ETSI TS 103 525-2 V1.1.1 (2019-03)



Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 2: Test Suite Structure and Test Purposes (TSS & TP) Reference DTS/ITS-00546

Keywords

ITS, security, testing, TSS&TP

ETSI

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

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

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

Important notice

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

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the 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 <u>https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx</u>

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

Copyright Notification

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

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

© ETSI 2019. All rights reserved.

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

GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

Intelle	ntellectual Property Rights		
Forew	vord	5	
Moda	l verbs terminology	5	
1	Scope	6	
2	References	6	
2.1	Normative references	6	
2.2	Informative references	6	
3	Definition of terms, symbols and abbreviations	7	
3.1	Terms		
3.2	Symbols		
3.3	Abbreviations		
4	Test Suite Structure (TSS)	0	
4 4.1			
4.1	Structure for Security tests		
4.2.1	ITS-S states		
4.2.2	EA states		
4.2.3	AA states		
4.2.4	RootCA states		
4.2.5	TLM states		
4.3	Test configurations	.10	
4.3.1	Overview		
4.3.2	Enrolment		
4.3.2.1	b = -		
4.3.2.2	\mathcal{O} = =		
4.3.3 4.3.3.1	Authorization		
4.3.3.2	ε $ -$		
4.3.4	Authorization Validation		
4.3.4.1	Configuration CFG_AVALID_AA		
4.3.4.2			
4.3.5	CA certificate generation		
4.3.5.1	Configuration CFG_CAGEN_INIT		
4.3.5.2	Configuration CFG_CAGEN_REKEY	.11	
4.3.5.3	∂		
4.3.6	ECTL generation		
4.3.6.1	0 – –		
4.3.6.2	\mathcal{O} = =		
4.3.7 4.3.7.1	Root CTL generation Configuration CFG_CTLGEN_RCA		
4.3.7.1	Configuration CFG_CTLOEN_RCA		
4.3.8.1		12	
5	Test Purposes (TP)		
5.1	Introduction		
5.1.1	TP definition conventions		
5.1.2 5.1.3	TP Identifier naming conventions		
5.1.3 5.1.4	Rules for the behaviour description Sources of TP definitions		
5.1.4	Mnemonics for PICS reference		
5.2	ITS-S behaviour		
5.2.0	Overview		
5.2.1	Manufacturing		
5.2.2	Enrolment		
5.2.2.0	Overview	.14	
5.2.2.1	Enrolment request	.14	

5.2.2.2	Enrolment response handling	
5.2.3	Authorization	
5.2.3.0	Overview	
5.2.3.1	Authorization request	
5.2.3.2	Authorization response handling	
5.2.4	CTL handling	
5.2.5	CRL handling	
5.3	EA behaviour	
5.3.1	Enrolment request handling	
5.3.2	Enrolment response	
5.3.3	Authorization validation request handling	
5.3.4	Authorization validation response	
5.3.5	CA Certificate Request	41
5.4	AA behaviour	
5.4.1	Authorization request handling	
5.4.2	Authorization validation request	
5.4.3	Authorization validation response handling	
5.4.4	Authorization response	55
5.4.5	CA Certificate Request	
5.5	RootCA behaviour	64
5.5.1	CTL generation	64
5.5.2	CRL generation	74
5.5.3	CA certificate generation	
5.6	DC behaviour	
5.7	TLM behavior	
5.7.1	CTL generation	
5.8	CPOC behavior	
History		

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

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

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

Modal verbs terminology

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

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

1 Scope

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

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

2 References

2.1 Normative references

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

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

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

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

- [1] ETSI TS 102 941 (V1.3.1): "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management".
- [2] ETSI TS 103 097 (V1.3.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".
- [3] IEEE Std 1609.2TM-2016: "IEEE Standard for Wireless Access in Vehicular Environments -Security Services for Applications and Management Messages", as amended by IEEE Std 1609.2aTM-2017: "Standard for Wireless Access In Vehicular Environments - Security Services for Applications and Management Messages Amendment 1".
- [4] ETSI TS 103 525-1 (V1.1.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 1: Protocol Implementation Conformance Statement (PICS)".

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".
r: 7 1	

[i.7] ETSI ETS 300 406 (1995): "Methods for testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

AID_CERT_REQ"Secured certificate request service" ITS-AIDAID_CTL"CTL service" ITS-AIDAID_CRL"CRL service" ITS-AID

3.2 Symbols

Void.

