ETSITS 103 525-2 V1.2.2 (2022-07)



Intelligent Transport Systems (ITS); Testing;

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

Reference RTS/ITS-005107 Keywords ITS, security, testing, TSS&TP

ETSI

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

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

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

Important notice

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

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

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

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

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

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:

https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

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

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

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

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

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

Copyright Notification

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

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

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

© ETSI 2022. All rights reserved.

Contents

Intelle	ectual Property Rights	5
Forew	vord	5
Moda	ıl verbs terminology	5
1	Scope	6
2	References	6
2.1	Normative references	
2.1	Informative references.	
∠. ∠		
3	Definition of terms, symbols and abbreviations	7
3.1	Terms	
3.2	Symbols	
3.3	Abbreviations	7
4	Test Suite Structure (TSS)	9
4.1	Structure for Security tests	
4.2	Test entities and states	
4.2.1	ITS-S states	
4.2.2	EA states	
4.2.3	AA states	
4.2.4	RootCA states	11
4.2.5	TLM states	11
4.3	Test configurations	11
4.3.1	Overview	11
4.3.2	Enrollment	
4.3.2.1		
4.3.2.2		
4.3.3	Authorization	
4.3.3.1		
4.3.3.2	8 = - =	
4.3.4	Authorization Validation	
4.3.4.1		
4.3.4.2	<u> </u>	
4.3.5	CA certificate generation	
4.3.5.1		
4.3.5.2		
4.3.5.3		
4.3.6	ECTL generation	
4.3.6.1	6 – –	
4.3.6.2		
4.3.7 4.3.7.1	Root CTL generation	
4.3.7.1 4.3.8	1 Configuration CFG_CTLGEN_RCA CRL generation	
4.3.8.1		
4.3.6.1 4.3.9	ITS-S CRL/CTL handling	
4.3.9.1	· · · · · · · · · · · · · · · · · · ·	
5	Test Purposes (TP)	
5.1	Introduction	
5.1.1	TP II. ('S	
5.1.2	TP Identifier naming conventions.	
5.1.3	Rules for the behaviour description	
5.1.4	Sources of TP definitions	
5.1.5	Mnemonics for PICS reference	
5.1.6	Certificates content	
5.2	ITS-S behaviour	
5.2.0	Overview	
5.2.1	Manufacturing	10

5.2.2	Enrollment	16
5.2.2.0	Overview	16
5.2.2.1	Enrollment request	17
5.2.2.2	Enrollment response handling	22
5.2.2.3	Enrollment request repetition	23
5.2.3	Authorization	25
5.2.3.0	Overview	25
5.2.3.1	Authorization request	25
5.2.3.2	Authorization response handling	34
5.2.3.3	Authorization request repetition	34
5.2.4	CTL handling	36
5.2.5	CTL distribution	37
5.2.6	CRL handling	43
5.2.7	CRL distribution	45
5.3	Common CA behaviour	48
5.3.0	Overview	48
5.3.1	Certificate validation	49
5.3.1.1	Basic certificate content	49
5.3.1.2	Check certificate region validity restriction	52
5.3.1.3	Check ECC point type of the certificate signature	56
5.3.1.4	Check ECC point type of the certificate public keys	56
5.3.1.5	Verify certificate signatures	57
5.3.1.6	Verify certificate permissions	58
5.3.1.7	Check time validity restriction in the chain	
5.4	EA behaviour	61
5.4.0	Overview	61
5.4.1	Enrollment request handling	
5.4.2	Enrollment response	67
5.4.3	Authorization validation request handling	
5.4.4	Authorization validation response	72
5.4.5	CA Certificate Request	76
5.5	AA behaviour	80
5.5.0	Overview	80
5.5.1	Authorization request handling	81
5.5.2	Authorization validation request	
5.5.3	Authorization validation response handling	
5.5.4	Authorization response	96
5.5.5	CA Certificate Request	
5.6	RootCA behaviour	105
5.6.0	Overview	105
5.6.1	CTL generation	106
5.6.2	CRL generation	
5.6.3	CA certificate generation	119
5.7	DC behaviour	
5.8	TLM behaviour	
5.8.1	CTL generation	
5.9	CPOC behaviour	128
History		129

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

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

Modal verbs terminology

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

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

1 Scope

The present document provides the Test Suite Structure and Test Purposes (TSS & TP) for PKI management as defined in ETSI TS 102 941 [1] in accordance with the relevant guidance given in ISO/IEC 9646-7 [i.6].

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

2 References

F13

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]	Management".
	[2]	ETSI TS 103 097 (V1.4.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".
	[3]	IEEE Std 1609.2 TM -2016: "IEEE Standard for Wireless Access in Vehicular Environments -

Security Services for Applications and Management Messages", as amended by IEEE Std 1609.2aTM-2017: "IEEE Standard for Wireless Access In Vehicular Environments - Security Services for Applications and Management Messages Amendment 1".

ETCLTC 102 041 (VI 4.1), "Intelligent Transment Systems (ITS), Security Trust and Drivery

[4] ETSI TS 103 525-1 (V1.2.2): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 1: Protocol Implementation Conformance Statement (PICS)".

[5] ETSI TS 103 096-2 (V1.5.2): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 2: Test Suite Structure and Test Purposes (TSS & TP)".

[6] ETSI TS 103 601 (V1.1.1): "Intelligent Transport Systems (ITS); Security; Security management messages communication requirements and distribution protocols".

[7] Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS) v1.1.

2.2 Informative references

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

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

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

[i.1]	ETSI EG 202 798 (V1.1.1): "Intelligent Transport Systems (ITS); Testing; Framework for conformance and interoperability testing".
[i.2]	ETSI TS 102 965 (V1.3.1): "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration".
[i.3]	ISO/IEC 9646-1 (1994): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 1: General concepts".
[i.4]	ISO/IEC 9646-2 (1994): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 2: Abstract Test Suite specification".
[i.5]	ISO/IEC 9646-6 (1994): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 6: Protocol profile test specification".
[i.6]	ISO/IEC 9646-7 (1995): "Information technology Open Systems Interconnection Conformance testing methodology and framework Part 7: Implementation Conformance Statements".
[i.7]	ETSI ETS 300 406 (1995): "Methods for testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".
[i.8]	United Nations Statistics Division: "Standard country or area codes for statistical use (M49)".

Definition of terms, symbols and abbreviations 3

Terms 3.1

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

AID_CERT_REQ: "Secured certificate request service" ITS-AID

AID_CTL: "CTL service" ITS-AID AID_CRL: "CRL service" ITS-AID

Symbols 3.2

Void.

Abbreviations 3.3

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 Enrollment Authority
EC Enrolment Credential
ECC Elliptic Curve Cryptography
ECTL European Certificate Trust List

GN GeoNetworking
GN-MGMT GeoNetworking
GN-MGMT GN Management

GPC GNSS positioning correction

HMAC Keyed-Hash Message Authentication Code

ITSIntelligent Transportation SystemsITS-SIntelligent Transport System - StationITS-SIntelligent Transport System - Station

IUT Implementation Under Test

IVIM Infrastructure to Vehicle Information Message MAPEM Road/lane topology and traffic maneuver 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 Message

SREM Signal Request Message
SSEM Signal Request Status 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
		CA certificate generation	Valid
		CRL handling	Valid
		CTL handling	Valid
	AA	Authorization	Valid
		Authorization Validation	Valid
		CA certificate generation	Valid
		CRL handling	Valid
		CTL handling	Valid
	RootCA	CA certificate generation	Valid
		CTL/CRL generation	Valid
	DC	CTL/CRL distribution	Valid
	TLM	ECTL generation	Valid
		TLM certificate generation	Valid
	CPOC	ECTL distribution	Valid

4.2 Test entities and states

4.2.1 ITS-S states

- State 'initialized':
 - ITS-S in 'initialized' state is ready to perform the enrollment 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 enrollment 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:
 - enrollment 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 enrollment 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 enrollment 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 the clause 5.

4.3.2 Enrollment

4.3.2.1 Configuration CFG_ENR_ITS-S

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

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

TS: EA is emulated by TS.

4.3.2.2 Configuration CFG_ENR_EA

IUT: EA is in the state 'operational', ready to handle enrollment 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 AATS: AA is emulated by the TS.

4.3.3.2 Configuration CFG_AUTH_AA

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

• The profile information for the emulated ITS-S.

TS: ITS-S is emulated by the TS:

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

4.3.4 Authorization Validation

4.3.4.1 Configuration CFG_AVALID_AA

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

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

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

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

4.3.4.2 Configuration CFG_AVALID_EA

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

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

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

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

4.3.5 CA certificate generation

4.3.5.1 Configuration CFG_CAGEN_INIT

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

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

4.3.5.2 Configuration CFG_CAGEN_REKEY

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

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

4.3.5.3 Configuration CFG_CAGEN_RCA

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

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

4.3.6 ECTL generation

4.3.6.1 Configuration CFG_CTLGEN_TLM

IUT: TLM in the operational state.

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

4.3.6.2 Configuration CFG_CTLGEN_CPOC

IUT: CPOC in the operational state.

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

4.3.7 Root CTL generation

4.3.7.1 Configuration CFG_CTLGEN_RCA

IUT: RCA in the operational state.

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

4.3.8 CRL generation

4.3.8.1 Configuration CFG_CRLGEN_RCA

IUT: RCA in the operational state.

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

4.3.9 ITS-S CRL/CTL handling

4.3.9.1 Configuration CFG_CXL_P2P

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

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

Neighbour ITS-S: is emulated by the TS.

RCA: is emulated by the TS.

DC: is emulated by the TS.

5 Test Purposes (TP)

5.1 Introduction

5.1.1 TP definition conventions

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

5.1.2 TP Identifier naming conventions

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

Table 2: TP naming convention

Identifier	TP_ <root>_<tgt>_<gr>_<sn>_<x></x></sn></gr></tgt></root>		
	<root> = root</root>	SECPKI	
	<tgt> = target</tgt>	ITS-S	ITS-Station
		CA	Common Certificate Authority
		AA	Authorization Authority
		EA	Enrollment Authority
		RCA	Root Certification Authority
		DC	Distribution Centre
		CPOC	C-ITS Point of Contact
	<gr> = group</gr>	ENR	Enrollment
		AUTH	Authorization
		AUTHVAL	Authorization Validation
		CRL	CRL handling
		CTL	CTL handling
		CERTGEN	Certificate generation
		CTLGEN	CTL generation
		ECTLGEN	ECTL generation
		CRLGEN	CRL generation
		LISTDIST	CTL/CRL/ECTL distribution
			TLM certificate generation
	<sgr>=sub-group</sgr>	SND	Sending behaviour
		RCV	Receiving behaviour
		REP	Repetition behaviour
	<sn> = test purpose sequential number</sn>		01 to 99
	<x> = category</x>	BV	Valid Behaviour tests
		BI	Invalid Behaviour Tests

5.1.3 Rules for the behaviour description

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

ETSI TS 102 941 [1] does not use the finite state machine concept. As consequence, the test purposes use a generic "Initial State" that corresponds to a state where the IUT is ready for starting the test execution. Furthermore, the IUT shall be left in this "Initial State", when the test is completed.

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

5.1.4 Sources of TP definitions

All TPs have been specified according to ETSI TS 102 941 [1] which shall be followed as specified in the clauses below.

5.1.5 Mnemonics for PICS reference

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

Table 3: Mnemonics for PICS reference

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

5.1.6 Certificates content

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

Table 4: Certificates content

AA certificate	Content	To be installed on the IUT
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 / 0xFF000000); DENM with all possible SSP (0x01FFFFF / 0xFF000000); SPATEM with all possible SSP (0x01E0 / 0xFF1F); MAPEM with all possible SSP (0x01C0 / 0xFF3F); IVIM with all possible SSP (0x01000000FFF8 / 0xFF000000007); 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 Enrollment

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:

 $PICS_SECPKI_ENROLLMENT = TRUE$

5.2.2.1 Enrollment request

TP ld	SECPKI_ITS-S_ENR_01_BV		
Summary	Check that IUT sends an enrollment 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 'init	ialized' state		
ensure that			
when			
the IUT is triggered to request a new Enrollment Credential (EC) certificate			
then			
the IUT sends to EA	the IUT sends to EA an EnrollmentRequestMessage		

PId SECPKI_ITS-S_ENR_02_BV			
Summary If the enrollment request of the IUT is an initial enrollment request, the itsld (conta the InnerECRequest) shall be set to the canonical identifier, the signer (contained outer EtsiTs1030971Data-Signed) shall be set to self and the outer signature shall 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 'initi	alized' state		
ensure that			
when			
the IUT is requested	to send an EnrollmentRequestMessage		
then			
	siTs103097Data-Encrypted		
	crypted EtsiTs103097Data-Signed		
•	tsiTs102941Data		
	g InnerECRequestSignedForPOP		
	containing InnerEcRequest		
containing itsld			
indicating the canonical identifier of the ITS-S			
	and containing signer		
declared			
and containir			
computed using the canonical private key			

TP Id	SECPKI_ITS-S_ENR_03_BV	
In presence of a valid EC, the enrollment request of the IUT is a rekeying enrollment request with the itsId (contained in the InnerECRequest) and the SignerIdentifier (contained in the outer EtsiTs1030971Data-Signed) both declared as digest containing HashedId8 of the EC and the outer signature computed using the current valid EC privilege.		
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_REENROLLMENT	
	Expected behaviour	
with the IUT being in the 'enrolled' state ensure that when the IUT is requested to send an EnrollmentRequestMessage then the IUT sends an EtsiTs103097Data-Encrypted containing an encrypted EtsiTs103097Data-Signed containing EtsiTs102941Data containing InnerECRequestSignedForPOP containing InnerEcRequest containing itsld declared as digest containing the HashedId8 of the EC identifier and containing signer declared as digest containing the HashedId8 of the EC identifier and containing signature		

TP Id	SECPKI_ITS-S_ENR_04_BV	
Summary If the EC is revoked, the IUT returns to the state 'initialized'		
Reference	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_CRL	
Expected behaviour		
with		
the IUT being in the 'enrolled' state		
ensure that		
when		
the IUT is informed about a revocation of its EC		
then		
the IUT returns to the 'initialized' state		

TP Id	SECPKI_ITS-S_ENR_05_BV		
Summary If the EC expires, the IUT returns to the state 'initialized'			
Reference	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 ensure that when the EC of the IUT expires then the IUT returns to the 'initialized' state			

FP Id SECPKI_ITS-S_ENR_06_BV	
Summany	For each enrollment request, the ITS-S shall generate a new verification key pair
Summary	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
Reference	ETSI TS 103 097 [2], clause 7
Configuration	CFG_ENR_ITS-S
PICS Selection	PICS_SECPKI_REENROLLMENT
	Expected behaviour
with	
the IUT being in the 'initi	alized' state
ensure that	
when	
the IUT is requested to send multiple EnrollmentRequestMessage	
then	
each EnrollmentRequestMessage	
contains a different and unique verification key pair within the InnerECRequest.	
	entRequestMessage should be an initial request, the following
EnrollmentRequestMessages should be rekeying requests.	

