributes
                    containing ValidityPeriod
                        indicating a time range ending before the starting time of the EC
    then
        and the IUT does not send the AuthorizationValidationRequestMessage
        and the IUT sends to the TS the AuthorizationResponseMessage
            containing authorizationResponse
                containing responseCode
                    indicating the value 'deniedpermissions'
                and not containing certificate
```

TP Id	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

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 receives the AuthorizationRequestMessage
            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 AuthorizationValidationRequestMessage
        and the IUT sends to the TS the AuthorizationResponseMessage
            containing authorizationResponse
                containing responseCode
                    indicating the value 'deniedpermissions'
                and not containing certificate
```

TP Id	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

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 receives the AuthorizationRequestMessage
            containing SharedAtRequest
                containing requestedSubjecAttributes
                    containing ValidityPeriod
                        indicating a value greater than the ValidityPeriod of the EC
    then
        and the IUT does not send the AuthorizationValidationRequestMessage
        and the IUT sends to the TS the AuthorizationResponseMessage
            containing authorizationResponse
                containing responseCode
                    indicating the value 'deniedpermissions'
                and not containing certificate
```

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

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 receives the AuthorizationRequestMessage
            containing SharedAtRequest
                containing requestedSubjecAttributes
                    containing ValidityPeriod
                        containing start date
                            indicating a value greater than the start date of the EC
    then
        and the IUT does not send the AuthorizationValidationRequestMessage
        and the IUT sends to the TS the AuthorizationResponseMessage
            containing authorizationResponse
                containing responseCode
                    indicating the value 'deniedpermissions'
                and not containing certificate
```

TP Id	SECPKI_AA_AUTH_RCV_16_BI
Summary	Send an AT request, but the expiry date of the CSR is after now + maximum preloading period (considering values in C-ITS CP [7])
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1, C-ITS CP [7], clause 7.2.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS_PKI_AUTH_POP

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 receives the AuthorizationRequestMessage
            containing SharedAtRequest
                containing requestedSubjecAttributes
                    containing ValidityPeriod
                        containing start date
                            indicating the current date
                        and a duration
                            indicating value grater then PIXIT_AT_PRELOADING_PERIOD
    then
        and the IUT does not send the AuthorizationValidationRequestMessage
        and the IUT sends to the TS the AuthorizationResponseMessage
            containing authorizationResponse
                containing responseCode
                    indicating the value 'deniedpermissions'
                and not containing certificate
```

NOTE: **PIXIT_AT_PRELOADING_PERIOD** shall be set as a TP parameter.

TP Id	SECPKI_AA_AUTH_RCV_17_BV
Summary	Check that AA sends 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 received AuthorizationRequestMessage (REQ)
        having checksum (CS)
    and the AA has sent the AuthorizationResponseMessage (RES)
        containing responseCode
            indicating OK
ensure that
    when
        the IUT receives an AuthorizationRequestMessage
            having checksum
                indicating value equal to CS
    then
        the IUT answers with an AuthorizationResponseMessage
            indicating RES
```

TP Id	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 'operational' state
    and the AA already received the AuthorizationRequestMessage (REQ)
        containing generationTime TG
        and having checksum (CS)
ensure that
    when
        the IUT receives an AuthorizationRequestMessage
            at the moment TR2
                indicating TR2 > TG + PIXIT_AA_AUTH_TIMEOUT
            and having checksum
                indicating value equal to CS
    then
        the IUT answers with an AuthorizationResponseMessage
            containing responseCode
                indicating deniedrequest
```

NOTE: PIXIT_AA_AUTH_TIMEOUT shall be set as a TP parameter.

5.5.2 Authorization validation request

TP Id	SECPKI_AA_AUTHVAL_01_BV
Summary	Check that the AA sends authorization validation request after receiving of the authorization request
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' state
        authorized with CERT_EA certificate
ensure that
    when
        the IUT received the AuthorizationRequestMessage
            containing EtsiTs102941Data
                containing content.authorizationRequest
                    containing sharedAtRequest
                        containing eaId (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
Summary	Check that the AuthorizationValidationRequestMessage is encrypted using approved algorithm and sent to only one EA
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' state
        authorized with CERT_EA certificate
ensure that
    when
        the IUT is triggered to send the authorization validation request to the EA
    then
        the IUT sends a EtsiTs103097Data-Encrypted
            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
```