3.3 Abbreviations

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

Authorization Authority
Application IDentifier
ITS Application IDentifier for CAM
Application Identifier for DENM
Application Identifier for general GeoNetworking messages
Authorization Ticket
Abstract Test Suite
exceptional BehaviOur
Valid Behaviour
Co-operative Awareness Messages
CERTificate
Decentralized Environmental Notification Message
Enrolment Authority
Elliptic Curve Cryptography
GeoNetworking
Intelligent Transportation Systems
Intelligent Transport System - Station
Implementation Under Test
MesSaGe
Protocol Implementation Conformance Statement
Service Specific Permissions
Test Purposes
Test System
Test Suite Structure

4 Test Suite Structure (TSS)

4.1 Structure for Security tests

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

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

Table 1: TSS for Security Management

4.2 Test entities and states

4.2.1 ITS-S states

- State 'initialized':
 - ITS-S in 'initialized' state is ready to perform the enrolment request.
 - ITS-S in 'initialized' state contains following information elements:
 - permanent canonical identifier (PCI);
 - public/private key pair for cryptographic purposes (canonical key pair);
 - the trust anchor (Root CA) public key certificate and the DC network address;
 - contact information for the EA which will issue certificates for the ITS-S:
 - network address;
 - public key certificate.
- State 'enrolled':
 - ITS-S in 'enrolled' state has successfully performed the enrolment request process.
 - ITS-S in 'enrolled' state is ready to perform an authorization request.
 - ITS-S in 'enrolled' state contains all information elements of the 'initialized' state and additionally:
 - enrolment credential (EC) with the condition of being neither expired nor revoked;

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

4.2.2 EA states

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

4.2.3 AA states

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

4.2.4 RootCA states

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

4.2.5 TLM states

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

4.3 Test configurations

- 4.3.1 Overview
- 4.3.2 Enrolment

4.3.2.1 Configuration CFG_ENR_ITSS

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

• Following information elements shall be provided by IUT for the EA emulated by the TS.

10

- permanent canonical identifier (PCI);
- public key of canonical key pair;
- profile information.
- TS: EA is emulated by TS.

4.3.2.2 Configuration CFG_ENR_EA

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

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

TS: ITS-S is emulated by the TS.

4.3.3 Authorization

4.3.3.1 Configuration CFG_AUTH_ITSS

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

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

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

4.3.3.2 Configuration CFG_AUTH_AA

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

- The profile information for the emulated ITS-S.
- TS: ITS-S is emulated by the TS:
 - EA is emulated by the TS and validates all incoming requests.

4.3.4 Authorization Validation

4.3.4.1 Configuration CFG_AVALID_AA

- IUT: AA in the operational state and containing following information:
 - the certificate of the emulated EA;
 - the URL of the emulated EA.
- TS: EA is emulated by the TS and ready to receive authorization validation requests:
 - ITS-S is emulated by TS to trigger the authorization process.

4.3.4.2 Configuration CFG_AVALID_EA

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

- the permanent canonical identifier of the emulated ITS-S;
- the profile information for the emulated ITS-S;
- the public key from the key pair belonging to the emulated ITS-S.
- TS: AA and ITS-S are emulated by the TS and contain following information elements:
 - EC certificate issued by IUT;
 - EA certificate of IUT;
 - the URL of the EA.

4.3.5 CA certificate generation

4.3.5.1 Configuration CFG_CAGEN_INIT

- IUT: CA (EA or AA) in the initial state
- TS: TS checks generated certificate requests and does not emulate any ITS entity

4.3.5.2 Configuration CFG_CAGEN_REKEY

- IUT: CA (EA or AA) in the operational state
- TS: TS checks generated certificate requests and does not emulate any ITS entity

4.3.5.3 Configuration CFG_CAGEN_RCA

- IUT: Offline RootCA in operational state, generating EA, AA or RCA certificate
- TS: TS checks generated certificate and does not emulate any ITS entity

4.3.6 ECTL generation

4.3.6.1 Configuration CFG_CTLGEN_TLM

- IUT: TLM in the operational state
- TS: TS checks generated CTL and does not emulate any ITS entity