TP Id	SECPKI_ITS-S_ENR_07_BV		
Summary	Within the InnerECRequest, the requestedSubjectAttributes shall not contain a		
Summary	certIssuePermissions field		
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.1		
Configurat	tion CFG_ENR_ITS-S		
PICS Selec	ction		
	Expected behaviour		
with			
the IUT	being in the X_STATE		
ensure that			
when			
the	IUT is requested to send an EnrollmentRequestMessage		
then	· · · · · · · · · · · · · · · · · · ·		
the	IUT sends an EtsiTs103097Data-Encrypted		
	containing an encrypted EtsiTs103097Data-Signed		
	containing EtsiTs102941Data		
	containing InnerECRequestSignedForPOP		
	containing InnerEcRequest		
containing requestedSubjectAttributes			
not containing certIssuePermissions			
Variants			
nn	X_STATE		
1	'initialized' state		
	O legis legis de de		

ı	Variants	
ſ		X_STATE
ĺ	1	'initialized' state
ſ	2	l'enrolled' state

TP Id	- 14		
Summary	In the headerInfo of the tbsData of the InnerECRequestSignedForPOP all other components of the component tbsdata.headerInfo except generationTime and psid are not used and absent. The psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [i.2] and the generationTime shall be present		
Reference			
Configurat	ion CFG_ENR_ITS-S		
PICS Selec	etion		
	Expected behaviour		
with			
the IUT	the IUT being in the X_STATE		
ensure that			
when			
	IUT is requested to send an EnrollmentRequestMessage		
then			
	the IUT sends an EtsiTs103097Data-Encrypted		
	containing an encrypted EtsiTs103097Data-Signed		
	containing EtsiTs102941Data		
containing InnerECRequestSignedForPOP containing tbsData			
	containing tospata containing headerInfo		
	containing reademno containing psid		
	indicating AID_CERT_REQ		
and containing generationTime			
and not containing any other component of tbsdata.headerInfo			
Variants	3 · · · · · · · · · · · · · · · · · · ·		
nn	X_STATE		
1	'initialized' state		
2	'enrolled' state		

TP Id	TP Id SECPKI_ITS-S_ENR_09_BV		
	In the headerInfo of the tbsData of the outer EtsiTs103097Data-Signed all other		
Summary	components of the component tbsdata.headerInfo except generationTime and psid are not		
	used and absent. The psid shall be set to "secured certificate request" as assigned in ETSI		
	TS 102 965 [i.2] and the generationTime shall be present		
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.1		
Configurati			
PICS Selec	tion		
	Expected behaviour		
with			
the IUT	peing in the X_STATE		
ensure that			
when			
the I	JT is requested to send an EnrolmentRequestMessage		
then			
	the IUT sends an EtsiTs103097Data-Encrypted		
С	ontaining an encrypted EtsiTs103097Data-Signed		
	containing tbsData		
	containing headerInfo		
	containing psid		
	indicating AID_CERT_REQ		
	and containing generationTime		
and not containing any other component of tbsdata.headerInfo			
Variants			
nn	X_STATE		
1	'initialized' state		
2	2 'enrolled' state		

TD IA	PECDIZI ITE C. END. 40 DV		
TP Id	SECPKI_ITS-S_ENR_10_BV		
	The EtsiTs103097Data-Encrypted containing the correctly encrypted ciphertext and a		
Cummoni	recipients component containing one instance of RecipientInfo of choice certRecipInfo		
Summary	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 pub in the EA certificate referenced in the recipientId			
Reference			
	ETSI TS 102 941 [1], clause 6.2.3.2.1		
Configuration			
PICS Selection			
	Expected behaviour		
with			
	ng in the X_STATE		
ensure that			
when			
	is requested to send an EnrollmentRequestMessage		
	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 (KEY)			
	and containing encKey		
being a symmetric key (SYMKEY) encrypted using the key KEY			
containing ciphertext			
which is encrypted using the symmetric key SYMKEY contained in encKey Variants			
	STATE		
∠ rer	2 'enrolled' state		

FP 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 X_STATE		
ensure that when the IUT is requested to send an EnrollmentRequestMessage		
then		
the IUT sends an EtsiTs103097Data-Encrypted		
containing an en	containing an encrypted EtsiTs103097Data-Signed	
containing E	containing EtsiTs103097Data	
containing InnerECRequestSignedForPOP		
containing tbsData		
CC	containing InnerEcRequest	
containing verificationKey (VKEY)		
containing signature		
computed on InnerECRequest		
using the private key corresponding to VKEY		
contained in InnerECRequest		
V STATE	Variants	
nn X_STATE		
1 'initialized' state		

'enrolled' state

FP Id SECPKI_ITS-S_ENR_12_BV			
Check that signing of Enrollment 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_SECPKI_REENROLLMENT			
	Expected behaviour		
with			
the IUT being in the 'enro	olled' state		
ensure that			
when			
•	the IUT is requested to send an EnrollmentRequestMessage		
then	T 40000TD 4 5 4 4		
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 an item of type FsidSsp			
	indicating AID_CERT_REQ		
and containing ssp			
	containing opaque[0] (version)		
	indicating 1		
	containing opaque[1] (value)		
	indicating 'Enrollment Request' (bit 1) set to 1		

5.2.2.2 Enrollment response handling

TP Id	SECPKI_ITS-S_ENR_RCV_01_BV		
Summary	If an enrollment 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		
Configurati			
PICS Selec	tion		
		Expected behaviour	
with			
the IUT	ne IUT being in the X_STATE		
and the	IUT has sent the Enrollmentl	RequestMessage	
ensure that	that		
when	when		
the I	UT received the EnrollmentR	ResponseMessage	
COI	containing a responseCode different than 0		
then			
the IUT returns to the X_STATE state			
Variants			
nn	X_STATE		
1	1 'initialized' state		
2	2 'enrolled' state		

TP ld	SECPKI_ITS-S_ENR_RCV_02_BV
Summary	The IUT is capable of parsing and handling of positive EnrollmentResponse messages containing the requested EC. In case of a successful enrollment, 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 EnrollmentRequestMessage ensure that when the IUT receives a subsequent EnrollmentResponseMessage as an answer of the EA containing a responseCode indicating 0 and containing an enrollment certificate then	
the IUT switches to the 'enrolled' state	

5.2.2.3 Enrollment request repetition

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

• PICS_SECPKI_ENROLLMENT_RETRY = TRUE

TP ld	SECPKI_ITS-S_ENR_REP_01_BV	
Summary	Check that IUT repeats an enrollment 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 Enrollment Request at the time T1 and the IUT has not yet received the Enrollment Response		
ensure that when the IUT local time is reached the T1 + PIXIT_ENR_TIMEOUT_TH1 then the IUT sends to EA an EnrollmentRequestMessage		

TP Id	SECPKI_ITS-S_ENR_REP_02_BV	
Summary	Check that IUT uses the same message to perform enrollment retry	
Reference	ETSI TS 103 601 [6], clause 5.1.2	
Configuration	CFG_ENR_ITS-S	
PICS Selection		
	Expected behaviour	
and the IUT already sen ensure that when	with the IUT being in the 'initialized' state and the IUT already sent the Enrollment Request (M) ensure that when the IUT is triggered to re-send an Enrollment Request then	

TP Id	SECPKI_ITS-S_ENR_REP_03_BV		
Summary	Check that IUT stops sending the Enrollment Request message if Enrollment 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 'ini	tialized' state		
and the IUT has sent th	and the IUT has sent the Enrollment Request more than 1 time		
ensure that	ensure that		
when			
the IUT receives an Enrollment Response			
then			
the IUT stops sending Enrollment Requests to EA			

TP ld	SECPKI_ITS-S_ENR_REP_04_BV	
Summary	Check that IUT stops sending the Enrollment 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 th	e 'initialized' state	
and the IUT has st	arted sending the Enrollment Request	
ensure that		
when		
the IUT sent the PIXIT_ENR_MAX_N1 Enrollment Request messages		
then	· •	
the IUT stops sending Enrollment Requests		

TP ld	SECPKI_ITS-S_ENR_REP_05_BV	
Summary	Check that IUT stops sending the Enrollment 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 th	e 'initialized' state	
and the IUT has st	arted sending the Enrollment Request at the time T1	
ensure that	•	
when		
the IUT local time is reached the T1 + PIXIT_ENR_TIMEOUT_TH2		
then		
the IUT stops s	sending an Enrollment Request messages	

TP Id	SECPKI_ITS-S_ENR_REP_05_BV
Summanı	Check that IUT stops sending the Enrollment Request message if sending timeout (TH2)
Summary	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 'ii	nitialized' state
and the IUT has started sending the Enrollment Request	
ensure that	
when	
the IUT sent the Enrollment Request messages	
then	
the IUT stops sending Enrollment 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 send 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	e	
and the AA in 'operation	and the AA in 'operational' state	
ensure that		
when		
the IUT is triggered to request new Authorization Ticket (AT)		
then		
the IUT sends an EtsiTs103097Data-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	e	
and the AA in 'operation	al' state	
authorized with CER	T_IUT_A_AA certificate	
ensure that		
when		
the IUT is triggered to request new Authorization Ticket (AT)		
then		
the IUT sends a Etsi	the IUT sends a EtsiTs103097Data to the AA	
containing content.encryptedData.recipients		
indicating size 1		
and containing the instance of RecipientInfo		
containing certRecipInfo		
	ning 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	d' state		
and the AA in 'ope	rational' state		
authorized with			
containing e	containing encryptionKey (AA_ENC_PUB_KEY)		
ensure that			
when			
the IUT is trigge	ered to request new Authorization Ticket (AT)		
then			
the IUT sends a EtsiTs103097Data to the AA			
containing content.encryptedData			
containing ciphertext			
cont	containing data		
encrypted 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' st	ate		
and the IUT already sen	and the IUT already sent one or more Authorization Requests		
and the AA in 'operation	al' state		
ensure that			
when	when		
the IUT is triggered to request new Authorization Ticket (AT)			
then			
the IUT sends a EtsiTs103097Data to the AA			
containing content.encryptedData			
containing ciphertext.aes128ccm.nonce			
indicating value not equal to the nonce in N previous messages			
	and 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 ld	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	e		
and the AA in 'operation	and the AA in 'operational' state		
ensure that	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 ld	SECPKI_ITS-S_AUTH_06_BV		
	Check that for each authorization request the ITS-S generates a new verification key pair		
Summary	Check that for each authorization request the ITS-S generates a new encryption key pair		
	Check that for each authorization request the ITS-S generates a new hmac-key		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1		
Configuration	CFG_AUTH_ITS-S		
PICS Selection			
	Expected behaviour		
with			
the IUT in 'enrolled' state	e		
and the AA in 'operation	al' state		
ensure that			
when			
the IUT is triggered to request new Authorization Ticket (AT)			
	then		
the IUT sends a EtsiTs103097Data to the AA			
containing EtsiTs			
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 'operation	and the AA in 'operational' state		
ensure that	ensure that		
when	when		
the IUT is triggered to request new Authorization Ticket (AT)			
then			
the IUT sends a Etsi	Ts103097Data to the AA		
containing EtsiTs102941Data			
containing authorizationRequest			
containing sharedAtRequest			
containing keyTag			
indicating properly calculated value			

TP ld	SECPKI_ITS-S_AUTH_08_BV	
Summary	Check that ITS-S sends Authorization request with eald of EA certificate	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_ITS-S	
PICS Selection		
	Expected behaviour	
with		
the IUT is enrolled by the	e EC, signed with the CERT EA certificate	
and the AA in 'operation	and the AA in 'operational' stateensure that	
when	·	
the IUT is triggered t	the IUT is triggered to request new Authorization Ticket (AT)	
then		
the IUT sends a Etsi	the IUT sends a EtsiTs103097Data to the AA	
containing EtsiTs102941Data		
containing authorizationRequest		
containing sharedAtRequest		
containing eald		
ind	indicating HashedId8 of CERT_ EA certificate	

TDIA	PECCHALITE & AUTU OO DV		
TP ld	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	e e e e e e e e e e e e e e e e e e e		
and the AA in 'operation	al' state		
ensure that	ensure that		
when	when		
the IUT is triggered t	the IUT is triggered to request new Authorization Ticket (AT)		
then			
the IUT sends a Etsi	Ts103097Data to the AA		
containing EtsiTs102941Data			
containing authorizationRequest			
containing sharedAtRequest			
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 'operation	al' state		
ensure that			
when	when		
the IUT is triggered to request new Authorization Ticket (AT)			
then	then		
the IUT sends a EtsiTs103097Data to the AA			
containing EtsiTs102941Data			
containing authorizationRequest			
containing sharedAtRequest			
containing requestedSubjectAttributes			
containing appPermissions			
and	and not containing certIssuePermissions		