TP Id	SECPKI_AA_AUTHVAL_03_BV
Summary	Check that the AA sends authorization validation request 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' state
        authorized with CERT_AA certificate
    and the EA in 'operational' state
ensure that
    when
        the IUT is triggered to send the authorization validation request to the EA
    then
        the IUT sends a EtsiTs103097Data-Encrypted message
            containing EtsiTs103097Data-Signed
                containing signedData
                    containing signer
                        containing digest
                            indicating HashedId8 value of the CERT_AA
```

TP Id	SECPKI_AA_AUTHVAL_04_BV
Summary	Check that the AA sends signed authorization validation request 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' state
        authorized with CERT_AA certificate
            containing verificationKey (AA_PUB_V_KEY)
    and the EA in 'operational' state
        authorized with CERT_EA certificate
ensure that
    when
        the IUT is triggered to send the authorization validation request to the EA
    then
        the IUT sends a EtsiTs103097Data-Encrypted message
            containing EtsiTs103097Data-Signed
                containing signedData
                    containing hashId
                        indicating supported hash algorithm (HASH_ALG)
                    and containing signature
                        calculated 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 AuthorizationValidationRequestMessage 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' state
        authorized with CERT_AA certificate
            containing verificationKey (AA_PUB_V_KEY)
    and the EA in 'operational' state
        authorized with CERT_EA certificate
ensure that
    when
        the IUT is triggered to send the authorization validation request to the EA
    then
        the IUT sends a EtsiTs103097Data-Encrypted message
            containing EtsiTs103097Data-Signed
                containing signedData
                    containing tbsData
                        containing headerInfo
                            containing psid
                                indicating AID_PKI_CERT_REQUEST
                            and containing generationTime
                            and not containing any other headers
```

TP Id	SECPKI_AA_AUTHVAL_06_BV
Summary	Check that the AA sends AuthorizationValidationRequestMessage 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' state
ensure that
    when
        the IUT is triggered to send the authorization validation request to the EA
    then
        the IUT sends a EtsiTs103097Data-Encrypted message
            containing EtsiTs102941Data
                containing version
                    indicating 1
```

TP Id	SECPKI_AA_AUTHVAL_07_BV
Summary	Check that the AA sends the AuthorizationValidationRequestMessage with `sharedAtRequest` and `ecSignature` as it was requested in the triggering of authorization request
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' state
    and the EA in 'operational' state
ensure that
    when
        the IUT received the AuthorizationRequestMessage
            containing EtsiTs102941Data
                containing content.authorizationRequest
                    containing sharedAtRequest (SHARED_AT_REQUEST)
                    and containing ecSignature (EC_SIGNATURE)
    then
        the 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 is permitted by the AA certificate
Reference	ETSI TS 102 941 [1], clause B.5
Configuration	CFG_AUTH_AA
PICS Selection	
Expected behaviour	

with
    the AA in 'operational' state
    and the EA in 'operational' state
ensure that
    when
        the IUT is triggered to send the authorization validation request to the EA
    then
        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 the authorization response after receiving the AuthorizationRequestMessage
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
Configuration	CFG_AUTH_AA
PICS Selection	
Expected behaviour	

```
with
    the ITS-S in 'enrolled' state
    the EA in 'operational' state
    and the IUT(AA) in 'operational' state
    and the IUT had received the AuthorizationRequestMessage from the ITS-S
    and the IUT sent the AuthorizationValidationRequestMessage
ensure that
    when
        the IUT received the AuthorizationValidationResponseMessage
    then
        the IUT sends the EtsiTs103097Data message to the ITS-S
```

TP Id	SECPKI_AA_AUTHVAL_RCV_02_BI
Summary	Check that AA does not accept the authorization validation response when the AuthorizationValidationResponseMessage 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 ITS-S in 'enrolled' state
    the EA in 'operational' state
    and the IUT(AA) in 'operational' state
    and the IUT had received the AuthorizationRequest from the ITS-S
    and the IUT sent the AuthorizationValidationRequest
ensure that
    when
        the IUT receives the AuthorizationValidationResponseMessage
          containing signer
             containing digest
                indicating HashedId8 of the 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 'AuthorizationValidationResponse' (bit 4) set to 0
    then
        the IUT answers with an AuthorizationValidationResponseMessage
          containing responseCode
             indicating non-zero value
```