4.3.6.2 Configuration CFG_CTLGEN_CPOC

- IUT: CPOC in the operational state
- TS: TS checks generated CTL emulating http client of CPOC

4.3.7 Root CTL generation

4.3.7.1 Configuration CFG_CTLGEN_RCA

- IUT: RCA in the operational state
- TS: TS checks generated CTL and does not emulate any ITS entity

4.3.8 CRL generation

4.3.8.1 Configuration CFG_CRLGEN_RCA

IUT: RCA in the operational state

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

5 Test Purposes (TP)

5.1 Introduction

5.1.1 TP definition conventions

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

5.1.2 TP Identifier naming conventions

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

Table 2: TP naming convention

Identifier	TP_ <root>_<tgt>_<gr>_<sn>_<x></x></sn></gr></tgt></root>]	
	<root> = root</root>	SECPKI	
	<tgt> = target</tgt>	ITSS	ITS-Station
		AA	Authorization Authority
		EA	Enrolment Authority
		RCA	Root Certification Authority
		DC	Distribution Center
		CPOC	C-ITS Point of Contact
	<gr> = group</gr>	ENR	Enrolment
		AUTH	Authorization
		AUTHVAL	Authorization Validation
		CRL	CRL handling
		CTL	CTL handling
		CACERTGEN	CA certificate generation
		CTLGEN	CTL generation
		ECTLGEN	ECTL generation
		CRLGEN	CRL generation
		LISTDIST	CTL/CRL/ECTL distribution
		TLMCERTGEN	TLM certificate generation
	<sgr>=sub-group</sgr>	SND	Sending behaviour
		RCV	Receiving behaviour
	<sn> = test purpose sequential number</sn>		01 to 99

Identifier	TP_ <root>_<tgt>_<gr>_<sn>_<x></x></sn></gr></tgt></root>		
	<x> = category</x>	BV	Valid Behaviour tests
		BO	Invalid Behaviour Tests

5.1.3 Rules for the behaviour description

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

ETSI TS 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 the clause A.6 of ETSI TS 103 525-1 [4] and in the IEEE 1609.2 [3] shall be used to determine the test applicability.

Mnemonic	PICS item
PICS_SECPKI_IUT_ITSS	[4] A.3.1
PICS_SECPKI_IUT_EA	[4] A.4.2
PICS_SECPKI_IUT_AA	[4] A.4.3
PICS_SECPKI_IUT_RCA	[4] A.4.4
PICS_SECPKI_IUT_DC	[4] A.4.5
PICS_SECPKI_IUT_TLM	[4] A.4.6
PICS_SECPKI_IUT_CPOC	[4] A.4.7
PICS_SECPKI_ENROLMENT	[4] A.3.2 or A.5.1
PICS_SECPKI_REENROLMENT	[4] A.3.2.1 or A.5.2
PICS_SECPKI_AUTHORIZATION	[4] A.3.3 or A.6.1
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_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_ECTL	[4] A.9.1 or A.8.1
PICS_SECPKI_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_SEC_SHA256	[3] S1.2.2.1.1 or S1.3.2.1.1
PICS_SEC_SHA384	[3] \$1.2.2.1.2 or \$1.3.2.1.2
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

Table 3: Mnemonics for PICS reference

5.2 ITS-S behaviour

5.2.0 Overview

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

PICS_SECPKI_IUT_ITSS = TRUE

5.2.1 Manufacturing

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

5.2.2 Enrolment

5.2.2.0 Overview

All test purposes in clause 5.2.2.1 may be included in the test sequence if following PICS items are set:

PICS_SECPKI_ENROLMENT = TRUE

5.2.2.1 Enrolment request

TP ld	SECPKI_ITSS_ENR_01_BV		
Summary	Immary Check that IUT sends an enrolment request when triggered		
Reference	ETSI TS 102 941 [1], clause 6.1.3		
Configuration	CFG_ENR_ITSS		
PICS Selection			
	Expected behaviour		
then	ilized' state requested a new Enrolment Certificate (EC) n EnrolmentRequestMessage		