TD L	OFODKLITO C AUTU 44 DV	
TP ld	SECPKI_ITS-S_AUTH_11_BV	
	Check that ITS-S sends Authorization request containing EC signature	
Summary	Check that the EC signature of the Authorization request contains valid hash algorithm	
	Check that the ecSignature DataHash is calculated over the sharedATRequest	
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' stat	e	
and the AA in 'operation	nal' state	
ensure that		
when		
the IUT is triggered to request new Authorization Ticket (AT)		
then		
the IUT sends a EtsiTs103097Data to the AA		
containing EtsiTs102941Data		
containing authorizationRequest		
containing ecSignature		
containing structure of type EtsiTs103097Data-SignedExternalPayload		
containing hashId		
indicating supported hash algorithm (HASH_ALG)		
and containing tbsData		
	containing payload	
	containing extDataHash	
indicating hash of sharedATRequest using HASH_ALG		

TP Id	SECPKI_ITS-S_AUTH_12_BV		
	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	e		
and the AA in 'operation	al' state		
ensure that	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		
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	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			
cor	containing hashld		
	indicating supported hash algorithm		

TP ld	SECPKI_ITS-S_AUTH_14_BV	
_	Check that the ecSignature of the Authorization request is signed with EC certificate	
Summary	Check that the signature over tbsData computed using the private key corresponding to	
	the EC's verification public key	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_ITS-S	
PICS Selection		
	Expected behaviour	
with		
the IUT is enrolled with 0	CERT_EC certificate	
and the AA in 'operation	al' state	
ensure that		
when		
the IUT is triggered to request new Authorization Ticket (AT)		
then		
the IUT sends a EtsiTs103097Data to the AA		
containing EtsiTs102941Data		
containing au	containing authorizationRequest	
containing	containing ecSignature	
containing structure of type EtsiTs103097Data-SignedExternalPayload		
containing signer		
	indicating HashedId8 of the CERT_EC certificate	
COI	ntaining 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 'operation		
and the EA in 'operation		
authorized with CER	RT_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		
an	d containing cyphertext	
	containing encrypted representation	
	of structure EtsiTs103097Data-SignedExternalPayload	

	0.0000000000000000000000000000000000000		
TP ld	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	e		
and the AA in 'operation	and the AA in 'operational' state		
ensure that			
when	when		
the IUT is triggered to request new Authorization Ticket (AT)			
then			
the IUT sends a EtsiTs103097Data to the AA			
containing 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' sta	ate	
and the AA in 'operation	and the AA in 'operational' state	
ensure that	ensure that	
when	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 leee1609Dot2Data		
containing	containing content.unsecuredData	

TP Id	SECPKI ITS-S AUTH 18 BV		
IF IU			
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		
Summary			
Defenses	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'			
and the AA in 'opera	ational' state		
ensure that			
when			
55	red 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		
ar	and containing signer		
	containing self		
ar	nd 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	e	
and the AA in 'operational' state		
ensure that		
when	. A	
	o request new Authorization Ticket (AT)	
then	T-102007D-1- 1- 1h - 1 1	
	Ts103097Data to the AA	
containing EtsiTs	thorizationRequest	
	g ecSignature	
	ning structure of type EtsiTs103097Data-SignedExternalPayload	
	ntaining signer	
	indicating HashedId8 of EC certificate	
	containing appPermissions	
containing an item of type PsidSsp		
	containing psid	
indicating AID_CERT_REQ		
and containing ssp		
	containing opaque[0] (version)	
	indicating 1	
containing opaque[1] (value)		
	indicating 'Enrollment 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 ld	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 <i>T1</i> and the IUT has not yet received the Authorization Response	
ensure that when the IUT local time is reached the <i>T1</i> + 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_ENR_ITS-S
PICS Selection	
	Expected behaviour
with the IUT being in the 'enrolled' state and the IUT already sent the Authorization Request (<i>M</i>) to AA ensure that when the IUT is triggered to re-send an AuthorizationRequestMessage to AA then the IUT sends <i>M</i> 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_ENR_ITS-S	
PICS Selection		
Expected behaviour		
with		
the IUT being in the 'enr	olled' state	
and the IUT has sent the	and the IUT has sent the Authorization Request more than 1 time	
ensure that		
when		
the IUT receives an Authorization Response		
then		
the IUT stops sending Authorization Requests to AA		

TP ld	SECPKI_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_ENR_ITS-S
PICS Selection	
	Expected behaviour
with	·
the IUT being in th	e 'enrolled' state
and the IUT has st	arted sending the Authorization Request
ensure that	·
when	
the IUT sent the PIXIT_AUTH_MAX_N1 Authorization Request messages	
then	·
the IUT stops s	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_ENR_ITS-S	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the	e 'enrolled' state	
and the IUT has sta	arted 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 s	ending an Authorization Request messages	

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 th	ne CERT_RCA_NEW	
and the IUT has receive	d the TLM CTL	
containing the CERT	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 Cl	ERT_RCA	
and the IUT has receive	and the IUT has received the TLM CTL	
not containing the	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	s CAM	

TD L	OCCUPATION OF THE COUNTY	
TP ld	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 CER	RT_RCA	
and the IUT does not have the CERT_AA_NEW		
and the IUT has received the RCA CTL		
containing the CERT	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 ld	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 downloa	aded the TLM CTL	
containing nextUpda	nte control of the co	
indicating timesta	indicating timestamp T1	
and containing CPOC URL		
ensure that		
when		
the T1 < CURRENT TIME		
then		
the IUT sends a requ	the IUT sends a request to the CPOC for a new CTL	

	T	
TP ld	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 downlo	aded the RCA CTL	
containing nextUpda	ate	
indicating timest	indicating timestamp T1	
and containing RCA DC URL		
ensure that		
when		
the T1 < CURRENT TIME		
then		
the IUT sends a req	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	PId SECPKI_ITS-S_CTLDIST_02_BV	
Summary	ummary Check that the IUT retransmits the updated Delta CTL	
Reference	ETSI TS 103 601 [6], clause 4.2.1.4	
Configuration	CFG_CXL_P2P	
PICS Selection	UC-SEC-05.2	

Expected behaviour

with

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

containing ctlSequence (SN)

ensure that

when

the IUT has received the Delta CTL containing ctlSequence

indicating value greater than SN

then

the IUT is started to broadcast the received Delta CTL

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

TP Id	SECPKI_ITS-S_CTLDIST_03_BV
Summary	Check that the IUT is using the proper BTP port to broadcast the Delta CTL
Reference	ETSI TS 103 601 [6], clause 5.4.4
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-05.2, X_PICS
Expected behaviour	

with

the IUT is configured to support P2P **X_DISTRIBUTION** distribution and the IUT has received the Delta **X_DISTRIBUTION** message

ensure that

when

the IUT is triggered to broadcast the Delta X_DISTRIBUTION message

then

the IUT sends the **X_MESSAGE** using the BTP port 2014

			Permutation table	
_	V DISTRIBILITION	V MESSACE		V DICC

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

TP ld	SECPKI_ITS-S_CTLDIST_04_BV	
Summary	heck that the IUT stops to redistribute the Delta CTL if another node is also sending it	
Reference	ETSI TS 103 601 [6], clause 5.3.1	
Configuration	CFG_CXL_P2P	
PICS Selection	UC-SEC-05.2	
English to the Control of the Contro		

Expected behaviour

with

the IUT is configured to support P2P Delta **X_DISTRIBUTION** distribution and the IUT has started broadcasting the Delta **X_DISTRIBUTION** message

signed with **X_CERTIFICATE** and containing ctlSequence (**SN**)

ensure that

when

the IUT has received the Delta X_DISTRIBUTION

signed with **X_CERTIFICATE** and containing ctlSequence

indicating value equal or higher than SN

then

the IUT stops broadfcasting the Delta X_DISTRIBUTION

signed with **X_CERTIFICATE** and containing ctlSequence (**SN**)

	Permutation table		
X	X_DISTRIBUTION	X_CERTIFICATE	X_PICS
Α	ECTL	CERT_TLM	PICS_SECPKI_ECTL_BROADCAST
В	RootCA CTL	CERT_IUT_A_RCA	PICS_SECPKI_CTL_BROADCAST

Expected behaviour		
PICS Selection	UC-SEC-06.1	
Configuration	CFG_CXL_P2P	
Reference	ETSI TS 103 601 [6], clause 5.3.4.3	
Summary	Check that the IUT requests the Delta CTL using P2P protocol when no CTL information available	
TP ld	SECPKI_ITS-S_CTLDIST_05_BV	

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 ${\tt ContributedExtensionBlock}$

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

indicating etsiHeaderInfoContributorId (2)

containing an item of type EtsiTs102941CtlRequest

containing issuerId

indicating HashedID8 of the CERT

and not containing lastKnownCtlSequence

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

TP ld	SECPKI_ITS-S_CTLDIST_06_BV	
Summary	Check that the IUT requests the Delta CTL using P2P protocol when new CTL information	
	is required	
Reference		
Configuration	CFG_CXL_P2P	
PICS Selection	UC-SEC-06.1	
	Expected behaviour	
with		
the IUT is configured to	support P2P Delta CTL distribution	
and the IUT contains va	lid TLM or/and RootCA certificate (<i>CERT</i>)	
and the IUT contain the	CERT CTL information	
containing ct1Sequ	ence	
indicating (SN)		
ensure that		
when		
	the IUT is triggered to request the CTL information, associated with CERT	
then		
	the IUT starts sending Secured GN messages	
<pre>containing contributedExtensions</pre>		
containing an	containing an item of type ContributedExtensionBlock	
containing	containing contributorId	
<pre>indicating etsiHeaderInfoContributorId (2)</pre>		
containing an item of type EtsiTs102941CtlRequest		
containing issuerId		
indicating HashedID8 of the CERT		
and co	ontaining lastKnownCtlSequence	
ind	indicating SN	
NOTE: This TP is applied	d for both: ECTL and RootCA CTL handling behaviour.	

TDIA	OFFICIAL ITO C. OTLINICT OF DV	
TP ld	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		
	to support P2P Delta CTL distribution	
	valid TLM or/and RootCA certificate (CERT)	
	the CERT CTL information	
containing ctlSeq		
indicating (SA	0	
ensure that when		
	the Secured GN Message	
	ntributedExtensions	
	an item of type ContributedExtensionBlock	
_	••	
<pre>containing contributorId indicating etsiHeaderInfoContributorId (2)</pre>		
containing an item of type EtsiTs102941CtlRequest		
	ntaining issuerId	
001	indicating HashedID8 of the CERT	
and	and containing lastKnownCtlSequence	
indicating value higher than SN		
then		
	nding Secured GN messages	
	containing contributedExtensions	
containing	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 app	olied for both: ECTL and RootCA CTL handling behaviour.	

TP ld	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	
	lid TLM or/and RootCA certificate (<i>CERT</i>)	
and the IUT has receive	d a Delta CTL message (M)	
signed using <i>CERT</i>		
and containing ctlSequence		
indicating (SN)		
ensure that		
when		
the IUT receives the		
<pre>containing contributedExtensions</pre>		
containing an item of type EtsiTs102941CtlRequest		
containing issuerId		
indicating HashedID8 of the CERT		
and containing lastKnownCtlSequence		
indicating value less than SN		
then		
	casting the Delta CTL (M)	
NOTE: This TP is applied	d for both: ECTL and RootCA CTL handling behaviour.	

TP ld	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	
and the IUT is configure and the IUT has started at the time <i>T</i>	support P2P Delta CTL distribution d to broadcast the Delta CTL during <i>D1</i> time to broadcast a Delta CTL message
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	d for both: ECTL and RootCA CTL handling behaviour.
NOTE 2: The D1 value sha	all be provided as a PIXIT.

TP ld	SECPKI ITS-S CTLDIST 10 BV	
IT IU		
Summary	Check that the IUT stops broadcasting the requested Delta CTL when broadcasting period	
	is expired	
Reference	ETSI TS 103 601 [6], clause 5.3.6	
Configuration	CFG_CXL_P2P	
PICS Selection	UC-SEC-06.2	
	Expected behaviour	
with		
the IUT is configured to	support P2P Delta CTL distribution	
and the IUT is configure	d to broadcast the requested Delta CTL during D2 time	
and the IUT has started	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 $T + D2$		
then		
the IUT stops broade	casting the Delta CTL	
NOTE 1: This TP is applied for both: ECTL and RootCA CTL handling behaviour.		
NOTE 2: The D2 value shall be provided as a PIXIT.		