5.5.4 Authorization response

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

```
with
    the ITS-S 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 ITS-S
    then
        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 authorization response
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
Configuration	CFG_AUTH_AA
PICS Selection	
Expected behaviour	

```
with
    the ITS-S 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 ITS-S
    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
```

TP Id	SECPKI_AA_AUTH_03_BV
Summary	Check that the AA sends signed authorization response 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 ITS-S in 'enrolled' state
    and the IUT(AA) in 'operational' state
        authorized with CERT_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 ITS-S
    then
        and the IUT sends the EtsiTs103097Data-Encrypted message
            containing the EtsiTs103097Data-Signed
                containing signedData
                    containing hashId
                        indicating supported hash algorithm (HASH_ALG)
                    and containing signature
                        calculated using the HASH_ALG and private key correspondent to the AA_PUB_V_KEY
```

TP Id	SECPKI_AA_AUTH_04_BV
Summary	Check that the AA sends signed AuthorizationResponseMessage using valid ITS AID and only allowed headers.
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
Configuration	CFG_AUTH_AA
PICS Selection	

Expected behaviour

```
with
    the ITS-S in 'enrolled' state
    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 ITS-S
    then
        the IUT sends a EtsiTs103097Data-Encrypted message
            containing EtsiTs103097Data-Signed
                containing signedData
                    containing tbsData
                        containing headerInfo
                            containing psid
                                indicating AID_PKI_CERT_REQUEST
                            and containing generationTime
                            and not containing any other headers
```

TP Id	SECPKI_AA_AUTH_05_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	**X_PICS**

Expected behaviour

```
with
    the ITS-S 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 ITS-S
    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	EtsiTs103097Data-Signed
2	NOT PICS_PKI_AUTH_POP	EtsiTs102941Data

TP Id	SECPKI_AA_AUTH_06_BV
Summary	Check that the AA includes the certificate in the positive authorization response
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
Configuration	CFG_AUTH_AA
PICS Selection	

Expected behaviour

```
with
    the ITS-S in 'enrolled' state
    and the ITS-S has sent the AuthorizationRequestMessage
    and the IUT(AA) in 'operational' state
    and the EA in 'operational' state
ensure that
    when
        the IUT is sending to the ITS-S 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 authorization response
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
Configuration	CFG_AUTH_AA
PICS Selection	
Expected behaviour	

```
with
    the ITS-S in 'enrolled' state
    and the ITS-S has sent the AuthorizationRequestMessage
    and the IUT(AA) in 'operational' state
    and the EA in 'operational' state
ensure that
    when
        the IUT is sending to the ITS-S the AuthorizationResponseMessage (MSG)
            containing responseCode
                indicating negative value
    then
        the message MSG
            not containing certificate
```

TP Id	SECPKI_AA_AUTH_08_BV
Summary	Check that signing of authorization response 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 receives the AuthorizationRequestMessage
        and the IUT is triggered to send an authorization response
    then
        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 'Authorization Response' (bit 3) set to 1
```

TP Id	SECPKI_AA_AUTH_09_BV
Summary	Check that generated AT 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
        the IUT is requested to send an authorization response
          containing a certificate (AT_CERT)
    then
        the IUT sends an AuthorizationResponseMessage
            containing authorizationResponse
                containing certificate (AT_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 1
                                containing opaque[1] (value)
                                    indicating 00h
                        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
```

5.5.5 CA Certificate Request

TP Id	SECPKI_AA_CERTGEN_01_BV
Summary	SubCA certificate requests of the AA are transported to the RCA using CACertificateRequestMessage structures 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 requested to send a CA certificate request
    then
        the IUT sends a CACertificateRequestMessage
            across the reference point S9 to the RCA
```

TP Id	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 ETSI TS 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 CA certificaterequest
    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.
```