TP ld	SECPKI_ITSS_ENR_02_BV
	If the enrolment request of the IUT is an initial enrolment request, the itsld (contained in
Cummon .	the InnerECRequest) shall be set to the canonical identifier, the signer (contained in the
Summary	outer EtsiTs1030971Data-Signed) shall be set to self and the outer signature shall be
computed using the canonical private key.	
Reference	ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1
Configuration	CFG_ENR_ITSS
PICS Selection	
	Expected behaviour
with	
the IUT being in the	e 'initialized' state
ensure that	
when	
the IUT is reques	sted to send an EnrolmentRequestMessage
then	
the IUT sends an EtsiTs103097Data-Encrypted	
	encrypted EtsiTs103097Data-Signed
	EtsiTs103097Data
	ng InnerECRequestSignedForPOP
	ining InnerEcRequest
	ntaining itsld
	indicating the canonical identifier of the ITS-S
and containing signer	
declared as self and containing signature	
TP ld	SECPKI_ITSS_ENR_03_BV
	In presence of a valid EC, the enrolment request of the IUT is a rekeying enrolment
	request with the itsId (contained in the InnerECRequest) and the SignerIdentifier

Summary	In presence of a valid EC, the enrolment request of the IUT is a rekeying enrolment request with the itsld (contained in the InnerECRequest) and the SignerIdentifier (contained in the outer EtsiTs1030971Data-Signed) both declared as digest containing the HashedId8 of the EC and the outer signature computed using the current valid EC private		
D. (key corresponding to the verification public key.		
Reference	ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1		
Configuration	CFG_ENR_ITSS		
PICS Selection	PICS_SECPKI_REENROLMENT		
	Expected behaviour		
with			
the IUT being in the 'enro	lled' state		
ensure that			
when			
the IUT is requested to	the IUT is requested to send an EnrolmentRequestMessage		
then			
the IUT sends an EtsiT	s103097Data-Encrypted		
containing an encryp	oted EtsiTs103097Data-Signed		
containing EtsiTs	103097Data		
	erECRequestSignedForPOP		
	nnerEcRequest		
	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		
computed using the current valid EC private key corresponding to the verification public key			

TP ld	SECPKI_ITSS_ENR_04_BV		
Summary	Summary If the EC is revoked, the IUT returns to the state 'initialized'.		
Reference	ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1		
Configuration	CFG_ENR_ITSS		
PICS Selection	PICS_SECPKI_CRL		
	Expected behaviour		
ensure that when	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 ld	SECPKI_ITSS_ENR_05_BV	
Summary	If the EC expires, the IUT returns to the state 'initialized'.	
Reference	ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1	
Configuration	CFG_ENR_ITSS	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the 'enro	olled' state	
ensure that		
when		
the EC of the IUT expires		
then		
the IUT returns to the 'initialized' state		