5.2.6 CRL handling

TP ld	SECPKI_ITS-S_CRL_01_BV	
Summary	Check that the IUT accept the received CRL information	
Reference	ETSI TS 102 941 [1], clause 5.4.2	
Configuration	CFG_CXL_P2P	
PICS Selection		
	Expected behaviour	
with	·	
and the IUT contains va	lid RootCA certificate (CERT_IUT_A_RCA)	
and the IUT has not rec	eived 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		

TP Id	SECPKI_ITS-S_CRL_02_BV	
Summary	Check that the IUT can handle the revocation of its own AA	
Reference	ETSI TS 102 941 [1], clause 5.4.2	
Configuration	CFG_CXL_P2P	
PICS Selection		
Expected behaviour		
with and the IUT contains valid RootCA certificate (CERT_IUT_A_RCA) and the IUT is authorized using AT certificate signed with CERT_IUT_A_B_AA ensure that when the IUT received the CRL information from the DC containing revocation of CERT_IUT_A_B_AA then the IUT switched to 'enrolled' state		

TP Id	SECPKI 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
and the IUT been enroll signed with CERT_I ensure that when the IUT the IUT rece	lid RootCA certificate (CERT_IUT_A_RCA) ed with EC certificate UT_A_EA certificate eived the CRL information from the DC ation of CERT_IUT_A_EA

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 val	lid RootCA certificate (CERT_IUT_A_RCA)		
and the IUT been enrolle	and the IUT been enrolled with EC certificate		
signed with EA certif	signed with EA certificate		
signed with CERT_IUT_A_RCA			
ensure that			
when			
the IUT the IUT received the CRL information from the DC			
containing revocation of CERT_IUT_A_RCA			
then			
the IUT switches to t	he 'initial' state		

TP Id	SECPKI_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 va	lid RootCA certificate (CERT_IUT_A_RCA)		
and the IUT has not rec	eived yet the CRL information issued by the RootCA		
and the IUT is authorize	d 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 S	ecured Message		
signed with AT certificate			
signed with CERT_IUT_A_B_AA			
then			
the IUT discards this message			

5.2.7 CRL distribution

TP ld	SECPKI_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	
	d to support P2P CRL distribution
and the IUT contains	s 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 br	oadcasting 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 configur	ed to support P2P CRL distribution		
and the IUT contain	ins valid RootCA certificate (CERT_IUT_A_RCA)		
and the IUT has no	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 va	lid 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	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 broadd	casting the CRL	
NOTE: The D1 value sha	all be provided as a PIXIT	

TP ld	PECCHALITE & COLDIET 03 DV	
TP IQ	SECPKI_ITS-S_CRLDIST_03_BV	
Summary	Check that the IUT stops broadcasting the CRL when the CRL became outdated because	
	of the nextUpdate value	
Reference	ETSI TS 103 601 [6], clause 5.4.3	
Configuration	CFG_CXL_P2P	
PICS Selection	UC-SEC-07.2	
	Expected behaviour	
with		
the IUT is configured to	support P2P CRL distribution	
and the IUT contains va	alid RootCA certificate (CERT_IUT_A_RCA)	
	y received the CRL information from DC	
	containing nextUpdate (N)	
and the IUT has started broadcasting the received CRL		
ensure that	3	
when		
the IUT current time	e is equal or more than N	
then	·	
the IUT stops broad	dicasting the CRL	

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

TP ld	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		
	support P2P CRL distribution	
and the IUT contains va	lid RootCA certificate (CERT_IUT_A_RCA)	
and the IUT has never r	eceived a CRL information issued by the RootCA	
ensure that		
when		
the IUT is triggered to request the CRL		
then		
the IUT starts sending Secured GN messages		
<pre>containing contributedExtensions</pre>		
containing an item of type ContributedExtensionBlock		
containing contributorId		
<pre>indicating etsiHeaderInfoContributorId (2)</pre>		
containin	containing an item of type EtsiTs102941CrlRequest	
	ning issuerId	
inc	dicating HashedID8 of the CERT_IUT_A_RCA	
and not containing lastKnownUpdate		

TDII	OFORKUITO O ORUBIOT OF BY		
TP ld	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 va	lid RootCA certificate (CERT_IUT_A_RCA)		
and the IUT has already	received the CRL information issued by the RootCA		
containing thisUpd	ate (T)		
ensure that			
when	when		
the IUT is triggered t	the IUT is triggered to request the CRL		
then			
the IUT starts sending Secured GN messages			
<pre>containing contributedExtensions</pre>			
containing an item of type ContributedExtensionBlock			
containing contributorId			
indicating etsiHeaderInfoContributorId (2)			
containing an item of type EtsiTs102941CrlRequest			
contai	containing issuerId		
ind	licating HashedID8 of the CERT_IUT_A_RCA		
	ontaining lastKnownUpdate		
indicating T			
L	Ŭ		

TP Id	SECPKI_ITS-S_CRLDIST_06_BV	
Summary	Check that the IUT starts broadcasting the CRL using P2P protocol when CRL information	
	has been requested by another ITS station	
Reference	ETSI TS 103 601 [6], clause 5.4.2	
Configuration	CFG_CXL_P2P	
PICS Selection	UC-SEC-08.2	
	Expected behaviour	
with		
	support P2P CRL distribution	
and the IUT contains va	alid RootCA certificate (CERT_IUT_A_RCA)	
and the IUT has alread	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		

TP ld	SECPKI ITS-S CRLDIST 06 BV
Summary	Check that the IUT stops broadcasting the CRL when distribution time (d2) has been expired after receiving of CRL request
Reference	ETSI TS 103 601 [6], clause 5.4.2
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-08.2
	Expected behaviour
and the IUT contains va and the IUT has already at the time <i>T</i> and the IUT has started and the IUT is configure ensure that when	ed to limit the broadcasting time to D2 sis equal or more than T+D1

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	CECDIAL CV CEDICEN OF DA		
1710	SECPKI_CA_CERTGEN_01_BV		
Summary	Check that the issuing certificate has version 3		
Reference	ETSI TS 103 097 [2], clause 6		
Reference	IEEE Std 1609.2 [3], clause 6.4.3		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
CA is in 'operation	nal' state		
ensure that			
when			
the CA is requ	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
•	ETSI TS 103 097 [2], clause 6
Reference	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' sta	te
CA is initialized with the	explicit certificate (CERT_IUT_A_CA)
ensure that	
when	
the CA is requested	to issue the explicit certificate
then	
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	

	0-0-0-0	
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	
Deference	ETSI TS 103 097 [2], clause 6	
Reference	IEEE Std 1609.2 [3], clause 6.4.3	
DIGG C. L. Albert	PICS_GN_SECURITY AND PICS_SEC_IMPLICIT_CERTIFICATES AND	
PICS Selection	PICS SEC EXPLICIT CERTIFICATES	
	Expected behaviour	
with	•	
CA is in 'operational' stat	te	
CA is initialized with the	explicit certificate (CERT_IUT_A_CA)	
ensure that		
when		
the CA is requested	to issue the implicit certificate	
then	·	
this certificate is of type EtsiTs103097Certificate		
containing version		
indicating 3		
containing type		
indicating 'implicit'		
and containing toBeSigned		
containing verifyKeyIndicator		
	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
Reference	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' sta	ate
CA is initialized with the	e implicit certificate (CERT_IUT_I_CA)
ensure that	
when	
the CA is requested to issue the implicit certificate	
then	
this certificate is of type EtsiTs103097Certificate	
containing version	
indicating 3	
containing type	
indicating 'implicit'	
and containing toBeSigned	
containing verifyKeyIndicator	
containing reconstructionValue	
and not containii	ng 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	
Reference	IEEE Std 1609.2 [3], clause 6.4.3	
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_IMPLICIT_CERTIFICATES AND	
PICS Selection	PICS_SEC_EXPLICIT_CERTIFICATES	
	Expected behaviour	
with		
CA is in 'operational' state		
CA is initialized with the 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 ld	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' sta	te	
ensure that		
when		
the CA is issuing the	certificate	
then		
	/pe EtsiTs103097Certificate	
containing toBeS	igned	
containing id		
indicating 'none' or 'name'		
and containing cracald		
indicating '000000'H		
and containing crlSeries		
indicating		
and not containing certRequestPermissions		
and not containing canRequestRollover		

TP ld	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
Α	sha256AndDigest	ISHA-256	ecdsaNistP256 or ecdsaBrainpoolP256r1	PICS_SEC_SHA256 AND PICS_SEC_BRAINPOOL_P256R1
В	sha384AndDigest	SHA-384	IecdsaBrainnooiP384r1	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' sta	ate		
the CA is authorized wit	h CA certificate		
containing toBeSign	ed		
containing region			
indicating RE	GION		
ensure that			
when			
the CA is requested to issue the certificate			
containing circular region restriction			
then	10 · · · · · · · · · · · · · · · · · · ·		
	ertificate of type EtsiTs103097Certificate		
	containing toBeSigned		
•	containing region		
containing circularRegion			
	ning centre		
	dicating a point inside the REGION		
	ontaining radius		
i inc	dicating a value when all points of the circle are inside the REGION		

TP ld	SECPKI_CA_CERTGEN_06_BV	
	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		
containing toBeSigne		
containing region		
indicating REG	GION	
ensure that		
when	- Versian than a self-ranks	
the CA is requested to issue the certificate		
9	gular region restriction	
then		
the CA issues the certificate of type EtsiTs103097Certificate containing toBeSigned		
containing region		
containing region containing rectangularRegion		
containing items of type RectangularRegion		
containing northwest		
indicating a point inside the REGION		
	I containing southeast	
indicating a point on the south and east from northwest and inside the REGION		

TP ld	SECPKI_CA_CERTGEN_07_BV
Summary	Check that CA is able to issue certificate with polygonal region validity restriction where: - the polygonal certificate validity region contains at least three points - the polygonal certificate validity region does not contain intersections - the polygonal certificate validity region is inside the validity region of the issuing certificate
Reference	IEEE Std 1609.2 [3], clauses 6.4.21, 6.4.17 and 5.1.2.4
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_POLYGONAL_REGION
	Expected behaviour
containing polyg then the CA issues the containing to Best containing re containin containin	th CA certificate ed n EGION to issue the certificate onal region validity restriction ertificate of type EtsiTs103097Certificate Signed

TP Id	SECPKI_CA_CERTGEN_08_BV	
_	Check that the CA is able to issue the certificate with identified region validity restriction	
Summary	contains values that correspond to numeric country codes as defined by United Nations Statistics Division [i.8]	
Reference	IEEE Std 1609.2 [3], clause 6.4.23	
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_IDENTIFIED_REGION	
	Expected behaviour	
with		
CA is in 'operation	nal' state	
the CA is authoriz	ed with CA certificate	
containing toB	eSigned	
containing region		
indicati	ng REGION	
ensure that		
when		
the CA is requ	ested to issue the certificate	
containing	identified region validity restriction	
indicati	ng country or area COUNTRY	
then		
	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 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		
ii iu	Check that the identified region validity restriction of the subordinate certificate is included		
Summary	in the identified region validity restriction of the issuing certificate		
Reference	IEEE Std 1609.2 [3], clauses 6.4.17 and 5.1.2.4		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_IDENTIFIED_REGION		
r ico Selection	Expected behaviour		
with	Expected benaviour		
the CA is in 'operational	ctate		
and the CA is authorized			
containing toBeSign			
containing region			
,	entifiedRegion		
	g countryOnly		
	ting COUNTRY		
	ning countryAndRegions		
	ning countryOnly		
inc	dicating COUNTRY		
and co	ontaining regions		
inc	dicating REGIONS		
	ning countryAndSubregions		
	ining country		
	dicating COUNTRY		
	containing regionAndSubregions		
	dicating REGIONS and SUBREGIONS		
ensure that			
when the CA issued the ce	artificato		
containing toBeS			
containing tobec			
•	gidentifiedRegion		
then	J Marianian togram		
	ype EtsiTs103097Certificate		
containing toBeS			
containing re-			
containing	g identifiedRegion		
	ning countryOnly		
	dicating value = COUNTRY		
	taining countryAndRegions		
со	ntaining countryOnly		
	indicating value = COUNTRY		
an	d containing regions		
containing region identifiers contained in REGIONS			
	staining countryAndSubregions		
co	ntaining country		
	indicating value = COUNTRY		
an	and containing regionAndSubregions		
	containing region identifiers contained in REGIONS and containing subRegion identifiers contained in SUBREGIONS for every region		
	and containing subregion identifiers contained in SUBREGIONS for every region		

5.3.1.3 Check ECC point type of the certificate signature

TP I	TP Id SECPKI_CA_ CERTGEN_10_BV_XX			
Summary			ficate signature contains ECC point of type set to either	
Sulli	illialy	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], clauses 6.3.29, 6.3.30 and 6.3.31		
PICS	Selection	PICS_GN_SECURI	TY AND PICS_SEC_EXPLICIT_CERTIFICATES AND X_PICS	
			Expected behaviour	
with				
th	ne CA is in 'operational'	state		
ensu	ire that			
V	/hen			
	the CA issued the ex	plicit certificate		
th	nen			
	this certificate is of ty		rtificate	
	containing signat			
		SIGNATURE		
	containing			
	containing x-only			
		ining compressed-y-		
	or containing compressed-y-1			
	Permutation table			
XX	X_SIGNATURE		X_PICS	
Α	ecdsaNistP256Signatu	ıre		
В	ecdsaBrainpoolP256r1	Signature	PICS_SEC_BRAINPOOL_P256R1	
С	C ecdsaBrainpoolP384r1Signature PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1			

5.3.1.4 Check ECC point type of the certificate public keys

PKI_CA_CERTGEN_11_BV		
Check that the certificate verification key contains ECC point of type set to either		
compressed_lsb_y_0, compressed_lsb_y_1 or uncompressed		
Std 1609.2 [3], clause 6.4.38		
_GN_SECURITY AND PICS_SEC_EXPLICIT_CERTIFICATES AND X_PICS		
Expected behaviour		
certificate		
siTs103097Certificate		
yIndicator		
cationKey		
<u>KEY</u>		
uncompressed		
ng compressed-y-0		
or containing compressed-y-1		
Permutation table		
X_PICS		
PICS_SEC_BRAINPOOL_P256R1		
PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1		

TP Id	d	SECPKI_CA_CERTGEN_12_BV	
C	nmary	Check that the certificate encryption key contains ECC point of type set to either	
Sum		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			
th	ne CA is in 'operational'	' state	
ensu	ire that		
V	vhen		
	the CA issued the ce	ertificate	
tł	nen		
	this certificate is of ty	/pe EtsiTs103097Certificate	
	containing toBeS	igned	
	containing en		
		g publicKey	
	containing X_KEY		
	containing uncompressed		
		ontaining compressed-y-0	
	or containing compressed-y-1		
	Permutation table		
XX	X_KEY	X_PICS	
Α	eciesNistP256		
В	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'			
and the CA is authorized	I with explicit certificate		
containing toBeSigne			
containing verifyh			
containing ve			
containing	X_KEY		
ensure that			
when			
the CA issued the ex	plicit certificate		
then			
	rpe EtsiTs103097Certificate		
containing issuer			
referencing the certificate			
	toBeSigned		
	ning verifyKeyIndicator		
cor	containing verificationKey		
containing X_KEY			
indicating KEY			
	and containing signature		
containing X_			
verifiable	verifiable using KEY		
VV V VEV	Permutation table		