TP Id	SECPKI_AA_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	

```
with
    the IUT being in the 'initial' state
ensure that
    when
        the IUT is requested to send a CA certificate request
    then
        the IUT sends a CACertificateRequestMessage
            being an EtsiTs103097Data-Signed structure
              containing hashId
                  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 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 CaCertificateRequestMessage An ECC encryption private key is randomly generated, the corresponding public key (encryptionKey) is provided to be included in the CACertificateRequestMessage 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 'initial' state ensure that when the IUT is requested to send a CA certificate request then the IUT sends a CACertificateRequestMessage containing caCertificateRequest containing publicKeys containing verification_key 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 'initial' state ensure that when the IUT is requested to send a CA certificate request then the IUT sends a CACertificateRequestMessage containing EtsiTs102941Data containing version indicating v1 (integer value set to 1)	

TP Id	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 'initial' state ensure that when the IUT is requested to send a CA certificate request then the IUT sends a CACertificateRequestMessage containing CaCertificateRequest 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 [8] 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 CA certificate request
    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 Id	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 the 'operational' state
ensure that
    when
        the IUT certificate is no longer valid (due to end of validity or revocation)
    then
        the IUT switches to the ''initial' state
        and sends a CACertificateRequestMessage
```

TP Id	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
    and the IUT was enrolled using the CA_CERT certificate
ensure that
    when
        the IUT is requested to perform a CA certificate rekeying procedure
    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 (CA_CERT)
            and containing signature
              computed over tbsData
                using the private key corresponding to CA_CERT
```

TP Id	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	

```
with
    the IUT being in the 'operational' state
ensure that
    when
        the IUT is requested to perform a CA certificate rekeying procedure
    then
        the sends a CACertificateRekeyingMessage
          containing tbsData
            containing CaCertificateRequestMessage
```

TP Id	SECPKI_AA_CERTGEN_11_BV
Summary	The (outer) tbsData of the CACertificateRekeyingMessage shall contain a headerInfo containing psid and generationTime. The psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [8] 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 'operational' state
ensure that
    when
        the IUT is requested to perform a CA certificate rekeying procedure
    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_AA_CERTGEN_12_BV
Summary	Check that the CA certificate rekeying 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 'operational' state
ensure that
    when
        the IUT is requested to perform a CA certificate rekeying procedure
    then
        the sends a CACertificateRekeyingMessage
          being an EtsiTs103097Data-Signed structure
             and containing tbsData
                and containing signer
                containing digest
                  indicating HashedId8 of the currently using 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 'CA Certificate Response' (bit 6) set to 1
```

5.5.6 Authorization using butterfly key expansion mechanism

5.5.6.1 Butterfly certificate response

TP Id	SECPKI_AA_BFK_AUTH_01_BV
Summary	Check that the AA sends the butterfly certificate response message after receiving of the butterfly certificate request Check that this message is encrypted using the same symmetric encryption key as the butterfly certificate request message
Reference	ETSI TS 102 941 [1], clauses 6.2.3.5.1 and 6.2.3.5.5
Configuration	CFG_BFK_AUTH_AA
PICS Selection	
Expected behaviour	

```
with
    the AA in 'operational' state
        authorized with CERT_AA certificate
ensure that
    when
        the IUT received the ButterflyCertificateRequestMessage
            containing content.encryptedData.recipients
                containing the instance of RecipientInfo
                    containing certRecipInfo
                        containing recipientId
                            indicating HashedId8 of the CERT_AA
                        and containing encKey
                            containing encrypted symmetric encryption key (ENC_KEY)
    then
        the IUT sends to the EA a EtsiTs103097Data-Encrypted
            containing content.encryptedData.recipients
                indicating size 1
                and containing the instance of RecipientInfo
                    containing pskRecipInfo
                        indicating HashedId8 of the ENC_KEY
```

TP Id	SECPKI_AA_BFK_AUTH_02_BV
Summary	Check that the butterfly certificate response message is signed using AA certificate Check that the message signature is valid
Reference	ETSI TS 102 941 [1], clauses 6.2.3.5.1 and 6.2.3.5.5
Configuration	CFG_BFK_AUTH_AA
PICS Selection	
Expected behaviour	

```
with
    the AA in 'operational' state
        authorized with CERT_AA certificate
ensure that
    when
        the IUT from the EA received the ButterflyCertificateRequestMessage
    then
        the IUT sends to the EA a EtsiTs103097Data-Encrypted
            containing content.encryptedData.ciperText
                containing EtsiTs103097Data-Signed
                    containing signedData
                        containing signer
                            containing digest
                                indicating HashedId8 value of the CERT_AA
                        and containing signature
                            validated using CERT_AA verification public key
```