PICS Selection PICS_SECPKI_REENROLMENT Expected behaviour with the IUT being in the 'initialized' state ensure that when the IUT is requested to send multiple EnrolmentRequestMessage then each EnrolmentRequestMessage contains a different and unique verification key pair within the InnerECRequest.	TP ld	SECPKI_ITSS_ENR_06_BV	
Corresponding to an approved signature algorithm as specified in ETSTTS 103 097 [2]. Reference ETSI TS 102 941 [1], clause 6.2.3.2.1 ETSI TS 103 097 [2], clause 7 Configuration CFG_ENR_ITSS PICS Selection PICS_SECPKI_REENROLMENT Expected behaviour with the IUT being in the 'initialized' state ensure that when the IUT is requested to send multiple EnrolmentRequestMessage then each EnrolmentRequestMessage contains a different and unique verification key pair within the InnerECRequest. NOTE: The first EnrolmentRequestMessage should be an initial request, the following EnrolmentRequestMessages	C	For each enrolment request, the ITS-S shall generate a new verification key pair	
Reference ETSI TS 103 097 [2], clause 7 Configuration CFG_ENR_ITSS PICS Selection PICS_SECPKI_REENROLMENT Expected behaviour with the IUT being in the 'initialized' state ensure that when the IUT is requested to send multiple EnrolmentRequestMessage then each EnrolmentRequestMessage contains a different and unique verification key pair within the InnerECRequest. NOTE: The first EnrolmentRequestMessage should be an initial request, the following EnrolmentRequestMessages	Summary	corresponding to an approved signature algorithm as specified in ETSI TS 103 097 [2].	
ETSTTS 103 097 [2], clause 7 Configuration CFG_ENR_ITSS PICS Selection PICS_SECPKI_REENROLMENT Expected behaviour with the IUT being in the 'initialized' state ensure that when the IUT is requested to send multiple EnrolmentRequestMessage then each EnrolmentRequestMessage contains a different and unique verification key pair within the InnerECRequest. NOTE: The first EnrolmentRequestMessage should be an initial request, the following EnrolmentRequestMessages	Poforonco	ETSI TS 102 941 [1], clause 6.2.3.2.1	
PICS Selection PICS_SECPKI_REENROLMENT Expected behaviour with the IUT being in the 'initialized' state ensure that when the IUT is requested to send multiple EnrolmentRequestMessage then each EnrolmentRequestMessage contains a different and unique verification key pair within the InnerECRequest. NOTE: The first EnrolmentRequestMessage should be an initial request, the following EnrolmentRequestMessages	Reference	ETSI TS 103 097 [2], clause 7	
Expected behaviour with the IUT being in the 'initialized' state ensure that when the IUT is requested to send multiple EnrolmentRequestMessage then each EnrolmentRequestMessage contains a different and unique verification key pair within the InnerECRequest. NOTE: The first EnrolmentRequestMessage should be an initial request, the following EnrolmentRequestMessages	Configuration	CFG_ENR_ITSS	
with the IUT being in the 'initialized' state ensure that when the IUT is requested to send multiple EnrolmentRequestMessage then each EnrolmentRequestMessage <u>contains a different and unique verification key pair within the InnerECRequest.</u> NOTE: The first EnrolmentRequestMessage should be an initial request, the following EnrolmentRequestMessages	PICS Selection	PICS_SECPKI_REENROLMENT	
the IUT being in the 'initialized' state ensure that when the IUT is requested to send multiple EnrolmentRequestMessage then each EnrolmentRequestMessage <u>contains a different and unique verification key pair within the InnerECRequest.</u> NOTE: The first EnrolmentRequestMessage should be an initial request, the following EnrolmentRequestMessages		Expected behaviour	
ensure that when the IUT is requested to send multiple EnrolmentRequestMessage then each EnrolmentRequestMessage <u>contains a different and unique verification key pair within the InnerECRequest.</u> NOTE: The first EnrolmentRequestMessage should be an initial request, the following EnrolmentRequestMessages	with		
when the IUT is requested to send multiple EnrolmentRequestMessage then each EnrolmentRequestMessage contains a different and unique verification key pair within the InnerECRequest. NOTE: The first EnrolmentRequestMessage should be an initial request, the following EnrolmentRequestMessages	the IUT being in the	'initialized' state	
the IUT is requested to send multiple EnrolmentRequestMessage then each EnrolmentRequestMessage contains a different and unique verification key pair within the InnerECRequest. NOTE: The first EnrolmentRequestMessage should be an initial request, the following EnrolmentRequestMessages	ensure that		
then each EnrolmentRequestMessage contains a different and unique verification key pair within the InnerECRequest. NOTE: The first EnrolmentRequestMessage should be an initial request, the following EnrolmentRequestMessages	when		
each EnrolmentRequestMessage contains a different and unique verification key pair within the InnerECRequest. NOTE: The first EnrolmentRequestMessage should be an initial request, the following EnrolmentRequestMessages	the IUT is requested to send multiple EnrolmentRequestMessage		
contains a different and unique verification key pair within the InnerECRequest. NOTE: The first EnrolmentRequestMessage should be an initial request, the following EnrolmentRequestMessages	then		
NOTE: The first EnrolmentRequestMessage should be an initial request, the following EnrolmentRequestMessages	each EnrolmentRequestMessage		
	contains a different and unique verification key pair within the InnerECRequest.		
should be rekeying requests.	NOTE: The first Enr	NOTE: The first EnrolmentRequestMessage should be an initial request, the following EnrolmentRequestMessages	
	should be rekeying requests.		