Permutation table			
XX	X_KEY	X_SIGNATURE	X_PICS
Α	ecdsaNistP256	ecdsaNistP256Signature	
В	ecdsaBrainpoolP256r1	ecdsaBrainpoolP256r1Signature	PICS_SEC_BRAINPOOL_P256R1
С	ecdsaBrainpoolP384r1	ecdsaBrainpoolP384r1Signature	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1

TP ld	TP Id SECPKI_CA_CERTGEN_13_BV_02		
Summary	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 Israerstianall state			

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

this signature can be verified using public key

reconstructed using VALUE and KEY

	Permutation table		
XX	X_KEY	X_PICS	
Α	ecdsaNistP256		
В	ecdsaBrainpoolP256r1	PICS_SEC_BRAINPOOL_P256R1	
С	ecdsaBrainpoolP384r1	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1	

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 ce	the CA issued the certificate		
containing toBeS	containing toBeSigned		
containing ap	containing appPermissions		
then			
this certificate is of ty	this certificate is of type EtsiTs103097Certificate		
containing toBeŚigned			
containing appPermissions			
containing	containing items of type PsidSsp		
contail	containing psid		
ind	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		
Summary	contained in the certIssuePermissions component in the issuing certificate		
Reference	IEEE Std 1609.2 [3], clauses 6.4.28 and 5.1.2.4		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the CA is in 'operational'	state		
ensure that			
when			
the CA issued the ce	· ···· · · · · · · · · · · · · · · · ·		
containing toBeS			
containing ap	pPermissions		
then	To FloiTo 400007C autiliants		
1	pe EtsiTs103097Certificate		
containing issuer			
	referenced to the certificate		
	containing toBeSigned containing certIssuePermissions		
	containing terms 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		
9	and containing toBeSigned		
containing ap			
	items of type PsidSsp		
	ning psid		
cor	contained in the X_PSID_RANGE_LIST		
	as a psid		

TP Id	SECONI CA CERTOEN 16 DV	
I P I a	SECPKI_CA_CERTGEN_16_BV	
Summary	Check that all PSID entries of the certIssuePermissions component of the certificate are	
Sammar y	unique	
Reference	IEEE Std 1609.2 [3], clauses 6.4.28 and 5.1.2.4	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the CA is in 'operational	'state	
ensure that		
when		
the CA issued the ce	ertificate	
containing toBeS	Signed	
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		
Summani	Check that SSP field in each entry of the appPermissions component of the AT certificate		
Summary	is equal to or a subset of the SSP Range in the corresponding issuing entry		
Reference	IEEE Std 1609.2 [3], clauses 6.4.28 and 5.1.2.4		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the CA is in 'operational	state		
ensure that			
when			
the CA issued the certi			
containing toBeSign			
containing appPe	rmissions		
then	- Ft-:T-4000070-:::::		
	e EtsiTs103097Certificate		
containing issuer referenced to the	cortificate		
containing toBe			
	ertIssuePermissions		
	items of type PsidGroupPermissions		
_	ing eeType		
	ating app(0)		
	ntaining subjectPermissions		
	aining 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			
	s of type PsidSsp		
	containing psid		
•	value equal to X_PSID_AA		
	containing ssp		
Indicating	value permitted by X_SSP_AA [X_PSID_AA]		

5.3.1.7 Check time validity restriction in the chain

TP Id SECPKI_CA_CERTGEN_18_BV			
Summary	Check that the validityPeriod of the subordinate certificate is inside the validityPeriod of the issuing certificate		
Reference	IEEE Std 1609.2 [3], clause 5.1.2.4		
PICS Selection	PICS_GN_SECURITY		
	Expected behaviour		
with			
the CA is in 'operational'			
and the CA is authorized			
containing toBeSigned			
containing validityP	eriod		
containing start	TART MALIRITY OA		
	TART_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 dur	containing duration		
indicating va	alue <= 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 Enrollment request handling

TP ld	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	PICS Selection		
	Expected behaviour		
with			
the EA is in 'operational'	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			

TDII	OFORKLEA FAIR ROLL OF RI	
TP ld	SECPKI_EA_ENR_RCV_02_BI	
Summary	Check that EA does not accept Enrollment rekeying request when enrollment 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		
	EnrollmentRequestMessage	
	crypted EtsiTs103097Data-Signed	
containing sig		
containing of		
	g Hashedld8 value	
referenced the certificate (CERT)		
cor	ntaining 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		
	indicating other value than 1	
	or containing opaque[1] (value)	
	indicating 'Enrollment Request' (bit 1) set to 0	
then	malouming Emoliment Request (sit 1) set to 0	
******	an EnrollmentResponseMessage	
containing InnerEC	·	
containing respo		
	niedpermissions'	
<u></u>		

TP Id	SECPKI EA ENR RCV 04 BI		
11 14	Enroll the ITS-Station, but the outer signature, created with the canonical private key,		
Summary	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 'operationa	l' state		
ensure that			
when	when		
the IUT receives an	EnrollmentRequestMessage		
	containing an outer signature		
signed with an unknown canonical private key			
then			
the IUT answers wit	the IUT answers with an EnrollmentResponseMessage		
containing InnerECResponse			
containing responseCode			
indicating 'invalidsignature'			
	ning a certificate		
and not contain	mig 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	when		
the IUT receives an I	EnrollmentRequestMessage		
containing an Inn	erEcRequest		
containing Ho	ostname		
indicating an unknown canonical-ID			
then			
the IUT answers with an EnrollmentResponseMessage			
containing InnerECResponse			
containing response	onseCode		
indicating un	knownits'		
and not containi	ng a certificate		

TP ld	SECPKI_EA_ENR_RCV_06_BI	
Summary	Enroll the ITS-Station, but the CSR requests more permissions than the issuer allows,	
Summary	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	l' state	
ensure that		
when		
the IUT receives an	EnrollmentRequestMessage	
containing an Ini	·	
containing SSP		
indicating more permissions than EA allows		
then		
the IUT answers with an EnrollmentResponseMessage		
containing InnerECResponse		
containing responseCode		
indicating 'de	eniedpermissions'	
and not contain	ning a certificate	

Summary	Enroll the ITS-Station, but the CSR requests an AID permission that the issuer does not		
Summary	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 Inn	erEcRequest		
containing SS	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			

SECPKI_EA_ENR_RCV_07_BI

TP Id

TP ld	SECPKI_EA_ENR_RCV_08_BI	
Summary	Enroll the ITS-Station, but the expiring date of the CSR is before the start date of the EA	
Reference	ETSI TS 102 941 [1]	
Configuration	CFG_ENR_EA	
PICS Selection		
	Expected behaviour	
with		
the EA is in 'operational'	state	
ensure that		
when		
the IUT receives an I	the IUT receives an EnrollmentRequestMessage	
containing an Inn	containing an InnerEcRequest	
containing Va	ılidityPeriod	
indicating	end validity time	
less than the start date of the EA		
then		
the IUT answers with	n an EnrollmentResponseMessage	
containing InnerECResponse		
containing respo	containing responseCode	
indicating 'de	indicating 'deniedpermissions'	
and not containing a certificate		

TP ld	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 I	EnrollmentRequestMessage	
	containing an InnerEcRequest	
containing Va	•	
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 containi	and not containing a certificate	

TD	OFORK FA FAIR ROLL 40 RI	
TP ld	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	l' state	
ensure that		
when		
the IUT receives an EnrollmentRequestMessage		
containing an Ini	containing an InnerEcRequest	
containing Va	alidityPeriod	
indicating	g a value greater than the ValidityPeriod of the EA	
then		
the IUT answers wit	h 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 I	the IUT receives an EnrollmentRequestMessage		
containing an Inn	containing an InnerEcRequest		
containing Va	containing ValidityPeriod		
containing	containing start date		
indicating a value greater than the start date of the EA			
then			
the IUT answers with an EnrollmentResponseMessage			
containing InnerECResponse			
containing response	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		
	EnrollmentRequestMessage	
containing an Inn	•	
containing Va		
indicating a value greater than 3 years		
then		
	n an EnrollmentResponseMessage	
containing InnerECResponse		
Ŭ.	containing responseCode	
indicating 'deniedpermissions'		
and not containing a certificate		

FP 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]		
Configuration	CFG_ENR_EA		
PICS Selection			
	Expected behaviour		
with			
the EA is in 'operational'	state		
ensure that			
when	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 contain	and not containing a certificate		

TP ld	SECPKI_EA_ENR_RCV_14_BV	
Summary	Check that EA send the same response for the repeated EC request	
Reference	ETSI TS 103 601 [6], clause 5.1	
Configuration	CFG_ENR_EA	
PICS Selection	PICS_SECPKI_ENROLLMENT_RETRY	
	Expected behaviour	
with		
the EA is in 'operational	l' state	
and the EA already rece	eived EnrollmentRequestMessage (<i>REQ</i>)	
having checksum (C	CS)	
and the EA has sent the	e ÉnrollmentResponseMessage (<i>RES</i>)	
	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 enrollment when message generation time is too far in the
Summary	past
Reference	ETSI TS 103 601 [6], clause 5.1.4
Configuration	CFG_ENR_EA
PICS Selection	PICS_SECPKI_ENROLLMENT_RETRY
	Expected behaviour
with	
the EA is in 'operational'	state
and the EA already rece	eived the EnrollmentRequestMessage (<i>REQ</i>)
containing generatio	
and having checksur	m (CS)
ensure that	
when	
the IUT receives an	EnrollmentRequestMessage
at the moment T	R2
indicating TR	2 > TG + PIXIT_EA_ENROLLMENT_TIMEOUT
and having checksum	
indicating value equal to CS	
then	
	n an EnrollmentResponseMessage
containing responseCode	
indicating der	niedrequest
NOTE: PIXIT_EA_ENRO	DLLMENT_TIMEOUT shall be set as a TP parameter.

5.4.2 Enrollment 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	
containing e	es an EnrollmentRequestMessage ncKey g an encrypted AES key (SYMKEY)
then	
containing ci being enc	ers with an EnrollmentResponseMessage pherText rypted using SYMKEY an ETSI TS 103 097 [2] approved algorithm

TP ld	SECPKI_EA_ENR_03_BV
Summary	The outermost structure is an EtsiTs103097Data-Encrypted structure containing the component recipients containing one instance of RecipientInfo of choice pskRecipInfo, which contains the HashedId8 of the symmetric key used by the ITS-S to encrypt the 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 enrollment 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	
Exported behaviour	

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 hashld

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 ld	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 [i.2] 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	then		
the IUT sends an EtsiTs103097Data-Encrypted structure			
containing an encr	ypted EtsiTs103097Data-Signed structure		
containing tbsDa	ata		
containing he	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	when	
the IUT sends an EnrollmentResponseMessage as an answer for an EnrollmentRequestMessage		
then		
the IUT sends an Ets	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)		

I a	and a responseCode indicating the result of the request
	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	

SECPKI_EA_ENR_08_BV

TP Id

	DESCRIPTION OF THE CO. THE	
TP ld	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	when	
the IUT is requested	to send an EnrollmentResponseMessage	
containing a respo	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 enrollment certificate		

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

TP ld	SECPKI_EA_ENR_11_BV
Summary	Check that signing of enrollment 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 En	rollmentResponseMessage as an answer for an EnrollmentRequestMessage
then	
the IUT sends an EtsiTs103097Data-Encrypted structure	
containing an encrypted EtsiTs103097Data-Signed structure	
containing signe	
declared as a	digest
containing t	he HashedId8 of the EA certificate
containii	ng 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 'Enrollment Response' (5) set to 1

TP ld	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 certific	cate (EC_CERT)	
then		
the EC_CERT		
containing appPermissions		
•	containing an item of type PsidSsp	
containing psid		
	ing AID_CERT_REQ	
and conta	ning ssp ning opaque[0] (version)	
	licating 1	
	ning opaque[1] (value)	
	licating 'Enrollment Request' (bit 0) set to 1	
indicating Emoline Request (bit 0) set to 1		
indicating other bits set to 0		
and NOT containing an item of type PsidSsp		
containing psid		
	ing AID_CTL	
and NOT con	taining an item of type PsidSsp	
containing	psid	
indicat	ring AID_CRL	

5.4.3 Authorization validation request handling

TDII	OFORKLEA ALITHVAL BOY OF BY	
TP Id	SECPKI_EA_AUTHVAL_RCV_01_BV	
	The authorization validation response shall be sent by the EA to the AA across the	
Summary	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	when	
the IUT receives a AuthorizationValidationRequestMessage		
then		
the IUT sends a AuthorizationValidationResponseMessage		
across the refere	across the reference point S4 to the AA	

TP Id	SECPKI EA AUTHVAL RCV 02 BI
11 14	Check that EA does not accept the authorization validation request when
Summary	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	
	AuthorizationValidationRequestMessage
containing EtsiTs	
containing ecSi	
containing s	
containin	
	ting HashedId8 of the certificate EC certificate
	ntaining appPermissions
n	ot containing an item of type PsidSsp
	containing psid
	indicating AID_CERT_REQ
0	r 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	indicating AdditionEdition Request (Sit 2) Set to 0
	an AuthorizationValidationResponseMessage
containing respons	
indicating 'denie	

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
receive	ETSI TS 103 097 [2], clause 7
Configuration	CFG_AVALID_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT receives a	a AuthorizationValidationRequestMessage
containing encKey	<i>y</i>
containing the e	ncrypted symmetric data encryption key (SYMKEY)
then	
the IUT sends a A	authorizationValidationResponseMessage
containing EtsiT	s103097Data-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 ld	SECPKI_EA_AUTHVAL_02_BV		
Summary	To read an authorization validation response, the AA shall receive an EtsiTs103097Data- Encrypted structure, containing a EtsiTs103097Data-Signed structure, containing a EtsiTs102941Data structure, containing an AuthorizationValidationResponse structure		
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2		
Configuration	CFG_AVALID_EA		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the IUT receives a A	the IUT receives a AuthorizationValidationRequestMessage		
then	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
containing EtsiTs10 then the IUT sends a Aut containing EtsiTs1 containing Etsi7 containing a containing	AuthorizationValidationRequestMessage D3097Data-Signed structure (REQDSS) horizationValidationResponseMessage D3097Data-Signed Ts102941Data UthorizationValidationResponse UthorizationValidationResponse UthorizationValidationResponse UthorizationValidationResponse UthorizationValidationResponse UthorizationValidationResponse UthorizationValidationResponse UthorizationValidationResponse
	ing the left-most 16 octets of the 31 M236 digest of REQD33