TP Id	SECPKI_AA_BFK_AUTH_03_BV
Summary	Check that the butterfly certificate response message contains all necessary fields Check that the acaResponse in the butterfly certificate response encrypted using valid encryption key Check that the acaResponse in the butterfly certificate response is signed using valid verification key
Reference	ETSI TS 102 941 [1], clauses 6.2.3.5.1 and 6.2.3.5.5
Configuration	CFG_BFK_AUTH_AA
PICS Selection	

Expected behaviour

```
with
    the AA in 'operational' state
        authorized with CERT_AA certificate
ensure that
    when
        the IUT received from the EA the ButterflyCertificateRequestMessage (REQ)
    then
        the IUT sends to the EA a ButterflyCertificateResponseMessage
            containing content.encryptedData.ciperText
                containing EtsiTs103097Data-Signed
                    containing signedData.tbsData
                        containing headerInfo
                            containing psid
                                indicating AID_PKI_CERT_REQUEST
                            and containing generationTime
                            and not containing other fields
                        and containing payload
                            containing EtsiTs102941Data
                                containing butterflyCertificateResponse
                                    indicating AcaRaCertResponse
                                        containing version
                                            indicating 2
                                        and containing generationTime
                                            indicating value between the REQ generation time and the current time
                                        and containing requestHash
                                            indicating the left-most 16 octets of the SHA256 digest of the REQ
                                        and containing acaResponse
                                            containing private
                                                indicating the AcaEeCertResponsePrivateSpdu
```

TP Id	SECPKI_AA_BFK_AUTH_04_BV
Summary	Check that the butterfly certificate response message contains AT certificate, encrypted with a properly derived key
Reference	ETSI TS 102 941 [1], clauses 6.2.3.5.1 and 6.2.3.5.5
Configuration	CFG_BFK_AUTH_AA
PICS Selection	
Expected behaviour	

```
with
    the AA in 'operational' state
        authorized with CERT_AA certificate
ensure that
    when
        the IUT received from the EA the ButterflyCertificateRequestMessage (REQ)
            containing ButterflyCertRequest
                containing certEncKey (ITSS_ENC_KEY)
    then
        the IUT sends to the EA a ButterflyCertificateResponseMessage
            containing the AcaEeCertResponsePrivateSpdu
                containing content.signedData
                    containing signer.digest
                        indicating HashedId8 of CERT_AA
                    containing tbsData.payload
                        containing Ieee1609Dot2Data-Encrypted
                            containing content.encryptedData.recepients
                                indicating size 1
                                and containing the instance of RecipientInfo
                                    containing rekRecipInfo
                                        containing recipientId
                                            indicating HashedId8 of the ITSS_ENC_KEY
```

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 Id	SECPKI_RCA_CTLGEN_01_BV
Summary	Check that the RootCA generates the Full CTL when a 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
        the IUT issues 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
        the IUT issues a new CTL of type CtlFormat
            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 issues a new CTL of type CtlFormat
            containing isFullCtl
                indicating TRUE
            and containing ctlCommands
                not containing CtlCommand
                    containing add
                        containing ea
                            containing eaCertificate
                                indicating CERT_EA
```

TP Id	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 issues a new CTL of type CtlFormat
            containing isFullCtl
                indicating FALSE
            and containing ctlCommands
                not containing CtlCommand
                    containing delete
                        containing cert
                            indicating Hashedid8 of CERT_EA
```

TP Id	SECPKI_RCA_CTLGEN_05_BV
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	

```
ensure that
    when
        the RootCA is triggered to add new EA access point URL (URL) to the CTL
    then
        the IUT issues 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 eaCertificate
                                indicating CERT_EA
```