TD ! !	DEODIC ITOD END AT DV	
PId SECPKI_ITSS_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	
Configuration	CFG_ENR_ITSS	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the X_	STATE	
ensure that		
when		
the IUT is requested	to send an EnrolmentRequestMessage	
then		
	siTs103097Data-Encrypted	
	rypted EtsiTs103097Data-Signed	
	Ts103097Data	
	nerECRequestSignedForPOP	
	g InnerEcRequest	
containing requestedSubjectAttributes		
not containing certIssuePermissions		
Variants		
nn X_STATE		
1 'initialized' sta	ate	
2 'enrolled' stat	'enrolled' state	

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

TP ld	SECPKI_ITSS_ENR_09_BV
Summary	In the headerInfo of the tbsData of the outer EtsiTs102941Data-Signed all other components of the component tbsdata.headerInfo except generationTime and psid are not used and absent. The psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [i.2] and the generationTime shall be present.
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.1
Configurat	on CFG_ENR_ITSS
PICS Selec	tion
	Expected behaviour
ensure that when the IU ⁻ then the IU ⁻ cont	 is requested to send an EnrolmentRequestMessage sends an EtsiTs103097Data-Encrypted aining 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	'enrolled' state

TP ld		SECPKI ITSS ENR 10 BV	
Summary	,	The EtsiTs103097Data-Encrypted containing the correctly encrypted ciphertext and a recipients component containing one instance of RecipientInfo of choice certRecipInfo containing the hashedId8 of the EA certificate in recipientId and the encrypted data encryption key in encKey. The data encryption key is encrypted using the public key found in the EA certificate referenced in the recipientId.	
Reference	Э	ETSI TS 102 941 [1], clause 6.2.3.2.1	
Configura	ation	CFG_ENR_ITSS	
PICS Sele	ection		
		Expected behaviour	
with			
	being in the X_S	ГАТЕ	
ensure that	at		
when			
	JI is requested to	send an EnrolmentRequestMessage	
then	IT sounds on EtsiT		
		s103097Data-Encrypted	
	containing recipients containing exactly one instance of RecipientInfo of choice certRecipInfo		
	containing recip		
	indicating the hashedId8 referencing to the EA certificate		
	containing encryptionKey (KEY)		
	and containing		
being a symmetric key (SYMKEY) encrypted using the key KEY			
containing ciphertext			
which is encrypted using the symmetric key SYMKEY contained in encKey			
Variants			
nn	X_STATE		
1	'initialized' state)	
•			

TP ld	SECPKI_ITSS_ENR_11_BV		
	In the inner signed data structure (InnerECRequestSignedForPOP), the signature is		
Summary	computed on InnerECRequest with the private key corresponding to the new		
verificationKey to prove possession of the generated verification key pair. Reference ETSI TS 102 941 [1], clause 6.2.3.2.1			
Configuratio			
PICS Select			
	Expected behaviour		
with			
	ing in the X_STATE		
ensure that			
when	is requested to send on EnrolmentDequestMessage		
the IUI	is requested to send an EnrolmentRequestMessage		
	sends an EtsiTs103097Data-Encrypted		
	ining an encrypted EtsiTs103097Data-Signed		
	intring EtsiTs103097Data		
	containing InnerECRequestSignedForPOP		
	containing thsData		
	containing InnerEcRequest		
	containing verificationKey (VKEY)		
	containing signature		
	computed on InnerECRequest		
	using the private key corresponding to VKEY		
contained in InnerECRequest			
	Variants		
nn)	K_STATE		
1 '	initialized' state		
2 '	enrolled' state		
I			
TP Id	SECPKI ITSS ENR 12 BV		

TP Id SECPKI_ITSS_ENR_12_BV			
Summary	Check that signing of Enrolment Request message is permitted by the EC certificate		
Reference	ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1		
Configuration	CFG_ENR_ITSS		
PICS Selection	PICS_SECPKI_REENROLMENT		
	Expected behaviour		
with			
the IUT being in the 'enro	Iled' state		
ensure that			
when			
	send an EnrolmentRequestMessage		
then			
	s103097Data-Encrypted		
	containing an encrypted EtsiTs103097Data-Signed		
00	containing signer		
containing diges			
3	indicating HashedId8 of the EC certificate containing appPermissions		
	containing an item of type PsidSsp containing psid		
indicating AID_CERT_REQ			
and containing ssp			
containing opaque[0] (version)			
	indicating 1		
	ning opaque[1] (value)		
indicating 'Enrolment Request' (bit 1) set to 1			
L			