TP Id	SECPKI_EA_AUTHVAL_04_BV	
	If the responseCode is 0, the AuthorizationValidationResponse structure contains the	
Summary	component confirmedSubjectAttributes with the attributes the EA wishes to confirm, except	
-	for certIssuePermissions which is not allowed to be present	
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2	
Configuration	CFG_AVALID_EA	
PICS Selection		
	Expected behaviour	
ensure that		
when		
the IUT receives a AuthorizationValidationRequestMessage		
and the IUT re	and the IUT responds with a AuthorizationValidationResponseMessage	
containing au	uthorizationValidationResponse	
containing	g responseCode	
indicating 0		
then		
the sent AuthorizationValidationResponseMessage		
contains an a	authorizationValidationResponse	
containing	g confirmedSubjectAttributes	
not cor	taining 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 respond	s with a AuthorizationValidationResponseMessage	
containing authoriz	containing authorizationValidationResponse	
containing response	onseCode	
indicating a value different than 0		
then		
the sent AuthorizationValidationResponseMessage		
contains an authorizationValidationResponse		
not containing confirmedSubjectAttributes		

TP ld	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 receive	es a AuthorizationValidationRequestMessage
then	
the IUT sends	a AuthorizationValidationResponseMessage
containing E	tsiTs103097Data-Signed
containing EtsiTs102941Data	
	ning version
	cating v1 (integer value set to 1)

TP ld	SECPKI_EA_AUTHVAL_07_BV	
Summary	EtsiTs103097Data-Signed.tbsData contains the EtsiTs102941Data as payload and the headerInfo containing psid and generationTime. The psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [i.2] and the generationTime shall be present. All other components of the component tbsdata.headerInfo are not used and absent	
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2	
Configuration	CFG_AVALID_EA	
PICS Selection		
	Expected behaviour	
ensure that when		
the IUT receives a AuthorizationValidationRequestMessage then		
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 ld	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 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			
	uthorizationValidationRequestMessage		
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 the			
•	and containing signer		
declared as a digest			
containing the HashedId8 of the EA certificate			
and containing signature			
computed over tbsData			
using the EA private key			
correspo	nding 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		
	iTs103097Data-Encrypted structure	
containing an encrypted EtsiTs103097Data-Signed structure		
containing signer		
containing dig		
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	
C	containing opaque[1] (value)	
	indicating 'Authorization Validation Response' (bit 4) set to 1	

5.4.5 CA Certificate Request

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

TP 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 ETSLTS 103 097 [2] approved hash algorithm
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_INIT
PICS Selection	
	Expected behaviour
with the IUT being in the '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	
Reference	ETSI TS 103 097 [2], clause 7	
Configuration	CFG_CAGEN_INIT	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the 'init	ial' state	
ensure that		
when		
the IUT is requested to send a CACertificateRequestMessage		
then		
	CertificateRequestMessage	
•	03097Data-Signed structure	
containing hashld		
	ne hash algorithm to be used	
	and containing signer	
indicating 's		
	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		
	An ECC private key is randomly generated, the corresponding public key (verificationKey)		
	is provided to be included in the CaCertificateRequest.		
Summary	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 'initi	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 'initi	al' state	
ensure that		
when	when	
the IUT is requested	the IUT is requested to send a CACertificateRequestMessage	
then	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 'init	ial' state	
ensure that	ensure that	
when	when	
the IUT is requested	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 ld	SECPKI EA CERTGEN 07 BV	
Summary	EtsiTs103097Data-Signed.tbsData contains the EtsiTs102941Data as payload and the headerInfo containing psid and generationTime. The psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [i.2] and the generationTime shall be present. All other components of the component tbsdata.headerInfo are not used and absent	
Reference	ETSI TS 102 941 [1], clause 6.2.1	
Configuration	CFG_CAGEN_INIT	
PICS Selection		
	Expected behaviour	
the IUT being in the 'initensure that when the IUT is requested then the IUT sends a CA containing head containing psi indicating S	with the IUT being in the 'initial' state ensure that when the IUT is requested to send a CACertificateRequestMessage	

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	
Summary	shall restart the initial certificate application process	
Reference	ETSI TS 102 941 [1], clause 6.2.1	
Configuration	CFG_CAGEN_REKEY	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the 'ope	erational' 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 CACert	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: hashld, tbsData, signer and signature. The hashld 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	e 'operational' state	
ensure that		
when		
	sted to perform a CA certificate rekeying procedure	
then		
	CertificateRekeyingMessage	
	s 103097Data-Signed structure	
containing h		
	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 'c	perational' state		
ensure that			
when			
the IUT is request	the IUT is requested to perform a CA certificate rekeying procedure		
then			
the sends a CACertificateRekeyingMessage			
containing tbsData			
containing C	containing CaCertificateRequestMessage		

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

TP ld	SECPKI EA CERTGEN 12 BV	
Summary	Check that the CaCertificateRekeyingMessage is permitted by CA certificate	
•	ETSI TS 102 941 [1], clause 6.2.1	
Configuration	CFG_CAGEN_REKEY	
PICS Selection	OI G_OAGEN_INERE I	
FICS Selection	Expected behaviour	
with	Expected benaviour	
the IUT being in the 'ope	erational' state	
ensure that	national state	
when		
the IUT is requested	to perform a CA certificate rekeying procedure	
then	31	
the sends a CACertif	ficateRekeyingMessage	
being an EtsiTs103	being an EtsiTs103097Data-Signed structure	
and containing the	and containing tbsData	
and containing	and containing signer	
containing dig	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	

5.5 AA behaviour

5.5.0 Overview

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

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

5.5.1 Authorization request handling

TP Id	SECPKI_AA_AUTH_RCV_01_BV	
	Check that the AA is able to decrypt the AuthorizationRequestMessage using the	
	encryption private key corresponding to the recipient certificate	
C	Check that the AA is able to verify the inner signature	
Summary	Check that the AA is able to verify the request authenticity using the hmacKey verification	
	Check that the AA sends the AuthorizationValidationRequest message to the	
	correspondent EA	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_AA	
PICS Selection	PICS_PKI_AUTH_POP	
	Expected behaviour	
with		
the AA in 'operational' s		
	certificate CERT_AA	
	ptionKey (AA_ENC_PUB_KEY)	
ensure that		
when		
	e EtsiTs103097Data-Encrypted message	
	ent.encryptedData	
containing re		
	g the instance of RecipientInfo	
	ining certRecipInfo	
cc	ontaining recipientId	
	indicating HashedId8 of the certificate CERT_AA	
ar	nd containing encKey	
	indicating symmetric key (S_KEY)	
	encrypted with the private key correspondent to the AA_ENC_PUB_KEY	
	ng cyphertext (ENC_DATA)	
	g encrypted representation of the EtsiTs103097Data-Signed	
	ining content.signedData	
CC	ontaining hashId	
	indicating valid hash algorithm	
	ontaining signer	
	ontaining self	
	ontaining tbsData (SIGNED_DATA)	
CC	ontaining payload	
	containing EtsiTs102941Data	
	containing content.authorizationRequest	
containing publicKeys.verificationKey (V_KEY)		
	and containing hmacKey (HMAC)	
	and containing sharedAtRequest	
	containing keyTag (KEY_TAG)	
and containing eald (EA_ID)		
and a	indicating HashedId8 of the known EA certificate	
then	ontaining signature (SIGNATURE)	
the IUT is able to de	ecrynt the S. KEY	
using the private		
	ng to the AA_ENC_PUB_KEY	
and the IUT is able to decrypt the cyphertext ENC_DATA		
using the S_KE		
	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		
lacitinea by the		

TP Id	SECPKI_AA_AUTH_RCV_02_BV	
	Check that the AA is able to decrypt the AuthorizationRequestMessage using the	
	encryption private key corresponding to the recipient certificate	
Summary	Check that the AA is able to verify the request authenticity using the hmacKey verification	
	Check that the AA sends the AuthorizationValidationRequest message to the	
	correspondent EA	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_AA	
PICS Selection	NOT PICS_PKI_AUTH_POP	
	Expected behaviour	
with		
the AA in 'operational' s	tate	
authorized with the	pertificate CERT_AA	
containing encry	ptionKey (AA_ENC_PUB_KEY)	
ensure that		
when		
the IUT receives the	EtsiTs103097Data-Encrypted message	
containing conte	nt.encryptedData	
containing re		
containing	g the instance of RecipientInfo	
contai	ning certRecipInfo	
containing recipientId		
	indicating HashedId8 of the certificate CERT_AA	
and containing encKey		
indicating symmetric key (S_KEY)		
encrypted with the private key correspondent to the AA_ENC_PUB_KEY		
	ng cyphertext (ENC_DATA)	
containing EtsiTs102941Data		
containing content.authorizationRequest		
containing hmacKey (HMAC)		
an	and containing sharedAtRequest	
containing keyTag (KEY_TAG)		
and containing eald (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' st	rate	
authorized with the c	certificate CERT_AA	
containing encryp	otionKey (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	ad the Authoritation Validation Democratika	
the IUT does not sen	the IUT does not send the AuthorizationValidationRequestMessage	

TP ld	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' s	tate
authorized with the o	certificate CERT_AA
containing encry	ptionKey (AA_ENC_PUB_KEY)
ensure that	
when	
the IUT receives the	EtsiTs103097Data message
containing content.encryptedData	
containing re-	cipients
containing	g the instance of RecipientInfo
	ning certRecipInfo
со	ntaining recipientId
	indicating value
	equal to the HashedId8 of the certificate CERT_AA
an	d containing encKey
	indicating symmetric key (S_KEY)
	encrypted with the OTHER private key than the correspondent to the
AA_ENC_PUB_KEY	
then	
the IUT does not ser	nd the AuthorizationValidationRequestMessage

TP ld	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' st	ate	
authorized with the o	certificate CERT_AA	
containing encrys	otionKey (AA ENC PUB KEY)	
ensure that		
when		
the IUT receives the	the IUT receives the EtsiTs103097Data message	
containing conter	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	
	Check that the AA rejects the authorization request if it is unable to verify the POP	
Summary	signature	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_AA	
PICS Selection	PICS_PKI_AUTH_POP	
	Expected behaviour	
with		
the AA in 'operational' st		
authorized with the o		
3 31	otionKey (AA_ENC_PUB_KEY)	
ensure that		
when		
	EtsiTs103097Data message	
	nt.encryptedData.cyphertext	
· ·	crypted 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 ILIT does not send the AuthorizationValidationRequestMessage		
and the IUT does not send the AuthorizationValidationRequestMessage and the IUT sends to the TS the AuthorizationResponseMessage		
containing authorizationResponse		
containing authorizationicesponse containing requestHash		
indicating the leftmost 16 bits of the SHA256 value		
	calculated over the SIGNED_DATA	
	g responseCode	
	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

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 ld	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

ther

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'

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 eald

indicating an unknown value

then

and the IUT does not send the AuthorizationValidationRequestMessage

and the IUT sends to the TS the AuthorizationResponseMessage

 $containing\ authorization Response$

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 $\operatorname{AuthorizationResponseMessage}$

containing authorizationResponse

containing responseCode

indicating the value 'its-aa-outofsyncrequest'

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 requested Subjec Attributes

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'

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

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

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'

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' st	ate	
authorized with the c	ertificate CERT_AA	
	otionKey (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		
and not conta	ining certificate	

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			
Reference ETSI TS 102 941 [1], clause 6.2.3.3.1, 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) Insure 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 AuthorizationNelidationRequestMessage and the IUT sends to the TS the AuthorizationResponseMessage containing responseCode indicating the value 'deniedpermissions'	TP ld	SECPKI_AA_AUTH_RCV_16_BI	
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	Summary		
Configuration CFG_AUTH_AA PICS_PECTION PICS_PKI_AUTH_POP			
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 validityPeriod 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'	Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1, C-ITS CP [7], clause 7.2.1	
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'	Configuration	CFG_AUTH_AA	
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'	PICS Selection	PICS_PKI_AUTH_POP	
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'		Expected behaviour	
authorized with the certificate CERT_AA	with		
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'	the AA in 'operational' st	tate	
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'	authorized with the o	pertificate CERT_AA	
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'	containing encry	ptionKey (AA_ENC_PUB_KEY)	
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'	ensure that		
containing SharedAtRequest	when		
containing requestedSubjecAttributes	the IUT receives the	AuthorizationRequestMessage	
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'	,		
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'	containing re-		
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'	containing	y ValidityPeriod	
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'	contai	ning start date	
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'	inc	dicating the current date	
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 the IUT does not send the AuthorizationValidationRequestMessage and the IUT sends to the TS the AuthorizationResponseMessage containing authorizationResponse containing responseCode indicating the value 'deniedpermissions'	indicating value grater then PIXIT_AT_PRELOADING_PERIOD		
and the IUT sends to the TS the AuthorizationResponseMessage containing authorizationResponse containing responseCode indicating the value 'deniedpermissions'	then		
containing authorizationResponse containing responseCode indicating the value 'deniedpermissions'	and the IUT does no	ot send the AuthorizationValidationRequestMessage	
containing responseCode indicating the value 'deniedpermissions'	and the IUT sends to	the TS the AuthorizationResponseMessage	
indicating the value 'deniedpermissions'	containing authorizationResponse		
·			
and not containing certificate	indicating	the value 'deniedpermissions'	
	and not conta	aining certificate	
NOTE: PIXIT_AT_PRELOADING_PERIOD shall be set as a TP parameter.	NOTE: PIXIT_AT_PREL	OADING_PERIOD shall be set as a TP parameter.	