TP Id	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 triggered to add new EA access point URL (URL) to the CTL
    then
        the IUT issues a new CTL of type CtlFormat
            containing isFullCtl
                indicating FALSE
            containing ctlCommands
                containing CtlCommand
                    containing add
                        containing ea
                            containing eaCertificate (CERT_EA)
                            and containing itsAccessPoint
                                indicating URL
```

TP Id	SECPKI_RCA_CTLGEN_07_BV
Summary	Check that the RootCA generates the Full 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 triggered to add new URL for EA-AA communication (URL) to the CTL
    then
        the IUT issues a new CTL of type CtlFormat
            containing isFullCtl
                indicating TRUE
            containing ctlCommands
                containing CtlCommand
                    containing add
                        containing ea
                            containing eaCertificate (CERT_EA)
                            containing aaAccessPoint
                                indicating URL
                and NOT containing any other CtlCommand
                    containing add
                        containing ea
                            containing 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 triggered to add new URL for EA-AA communication (URL) to the CTL
    then
        the IUT issues a new CTL of type CtlFormat
            containing isFullCtl
                indicating FALSE
            containing ctlCommands
                containing CtlCommand
                    containing add
                        containing ea
                            containing eaCertificate (CERT_EA)
                            containing aaAccessPoint
                                indicating URL
```

TP Id	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 triggered to add new AA certificate (CERT_AA) in the CTL
    then
        the IUT issues a new CTL of type CtlFormat
            containing isFullCtl
                indicating TRUE
            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 triggered to add new AA certificate (CERT_AA) in the CTL
    then
        the IUT issues a new CTL of type CtlFormat
            containing isFullCtl
                indicating FALSE
            and containing ctlCommands
                containing CtlCommand
                    containing add
                        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 issues 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 triggered to delete AA certificate (CERT_AA) from the CTL
    then
        the IUT issues a new CTL of type CtlFormat
            containing isFullCtl
                indicating FALSE
            and containing ctlCommands
                not containing CtlCommand
                    containing delete
                        containing cert
                            indicating HashedId8 of CERT_AA
```

TP Id	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 triggered to add new URL for AA access point (URL) to the CTL
    then
        the IUT issues a new 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
                        containing aa
                            containing aaCertificate
                                indicating CERT_AA
```

TP Id	SECPKI_RCA_CTLGEN_14_BV
Summary	Check that the RootCA generates the Delta CTL when AA access point URL 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 triggered to add new URL for AA access point (URL) to the CTL
    then
        the IUT issues 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 the TLM CTL list
        containing RootCA certificate (CERT_RCA)
ensure that
    when
        the RootCA is triggered to issue a new CTL
    then
        the IUT issues a new CTL of type RcaCertificateTrustListMessage
            containing signedData
                containing signer.digest
                  indicating HashedID8 of the RootCA certificate (CERT_RCA)
                      containing appPermissions
                          containing 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 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 EtsiTs103097Data and EtsiTs102941Data envelopes are not yet removed from the analysing message.	

TP Id	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 issued the previous CTL of type CtlFormat
        containing ctlSequence
            indicating N
ensure that
    when
        the RCA is triggered to issue a new CTL
    then
        the IUT issues a new CTL of type CtlFormat
            containing ctlSequence
                indicating N+1	

TP Id	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 issued the previous CTL of type CtlFormat
        containing ctlSequence
            indicating 255
ensure that
    when
        the RCA is triggered to issue a new CTL
    then
        the IUT issues a new CTL of type CtlFormat
            containing ctlSequence
                indicating 0
```

TP Id	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 issues a new CTL of type CtlFormat
            containing nextUpdate
                indicating timestamp greater then T1
```

TP Id	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 to issue a new CTL
    then
        the IUT issues a new CTL of type CtlFormat
            containing ctlCommands
                not containing any item of type CtlCommand
                    containing add
                        containing tlm
                        or containing rca
```

TP Id	SECPKI_RCA_CTLGEN_20_BV
Summary	Check that the RCA Delta CTL is generated at the same time as FullCTL 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 ctlSequence
            indicating N
ensure that
    when
        the RCA is triggered to issue a new CTL
    then
        the IUT issues a new CTL of type CtlFormat (CTL_FULL)
            containing isFullCtl
                indicating TRUE
            and containing ctlSequence
                indicating N+1
        and the IUT issues a new CTL of type CtlFormat (CTL_DELTA)
            containing isFullCtl
                indicating FALSE
            and containing ctlSequence
                indicating N+1
            containing ctlCommands
                indicating difference between CTL_FULL and CTL_FULL_PREV	

TP Id	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 issues 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 triggered to delete the CA from the CTL
    then
        the IUT issues a new CTL of type CtlFormat (CTL_FULL)
            containing isFullCtl
                indicating TRUE
            and containing ctlCommands
                NOT containing any item of type CtlCommand
                    containing delete	

TP Id	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 to issue a new CTL
    then
        the IUT issues a new CTL of type CtlFormat
            containing isFullCtl
                indicating TRUE
            and containing ctlCommands
                containing at least one ctlCommand
                    containing add
                        containing url
                            indicating URL of the DC of the IUT
                        containing 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 Id	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 triggered to generate new CRL
    then
        the IUT generates the CertificateRevocationListMessage
          containing signer
            containing digest
              indicating HashedId8 of RootCA certificate
                containing appPermissions
                  containing an item of type PsidSsp
                    containing psid
                      indicating AID_CRL
                    and containing ssp
                      containing opaque[0] (version)
                        indicating 1
```