TP ld		SECPKI_ITSS_ENR_RCV_01_BV
Summary		If an enrolment request fails, the IUT returns to the state 'initialized.
Reference		ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1
Configura	tion	CFG_ENR_ITSS
PICS Sele	ction	
		Expected behaviour
with		
the IUT I	being in the X_S	TATE
ensure that	t	
when		
		send an EnrolmentRequestMessage
		ponseMessage is received
	taining a respons	eCode different than 0
then		
	T returns to the '	initialized' state
Variants		
nn	X_STATE	
1	'initialized' state	
2	'enrolled' state	
TP Id		SECPKI_ITSS_ENR_RCV_02_BV
		The IUT is capable of parsing and handling of positive EnrolmentResponse messages
Summary		containing the requested EC. In case of a successful enrolment, the IUT switches to the
-		state 'enrolled'.
Reference		ETSI TS 102 941 [1], clauses 6.1.3, 6.2.3.2.1 and 6.2.3.2.2
Configuration		CFG_ENR_ITSS
PICS Selection		
		Expected behaviour
with		•
the IUT I	being in the 'initia	lized' state
ensure that	•	
when		
the IUT is requested to send an initial EnrolmentRequestMessage		

the IUT is requested to send an initial EnrolmentRequestMessage

and when the IUT receives a subsequent EnrolmentResponseMessage as an answer of the EA

containing a responseCode

indicating 0 and containing an enrolment certificate

then

the IUT switches to the 'enrolled' state

5.2.3 Authorization

5.2.3.0 Overview

All test purposes in clause 5.2.3.1 may be included in the test sequence if following PICS items are set:

PICS_SECPKI_AUTHORIZATION = TRUE

5.2.3.1 Authorization request

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

the IUT sends an EtsiTs103097Data to the AA

TP ld	SECPKI ITSS AUTH 02 BV		
	Check that the AuthorizationRequest message is encrypted and sent to only one		
Summary	Authorization Authority		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1		
Configuration	CFG_AUTH_ITSS		
PICS Selection			
	Expected behaviour		
with			
the AA in 'operational' sta	te		
authorized with CERT_	AA certificate		
ensure that			
when			
the IUT is triggered to a	request new Authorization Ticket (AT)		
then	then		
the IUT sends a EtsiTs			
containing content.encryptedData.recipients			
indicating size 1			
and containing the instance of RecipientInfo			
containing certRecipInfo			
containing recipientId			
indicating HashedId8 of the CERT_AA			

TP ld	SECPKI ITSS AUTH 03 BV
Summary	Check that the AuthorizationRequest message is encrypted using the encryptionKey
	found in the AA certificate referenced in recipientId
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITSS
PICS Selection	
	Expected behaviour
with	
the AA in 'operational' s	state
authorized with CER	T_AA certificate
containing encrypt	ionKey (AA_ENC_PUB_KEY)
ensure that	
when	
the IUT is triggered to	o request new Authorization Ticket (AT)
then	
the IUT sends a Etsi	Ts103097Data to the AA
containing content	t.encryptedData
containing ciphe	ertext
containing da	
encrypted	using AA_ENC_PUB_KEY

TP ld	SECPKI_ITSS_AUTH_04_BV
Summany	Check that the AuthorizationRequest message is never reused the same encryption key
Summary	and nonce
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITSS
PICS Selection	
	Expected behaviour
with	
the AA in 'operational' s	itate
ensure that	
when	
the IUT is triggered to	o request new Authorization Ticket (AT)
then	
the IUT sends a Etsi	Ts103097Data to the AA
containing content	
	ertext.aes128ccm.nonce
	ue not equal to the nonce in N previous messages
	recipients[0].certRecipInfo.encKey
	crypted symmetric key (S_KEY)
م به مناده ما ام من	symmetric key not equal to the key was used in N previous messages

TP ld	SECPKI_ITSS_AUTH_05_BV	
Summary	Check that the Authorization request protocol version is set to 1	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_ITSS	
PICS Selection		
	Expected behaviour	
with		
the AA in 'operation	nal' state	
ensure that		
when		
the IUT is trigger	red to request new Authorization Ticket (AT)	
then		
the IUT sends a	EtsiTs103097Data to the AA	
containing Ets	siTs102941Data	
containing	version	
containin	ng indicating 1	
containing		

containing conte	ent
containing au	thorizationRequest

TP ld	SECPKI_ITSS_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_ITSS
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT is triggered to	request new Authorization Ticket (AT)
then	
the IUT sends a EtsiT	s103097Data to the AA
containing EtsiTs10	02941Data
containing autho	rizationRequest
containing put	blicKeys
containing	verificationKey
indicating	value not equal to the field verificationKey of N previous messages
and not con	taining encryptionKey
or containin	g encryptionKey
	value not equal to the field encryptionKey of N previous messages
and containing	g hmacKey
	alue not equal to the field hmacKey of N previous messages