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

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	l' state
and the AA already rece	eived the AuthorizationRequestMessage (<i>REQ</i>)
containing generation	onTime <i>TG</i>
and having checksu	
ensure that	
when	
the IUT receives an	AuthorizationRequestMessage
at the moment 7	TR2
indicating TF	R2 > TG + PIXIT_AA_AUTH_TIMEOUT
and having chec	ksum
indicating val	lue equal to CS
then	
	h an AuthorizationResponseMessage
containing respo	
indicating de	niedrequest
NOTE: PIXIT_AA_AUTI	H_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' st	tate	
authorized with CERT_EA certificate		
ensure that		
when		
the IUT received the	the IUT received the AuthorizationRequestMessage	
containing EtsiTs	s102941Data	
containing content.authorizationRequest		
containing sharedAtRequest		
containing eald (EA_ID)		
indicating HashedId8 of the CERT_EA		
then	_	
and the IUT sends the EtsiTs103097Data message		
to the EA identified by EA_ID		

TD IA	SECDICI AA ALITHIYAL OO DV		
TP ld	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' st	ate		
authorized with CER	T_EA certificate		
ensure that			
when	when		
the IUT is triggered to send the authorization validation request to the EA			
then			
the IUT sends a Etsi	Ts103097Data-Encrypted		
containing conter	nt.encryptedData.recipients		
	indicating size 1		
	and containing the instance of RecipientInfo		
	g 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' st	rate		
authorized with CER	T_AA certificate		
and the EA in 'operation	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			

	IOSOPKI AA AUTUWAL OA DV	
TP ld	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' st	ate	
authorized with CER	T_AA certificate	
containing verific	ationKey (AA_PUB_V_KEY)	
and the EA in 'operation	al' state	
authorized with CERT_EA certificate		
ensure that		
when		
the IUT is triggered t	o send the authorization validation request to the EA	
then	'	
the IUT sends a Etsi	Ts103097Data-Encrypted message	
containing EtsiTs	103097Data-Signed	
containing sig	-	
containing		
_	ing supported hash algorithm (HASH_ALG)	
and containing signature		
	ated using the HASH_ALG and private key correspondent to the AA_PUB_V_KEY	

TP Id	SECPKI_AA_AUTHVAL_05_BV
Summary	Check that the AA sends signed 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' st	
authorized with CER	-
	ationKey (AA_PUB_V_KEY)
and the EA in 'operation	
authorized with CER	T_EA certificate
ensure that	
when	and the south significant and the first section of the first section of the secti
the IUT is triggered then	o send the authorization validation request to the EA
	To 102007 Data Engripted massage
	Ts103097Data-Encrypted message
containing EtsiTs103097Data-Signed containing signedData	
containing signed bata	
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' s	tate	
ensure that		
when		
the IUT is triggered	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	
	Check that the AA sends the AuthorizationValidationRequestMessage with	
Summary	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' st		
and the EA in 'operation	al' state	
ensure that		
when		
the IUT received the AuthorizationRequestMessage		
	containing EtsiTs102941Data	
	ntent.authorizationRequest	
containing sharedAtRequest (SHARED_AT_REQUEST)		
and containing ecSignature (EC_SIGNATURE)		
then	To 102007 Data Engripted massage	
the IUT sends a EtsiTs103097Data-Encrypted message		
containing EtsiTs102941Data containing content.authorizationValidationRequest		
containing sharedAtRequest		
indicating SHARED_AT_REQUEST		
and containing ecSignature		
indicating EC_SIGNATURE		
indicat	ing Lo_olorwit of L	

PId 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' st		
and the EA in 'operation	al' state	
ensure that		
when		
	o send the authorization validation request to the EA	
then	T 400007D (0' IA IF) (I)	
	siTs103097Data-SignedAndEncrypted structure	
containing signe		
declared as a	he HashedId8 of the AA certificate	
	ng appPermissions	
	aining an item of type PsidSsp	
containing arritem or type i siddsp		
indicating AID_CERT_REQ		
and containing ssp		
containing opaque[0] (version)		
indicating 1		
	containing opaque[1] (value)	
	indicating 'Enrollment Request' (bit 1) set to 1	

5.5.3 Authorization validation response handling

TP ld	SECPKI_AA_AUTHVAL_RCV_01_BV	
Summary	Check that the AA sends the authorization response after receiving the	
Julilliai y	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' st	ate	
the EA in 'operational' s	tate	
and the IUT(AA) in 'ope	rational' state	
and the IUT had receive	and the IUT had received the AuthorizationRequestMessage from the ITS-S	
and the IUT sent the Au	and the IUT sent the AuthorizationValidationRequestMessage	
ensure that		
when		
the IUT received the AuthorizationValidationResponseMessage		
then		
the IUT sends the E	tsiTs103097Data message to the ITS-S	

PId SECPKI_AA_AUTHVAL_RCV_02_BI		
	Check that AA does not accept the authorization validation response when the	
Summary	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' sta		
the EA in 'operational' st		
and the IUT(AA) in 'oper		
	d the AuthorizationRequest from the ITS-S	
	thorizationValidationRequest	
ensure that		
when	Add to the Military D. M.	
the IUT receives the AuthorizationValidationResponseMessage		
	containing signer	
	containing digest	
	indicating HashedId8 of the certificate	
_	appPermissions	
	aining an item of type PsidSsp	
	aining psid	
	dicating AID_CERT_REQ	
	ntaining an item of type PsidSsp	
	containing psid	
an	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	indicating Admonization validation response (bit 4) set to 0	
	n an AuthorizationValidationResponseMessage	
containing respons	·	
indicating non-z		
maioding non z	0.0 10.00	

5.5.4 Authorization response

TP ld	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 ld	SECPKI_AA_AUTH_03_BV	
Summary	Check that the AA sends signed authorization response with signature properly calculated	
Summary	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' sta	ate	
and the IUT(AA) in 'oper		
authorized with CER	T_AA certificate	
containing verific	ationKey (AA_PUB_V_KEY)	
and the EA in 'operational' state		
ensure that		
when		
the IUT is triggered t	the IUT is triggered to send the authorization response to the ITS-S	
then	1	
and the IUT sends the EtsiTs103097Data-Encrypted message		
containing the EtsiTs103097Data-Signed		
containing signedData		
containing hashld		
indicating supported hash algorithm (HASH_ALG)		
and containing signature		
	ated using the HASH_ALG and private key correspondent to the AA_PUB_V_KEY	

PId 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' sta	ate	
and the IUT(AA) in 'oper	rational' state	
and the EA in 'operation	al' state	
ensure that		
when		
the IUT is triggered t	o 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		

Summary using approved hash algorithm Reference ETSI TS 102 941 [1], clause 6.2.3.3.2 Configuration CFG_AUTH_AA	TP Id	SECPKI_AA_AUTH_05_BV
Reference ETSI TS 102 941 [1], clause 6.2.3.3.2 Configuration CFG_AUTH_AA	Summary	Check that the AA sends signed AuthorizationResponse with signature properly calculated
Configuration CFG_AUTH_AA		using approved hash algorithm
	Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
PICS Selection X PICS	Configuration	CFG_AUTH_AA
N_1 100	PICS Selection	X_PICS

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

P 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 ld	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	l' state	
and the ITS-S has se	ent the AuthorizationRequestMessage	
and the IUT(AA) in 'o	and the IUT(AA) in 'operational' state	
and the EA in 'operat	and the EA in 'operational' state	
ensure that		
when		
the IUT is sending	g to the ITS-S the AuthorizationResponseMessage (MSG)	
containing responseCode		
indicating negative value		
then	•	
the message MSG		
not containing certificate		

PId SECPKI_AA_AUTH_08_BV		
Check that signing of authorization response is permitted by the AA certificate		
Reference		
Configuration	CFG_ENR_EA	
PICS Selection		
	Expected behaviour	
ensure that		
when		
	AuthorizationRequestMessage	
and the IUT is trigger	and the IUT is triggered to send an authorization response	
then		
the IUT sends an EtsiTs103097Data-SignedAndEncrypted structure		
0 0	containing signer	
declared as a di		
	e 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 certific	cate (AT_CERT)	
then		
	horizationResponseMessage	
	rizationResponse	
_	rtificate (AT_CERT)	
	containing appPermissions	
NOT containing an item of type PsidSsp		
containing psid		
07.000	indicating AID_CERT_REQ	
	taining an item of type PsidSsp ntaining psid	
Col	• ·	
indicating AID_CERT_REQ		
and	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		
COI	containing psid	
indicating AID_CRL		

5.5.5 CA Certificate Request

TP Id	SECPKI_AA_CERTGEN_01_BV		
0	SubCA certificate requests of the AA are transported to the RCA using		
Summary	CACertificateRequestMessage structures across the reference point \$9		
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 ld	SECPKI_AA_CERTGEN_02_BV	
S	The application form should include the digital fingerprint of the	
	CACertificateRequestMessage in printable format. The digital fingerprint of the	
Summary	CACertificateRequestMessage is computed using a ETSI TS 103 097 [2] approved hash	
	algorithm	
Reference	ETSI TS 102 941 [1], clause 6.2.1	
Reference	ETSI TS 103 097 [2], clause 7	
Configuration	CFG_CAGEN_INIT	
PICS Selection		
Expected behaviour		
with		
the IUT being in the 'init	iial' 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 hashld shall indicate the hash algorithm to be used as specified in ETSI		
	ETSI TS 103 097 [2], the signer is set to 'self' and the signature over the tbsData is		
Summary	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		
Reference	ETSI TS 103 097 [2], clause 7		
Configuration	CFG_CAGEN_INIT		
PICS Selection			
	Expected behaviour		
with			
the IUT being in the 'initi	al' state		
ensure that	ensure that		
when			
	the IUT is requested to send a CA certificate request		
then			
	CertificateRequestMessage		
	03097Data-Signed structure		
containing hashId			
	indicating the hash algorithm to be used		
and containing			
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		
	An ECC private key is randomly generated, the corresponding public key (verificationKey) is provided to be included in the CaCertificateRequestMessage.		
Summary	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	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 ld	SECPKI_AA_CERTGEN_05_BV	
Summary	The EtsiTs102941Data structure is built with version set to v1 (integer value set to 1).	
Reference	ETSI TS 102 941 [1], clause 6.2.1	
Configuration	CFG_CAGEN_INIT	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the 'initi	ial' state	
ensure that		
when	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 ld	SECPKI_AA_CERTGEN_06_BV
Summary	CaCertificateRequest.requestedSubjectAttributes shall contain the requested certificates
	attributes as specified in ETSI TS 103 097 [2], clause 7.2.4
Reference	ETSI TS 102 941 [1], clause 6.2.1
Reference	ETSI TS 103 097 [2], clause 7.2.4
Configuration	CFG_CAGEN_INIT
PICS Selection	
	Expected behaviour
with	
the IUT being in th	e 'initial' state
ensure that	
when	
the IUT is requ	ested to send a CA certificate request
then	
the IUT sends a CACertificateRequestMessage	
containing CaCertificateRequest	
containin	g requestedSubjectAttributes
as specified in ETSI TS 103 097 [2], clause 7.2.4.	

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

TP ld	SECPKI_AA_CERTGEN_08_BV
S	If the current private key has reached its end of validity period or is revoked, the SubCA
Summary	shall restart the initial certificate application process
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_REKEY
PICS Selection	
	Expected behaviour
with	
the IUT being in th	e 'operational' state
ensure that	
when	
the IUT certifica	ate 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: hashld, tbsData, signer and signature. The hashld shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [2]. The signer declared as a digest, containing the hashedld8 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
ensure that when the IUT is requested then the sends a CACerti being an EtsiTs103 containing hashl indicating the and containing ti and containing si declared as of indicating the and containing si computed ove	d using the CA_CERT certificate to perform a CA certificate rekeying procedure ficateRekeyingMessage 3097Data-Signed structure Id hash algorithm to be used bsData signer digest he hashedId8 of the SubCA certificate (CA_CERT) signature

TP ld	SECPKI_AA_CERTGEN_10_BV
0	The (outer) tbsData of the CACertificateRekeyingMessage shall contain the
Summary	CaCertificateRequestMessage as payload
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_REKEY
PICS Selection	
Expected behaviour	·
with	
the IUT being in th	e 'operational' state
ensure that	·
when	
the IUT is requ	ested to perform a CA certificate rekeying procedure
then	
the sends a CA	ACertificateRekeyingMessage
containing tbsData	
•	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 [i.2] and the generationTime shall be present. All other components of the component tbsdata.headerInfo are not used and absent
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_REKEY
PICS Selection	
	Expected behaviour
then the sends a CACertii containing tbsData containing heade containing ps indicating S and containin	to perform a CA certificate rekeying procedure ficateRekeyingMessage

TP ld	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 'ope	erational' state		
ensure that			
when			
•	to perform a CA certificate rekeying procedure		
then			
	the sends a CACertificateRekeyingMessage		
being an EtsiTs103097Data-Signed structure			
and containing tbsData			
and containing			
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 ssp containing opaque[0] (version)		
C			
indicating opaque[0] (version) indicating 1 containing opaque[1] (value) indicating 'CA Certificate Response' (bit 6) set to 1			

5.6 RootCA behaviour

5.6.0 Overview

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

```
PICS_SECPKI_IUT_RCA = TRUE
```

5.6.1 CTL generation

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

TP 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 trigger	the RootCA is triggered to add new EA certificate (CERT_EA) in the CTL		
then			
the IUT issue a new containing isFull(the IUT issue a new CTL of type CtlFormat containing isFullCtl		
indicating TRUE			
and containing ctlCommands			
containing CtlCommand			
containing add			
containing ea			
containing eaCertificate indicating CERT_EA			