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

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 issues a new CRL of type ToBeSignedCrl
            and containing entries
                containing item of type CrlEntry
                    indicating HashID8 of the CERT_CA
```

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 issues a new CRL of type ToBeSignedCrl
            containing entries
                containing item of type CrlEntry
                    indicating HashID8 of the CERT_RCA
```

TP Id	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
        the RootCA is triggered to issue a new CRL at the time T1
    then
        the IUT issues a new CRL of type ToBeSignedCrl
            containing thisUpdate
                indicating timestamp greater or equal to the T1
```

TP Id	SECPKI_RCA_CRLGEN_05_BV
Summary	Check that the RCA issues a new CRL when the 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 nextUpdate
            indicating time Tprev
ensure that
    when
        the Tprev is less than current time (Tcur)
    then
        the IUT issues a new CRL of type ToBeSignedCrl
            containing thisUpdate
                indicating timestamp greater or equal to the Tcur
            and containing nextUpdate
                indicating timestamp greater than Tcur and greater than thisUpdate
```

TP Id	SECPKI_RCA_CRLGEN_06_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	

```
ensure that
    when
        the RootCA is triggered to issue a new CRL
    then
        the IUT issues a new CRL of type ToBeSignedCrl
            containing entries
                does not containing item of type CrlEntry
                    indicating HashID8 of other RootCA
```

TP Id	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
        the RootCA is triggered to issue a new CRL
    then
        the IUT issues 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 issues a new CRL of type ToBeSignedCrl
            containing version
                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 generates 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 generates 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 Request (bit 2) set to 1
                            and indicating 'Authorization Response' (bit 3) 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
                            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
                            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_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 RootCA certificate
    then
        the IUT generates 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 asks the IUT for the newly issued CRL
    then
        the IUT is answered with this CRL
```

TP Id	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 CTL
ensure that
    when
        the ITS-S asks 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 `EtsiTs103097Data` and `EtsiTs102941Data` 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 issues a new CTL of type CtlFormat
            containing isFullCtl
                indicating TRUE
            and containing ctlCommands
                containing CtlCommand
                    containing add
                        containing rca
                            containing selfsignedRootCa
                                indicating CERT_RCA
```

TP Id	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 issues a new CTL of type CtlFormat
            containing isFullCtl
                indicating FALSE
            and containing ctlCommands
                containing CtlCommand
                    containing add
                        containing rca
                            containing 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 to delete RootCA certificate (CERT_RCA) from the CTL
    then
        the IUT issues a new CTL of type CtlFormat
            containing isFullCtl
                indicating TRUE
            and containing ctlCommands
                not containing CtlCommand
                    containing add
                        containing rca
                            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 to delete RootCA certificate (CERT_RCA) from the CTL
    then
        the IUT issues a new CTL of type CtlFormat
            containing isFullCtl
                indicating FALSE
            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 issues a new CTL of type CtlFormat
            containing isFullCtl
                indicating TRUE
            and containing ctlCommands
                not containing CtlCommand
                    containing add
                        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 issues a new CTL of type CtlFormat
            containing isFullCtl
                indicating FALSE
            and containing ctlCommands
                not containing CtlCommand
                    containing add
                        containing tlm
                            containing selfSignedTLMCertificate
                                indicating CERT_TLM
```

TP Id	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 to change the CPOC URL in the CTL
    then
        the IUT issues a new CTL of type CtlFormat
            containing isFullCtl
                indicating TRUE
            and containing ctlCommands
                not containing CtlCommand
                    containing add
                        containing tlm
                            containing accessPoint
                                indicating URL
```

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
        the TLM is triggered to change the CPOC URL in the CTL
    then
        the IUT issues a new CTL of type CtlFormat
            containing isFullCtl
                indicating FALSE
            and containing ctlCommands
                not containing CtlCommand
                    containing add
                        containing tlm
                            containing accessPoint
                                indicating URL
```

TP Id	SECPKI_TLM_ECTLGEN_09_BV
Summary	Check that the TLM CTL is signed using TLM verification key Check that signing of TLM CTL is allowed by the TLM certificate
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
    then
        the IUT issues a new CTL of type TlmCertificateTrustListMessage
            containing signedData
                containing signer.digest
                    indicating HashedID8 of the TLM certificate (TLM_CERT)
                        containing appPermissions
                          containing 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 tlm
                                            containing selfSignedTLMCertificate
                                                indicating TLM_CERT
```

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

TP Id	SECPKI_TLM_ECTLGEN_10_BV
Summary	Check that the TLM CTL sequence counter is monotonically increased
Reference	ETSI TS 102 941 [1], clause 6.3.1
Configuration	CFG_CTLGEN_TLM
PICS Selection	

Expected behaviour

```
with
    the TLM already has issued the previous CTL of type CtlFormat
        containing ctlSequence
            indicating N
ensure that
    when
        the TLM is triggered to issue a new CTL
    then
        the IUT issues 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	ETSI TS 102 941 [1], clause 6.3.1
Configuration	CFG_CTLGEN_TLM
PICS Selection	

Expected behaviour

```
with
    the TLM already has issued the previous CTL of type CtlFormat
        containing ctlSequence
            indicating 255
ensure that
    when
        the TLM is triggered to issue a new CTL
    then
        the IUT issues a new CTL of type CtlFormat
            containing ctlSequence
                indicating 0
```

TP Id	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 issues a new CTL of type CtlFormat
            containing nextUpdate
                indicating timestamp greater then T1
```

TP Id	SECPKI_TLM_ECTLGEN_13_BV
Summary	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
        the TLM is triggered to issue a new CTL
    then
        the IUT issues a new CTL of type CtlFormat
            containing ctlCommands
                not containing any item of type CtlCommand
                    containing add
                        containing ea
                        or containing aa
```

TP Id	SECPKI_TLM_ECTLGEN_14_BV
Summary	Check that the TLM Delta CTL is generated at the same time as FullCTL 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 ctlSequence
            indicating N
ensure that
    when
        the TLM is triggered to issue a new CTL
    then
        the IUT issues a new CTL of type CtlFormat (CTL_FULL)
            containing isFullCtl
                indicating TRUE
            and containing ctlSequence
                indicating N+1
        and the IUT issues a new CTL of type CtlFormat (CTL_DELTA)
            containing isFullCtl
                indicating FALSE
            and containing ctlSequence
                indicating N+1
            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
    when
        the IUT is triggered to issue a new CTL
    then
        the IUT issues a new CTL of type CtlFormat
            containing version
                indicating 1
```

TP Id	SECPKI_TLM_ECTLGEN_16_BV
Summary	Check that the TLM Full CTL does not contain commands of type 'delete'
Reference	ETSI TS 102 941 [1], clause 6.3.1
Configuration	CFG_CTLGEN_TLM
PICS Selection	

Expected behaviour

```
ensure that
    when
        the IUT is triggered to delete the CA from the CTL
    then
        the IUT issues a new CTL of type CtlFormat
            containing isFullCtl
                indicating TRUE
            and containing ctlCommands
                NOT containing any item of type CtlCommand
                    containing delete
```

5.9 CPOC behaviour

TP Id	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	CFG_CPOC
PICS Selection	
Expected behaviour	
with the TLM issued a new CTL ensure that when the ITS-S asks the IUT for the newly issued CTL then the IUT is answered with this CTL	

History

Document history		
V1.1.1	March 2019	Publication
V1.2.1	January 2022	Publication
V1.2.2	July 2022	Publication
V2.1.1	September 2024	Publication