TP Id	SECPKI_RCA_CTLGEN_02_BV	
Summary	Check that the RootCA generates the Delta CTL when new EA is about to be added to the Root CTL	
Reference	ETSI TS 102 941 [1], clauses 6.3.2 and 6.3.4	
Configuration	CFG_CTLGEN_RCA	
PICS Selection		
Expected behaviour		
ensure that		
when		
the RootCA is triggered to add new EA certificate (CERT_EA) in the CTL		
then		
the IUT issue a new	CTL of type CtlFormat	
containing isFullC	Ctl	
indicating FALSE		
and containing ctlCommands		
containing CtlCommand		
containing add		
containing ea		
COI	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	then		
the IUT issue a new CTL of type CtlFormat			
	containing isFullCtl		
indicating TRUE			
and containing ct	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 issue a new	CTL of type CtlFormat	
containing isFullCtl		
indicating FALSE		
and containing ctlCommands		
not containing CtlCommand		
containing delete		
containing cert		
ind	dicating Hashedid8 of CERT_EA	

TP Id	SECPKI_RCA_CTLGEN_05_BV		
I F IU			
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 trigge	ered to add new EA access point URL (URL) to the CTL		
then			
the IUT issue a new	CTL of type CtlFormat		
containing isFull	containing isFullCtl		
indicating TRUE			
containing ctlCommands			
containing C	containing CtlCommand		
containin	g add		
conta	containing ea		
co	containing eaCertificate (CERT_EA)		
and containing itsAccessPoint			
indicating URL			
and NOT containing any other CtlCommand			
containin	containing add		
conta	containing ea		
co	ontaining 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 issue a	a new CTL of type CtlFormat	
containing	isFullCtl	
indicati	indicating FALSE	
containing	containing ctlCommands	
containing CtlCommand		
containing add		
containing ea		
	containing eaCertificate (CERT_EA)	
and containing itsAccessPoint		
	indicating ŪRL	

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 trigg	the RootCA is triggered to add new URL for EA-AA communication (URL) to the CTL		
then			
the IUT issue a nev	the IUT issue a new CTL of type CtlFormat		
	containing isFullCtl		
indicating TRUE			
containing ctlCommands			
containing CtlCommand			
containing add			
containing ea			
containing eaCertificate (CERT_EA)			
containing aaAccessPoint			
indicating URL			
and NOT containing any other CtlCommand			
containing add			
	aining ea		
C	containing eaCertificate		
	indicating CERT_EA		

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

TP ld	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 issue a new	the IUT issue a new CTL of type CtlFormat		
containing isFullCtl			
indicating FALSE			
and containing ctlCommands			
containing CtlCommand			
containing add			
contai	containing aa		
containing aaCertificate			
indicating CERT_AA			

TP ld	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 trigge	ered to delete AA certificate (CERT_AA) from the CTL	
then		
the IUT issue a new	CTL of type CtlFormat	
containing isFull	Ctl	
indicating TR		
and containing c	tlCommands	
not containin	g CtlCommand	
containing add		
	containing aa	
со	ntaining aaCertificate	
	indicating CERT_AA	

TP ld	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 issue 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	
IF IU	Check that the RootCA generates the Full CTL when AA access point URL is about to be	
Summary		
Deference	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 t	triggered to add new URL for AA access point (URL) to the CTL	
then		
the IUT issue a	new CTL of type CtlFormat	
containing i	sFullCtl	
indicating TRUE		
containing of	ctlCommands	
containi	ng CtlCommand	
cont	aining add	
C	containing aa	
	containing aaCertificate	
	containing accessPoint	
	indicating URL	
and NOT containing any other CtlCommand		
containing add		
C	containing aa	
	containing aaCertificate	
	indicating CERT AA	

```
TP Id
                          SECPKI_RCA_CTLGEN_14_BV
                          Check that the RootCA generates the Delta CTL when AA access point URL is about to be
Summary
                          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
      the IUT issue a new CTL of type CtlFormat
         containing isFullCtl
             indicating TRUE
         containing ctlCommands
             containing CtlCommand
                containing add
                   containing aa
                      containing aaCertificate
                      containing accessPoint
                          indicating URL
```

TP Id	SECPKI_RCA_CTLGEN_15_BV	
Summary	Check that the RootCA CTL is signed using RootCA verification key	
	Check that signing of the RootCA CTL is permitted by the RootCA certificate	
Reference	ETSI TS 102 941 [1], clause 6.3.2	
Configuration	CFG_CTLGEN_RCA	
PICS Selection		
	Expected behaviour	
with		
the TLM already issued		
	ertificate (CERT_RCA)	
ensure that		
when		
	red to issue a new CTL	
then		
	CTL of type RcaCertificateTrustListMessage	
containing signed		
containing signer.digest		
indicating HashedID8 of the RootCA certificate (CERT_RCA)		
	ng 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 'PEM entries' (bit 0) set to 0	
	indicating 'FA entries' (bit 2) set to 1	
	indicating 'AA entries' (bit 3) set to 1	
	indicating 'DC entries' (bit 4) set to 1	
NOTE: The EtsiTs10309	7Data and EtsiTs102941Data envelopes are not yet removed from the analysing message.	

TP Id

SECPKI_RCA_CTLGEN_16_BV

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	when		
the RCA is triggere	the RCA is triggered to issue a new CTL		
then			
the IUT issue 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
	Check that the RCA Delta CTL is generated at the same time as FullCTL.
Summary	Check that the RCA Delta CTL is a difference between correspondent Full CTL and the
	previous Full CTL
Reference	ETSI TS 102 941 [1], clause 6.3.2
Configuration	CFG_CTLGEN_RCA
PICS Selection	
	Expected behaviour
with	
the RCA already issued	the previous CTL of type CtlFormat (CTL_FULL_PREV)
containing isFullCtl	
indicating TRUE	
containing ctlSequer	nce
indicating N	
ensure that	
when	
the RCA is triggered	to issue a new CTL
then	
	CTL of type CtlFormat (CTL_FULL)
containing isFull	
indicating TR	
and containing cf	
indicating N+	
	new CTL of type CtlFormat (CTL_DELTA)
containing isFull(
indicating FA and containing ct	
indicating N+	
containing ctlCor	
_	
indicating diff	erence 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	ensure that		
when			
the IUT is triggered to issue a new CTL			
then			
the IUT issue a new CTL of type CtlFormat			
containing version			
indicating 1			

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

TP ld	SECPKI_RCA_CTLGEN_23_BV		
Summary	Check that the RCA CTL contains at least one DC entry		
Reference	ETSI TS 102 941 [1], clause 6.3.2		
Configuration	CFG_CTLGEN_RCA		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the IUT is triggered t	o issue a new CTL		
then			
the IUT issue a new	the IUT issue a new CTL of type CtlFormat		
containing isFull(containing isFullCtl		
	indicating TRUE		
and containing ctlCommands			
containing at least one ctlCommand			
containing	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 ld	SECPKI_RCA_CRLGEN_01_BV		
Summary	Check that the RootCA generates the CRL signed with appropriate certificate		
Reference	ETSI TS 102 941 [1], clause 6.3.3		
Configuration	CFG_CRLGEN_RCA		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the RootCA is trigger	red to generate new CRL		
then			
the IUT generates the CertificateRevocationListMessage			
containing signer	containing signer		
containing diges	st st		
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		

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

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

TP ld	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	containing the RCA certificate CERT_RCA		
ensure that	ensure that		
when			
the RootCA is triggered to revoke itself			
then	then		
the IUT issue a new CRL of type ToBeSignedCrl			
containing entries			
containing item of type CrlEntry			
indicating	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	when		
the RootCA is triggered to issue a new CRL at the time T1			
then			
the IUT issue a new CRL of type ToBeSignedCrl			
containing thisUpdate			
indicating ti	indicating timestamp greater or equal to the T1		

TP ld	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 nextUpda			
indicating time Tr	indicating time Tprev		
ensure that			
when	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 ld	SECPKI_RCA_CRLGEN_07_BV	
Summary	Check that the RootCA generates the CRL when CA certificate is about to be revoked	
Reference	ETSI TS 102 941 [1], clause 6.3.3	
Configuration	CFG_CRLGEN_RCA	
PICS Selection		
	Expected behaviour	
ensure that		
when		
the RootCA is trig	gered 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	when	
the RCA is triggered to issue a new CRL		
then		
the IUT issues a new CRL of type ToBeSignedCrl		
containing version		
indicating	indicating 1	

5.6.3 CA certificate generation

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

```
Expected behaviour
ensure that
   when
      the IUT is requested to generate EA certificate
   then
       the IUT generate the certificate
          containing appPermissions
              containing an item of type PsidSsp
                 containing psid
                    indicating AID_CERT_REQ
                 and containing ssp
                    containing opaque[0] (version)
                        indicating 1
                    containing opaque[1] (value)
                        indicating 'Authorization validation Response' (bit 4) set to 1
                        and indicating 'Enrollment 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
                           Check that generated AA certificate contains only allowed permissions
Summary
                           ETSI TS 102 941 [1], clause B.5
Reference
Configuration
                           CFG_CAGEN_RCA
PICS Selection
                                               Expected behaviour
ensure that
   when
      the IUT is requested to generate AA certificate
      the IUT generate the certificate
          containing appPermissions
             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

and NOT containing an item of type PsidSsp

containing psid

containing psid

indicating AID_CTL

indicating AID CRL

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

5.7 DC behaviour

TP Id	SECPKI_DC_LISTDIST_01_BV	
Summary	Check that the RCA CRL is published and accessible when issued	
Reference	ETSI TS 102 941 [1], clause 6.3.3	
Configuration	CFG_DC	
PICS Selection		
Expected behaviour		
with		
the TLM issued a new C	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 ld	SECPKI_DC_LISTDIST_02_BV		
Summary	Check that the RCA CTL is published and accessible when issued		
Reference	ETSI TS 102 941 [1], clauses 6.3.2 and 6.3.3		
Configuration	CFG_DC		
PICS Selection			
	Expected behaviour		
with			
the TLM issued a new 0	the TLM issued a new CTL		
ensure that			
when	when		
the ITS-S asks the IUT for the newly issued CTL			
then			
the IUT is answered	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		
cor	containing selfsignedRootCa	
	indicating CERT_RCA	

TP ld	SECPKI_TLM_ECTLGEN_02_BV		
Summary	Check that the TLM generates the Delta ECTL when new RootCA is about to be added		
Reference	ETSI TS 102 941 [1], clause 6.3.1		
Configuration	CFG_CTLGEN_TLM		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the TLM is triggered to add new RootCA certificate (CERT_RCA) in the CTL			
then	then		
the IUT issues a new CTL of type CtlFormat			
containing isFullC	containing isFullCtl		
indicating FALSE			
and containing ctlCommands			
containing CtlCommand			
containing add			
containing rca			
COI	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	the TLM is triggered to delete RootCA certificate (CERT_RCA) from the CTL		
then	· · · · · · · · · · · · · · · · · · ·		
the IUT issues a new	the IUT issues a new CTL of type CtlFormat		
containing isFull0	containing isFullCtl		
indicating TRUE			
and containing ct	and containing ctlCommands		
not containing CtlCommand			
containing add			
containing rca			
COI	containing selfsignedRootCa		
indicating CERT_RCA			

TP Id	SECPKI_TLM_ECTLGEN_04_BV	
Summary	Check that the TLM generates the Delta ECTL when RootCA is about to be deleted	
Reference	ETSI TS 102 941 [1], clause 6.3.1	
Configuration	CFG_CTLGEN_TLM	
PICS Selection		
	Expected behaviour	
ensure that	•	
when		
the TLM is triggered	to delete RootCA certificate (CERT_RCA) from the CTL	
then		
the IUT issues a nev	w CTL of type CtlFormat	
containing isFull	Ctl	
indicating FA	LSE	
and containing c	tlCommands	
containing Ct		
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	then		
the IUT issues a new CTL of type CtlFormat			
containing isFullC	containing isFullCtl		
indicating TRUE			
and containing ctlCommands			
not containing CtlCommand			
containing add			
	containing tlm		
COI	ntaining 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	the TLM is triggered to add new the TLM certificate (CERT_TLM) in the CTL		
then	· · · · · · · · · · · · · · · · · · ·		
the IUT issues a new	the IUT issues a new CTL of type CtlFormat		
containing isFullC	containing isFullCtl		
indicating FAI	LSE		
and containing ct	and containing ctlCommands		
not containing CtlCommand			
containing add			
containing tlm			
COI	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 nev	the IUT issues a new CTL of type CtlFormat		
containing isFull(containing isFullCtl		
indicating TR	indicating TRUE		
and containing ct	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	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 ct	and containing ctlCommands		
not containing CtlCommand			
containing add			
containing tlm			
CO	containing accessPoint		
indicating URL			

TP Id	SECPKI_TLM_ECTLGEN_09_BV		
TF IG	Check that the TLM CTL is signed using TLM verification key		
Summary	Check that signing of TLM CTL is allowed by the TLM certificate		
Reference	ETSI TS 102 941 [1], clause 6.3.1		
Configuration	CFG_CTLGEN_TLM		
PICS Selection			
	Expected behaviour		
ensure that			
when	4 · OTI		
the TLM is triggered	to issue a new CTL		
then	v CTL of type TimCortificateTrustLigtMoseage		
	v CTL of type TImCertificateTrustListMessage		
containing signed containing signed			
	indicating HashedID8 of the TLM certificate (TLM_CERT) containing appPermissions		
	containing apprermissions containing an item of type PsidSsp		
	containing an item of type PsidSsp containing psid		
	indicating AID_CTL		
a	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		
NOTE TI SUIT (200	indicating TLM_CERT		
NOTE: The EtsiTs10309	77Data and EtsiTs102941Data envelopes are not yet removed from the analysing message.		

TP ld	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 is	sued 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	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 ld	SECPKI_TLM_ECTLGEN_13_BV	
Summary		
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		

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