TP ld	SECPKI_ITSS_AUTH_07_BV
Summary	Check that ITS-S sends Authorization request with properly calculated keyTag field
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITSS
PICS Selection	
	Expected behaviour
with	
the AA in 'operationa	al' state
ensure that	
when	
the IUT is triggere	d to request new Authorization Ticket (AT)
then	
the IUT sends a E	tsiTs103097Data to the AA
containing Etsi7	rs102941Data
containing au	uthorizationRequest
containing	sharedAtRequest
	ng keyTag
	ating properly calculated value

TP ld	SECPKI_ITSS_AUTH_08_BV
Summary	Check that ITS-S sends Authorization request with eald of EA certificate
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITSS
PICS Selection	
	Expected behaviour
with	
the AA in 'operationa	al' state
ensure that	
when	
the IUT is triggere	ed to request new Authorization Ticket (AT)
then	
the IUT sends a E	tsiTs103097Data to the AA
containing Etsi	Fs102941Data
containing au	uthorizationRequest
containing	sharedAtRequest
containi	ing eald
indica	ating HashedId8 if EA certificate

TP ld	SECPKI_ITSS_AUTH_09_BV
Summary	Check that ITS-S sends Authorization request with the certificateFormat equal to 1
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITSS
PICS Selection	
	Expected behaviour
with	
the AA in 'operationa	al' state
ensure that	
when	
the IUT is triggere	ed to request new Authorization Ticket (AT)
then	
the IUT sends a E	EtsiTs103097Data to the AA
containing Etsi	Ts102941Data
containing a	uthorizationRequest
	g sharedAtRequest
	ing certificateFormat
	ating 1

TP ld	SECPKI_ITSS_AUTH_10_BV
Summary	Check that ITS-S sends Authorization request certificate attributes are properly set
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITSS
PICS Selection	
	Expected behaviour
with	
the AA in 'operational'	state
ensure that	
when	
the IUT is triggered t	to request new Authorization Ticket (AT)
then	
the IUT sends a Etsi	Ts103097Data to the AA
containing EtsiTs?	102941Data
containing auth	orizationRequest
containing sh	naredAtRequest
containing	requestedSubjectAttributes
containi	ng appPermissions
	containing certIssuePermissions

TP ld	SECPKI_ITSS_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_ITSS
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT is trigge	red to request new Authorization Ticket (AT)
then	
the IUT sends a	EtsiTs103097Data to the AA
containing Ets	siTs102941Data
containing	authorizationRequest
containir	ng ecSignature
contai	ning structure of type EtsiTs103097Data-SignedExternalPayload
con	taining hashId
iı	ndicating supported hash algorithm (HASH_ALG)
and	I containing tbsData
C	ontaining payload
	containing extDataHash
	indicating hash of sharedATRequest using HASH_ALG

TP ld	SECPKI_ITSS_AUTH_12_BV
C	Check that the ecSignature psid is set to the proper ITS_AID
Summary	Check that the ecSignature generation time is present
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITSS
PICS Selection	
	Expected behaviour
with	
the AA in 'operation	al' state
ensure that	
when	
the IUT is trigger	ed to request new Authorization Ticket (AT)
then	
the IUT sends a I	EtsiTs103097Data to the AA
	iTs102941Data
	nuthorizationRequest
	g ecSignature
	ing structure of type EtsiTs103097Data-SignedExternalPayload
	aining tbsData
CC	ontaining headerInfo
	containing psid
	indicating AID_PKI_CERT_REQUEST
	and containing generationTime
	and not containing any other headers
TP ld	SECPKI ITSS AUTH 13 BV

ummary Check that ITS-S sends Authorization request containing EC signature Leference ETSI TS 102 941 [1], clause 6.2.3.3.1	
eference ETSI TS 102 941 [1], clause 6.2.3.3.1	
configuration CFG_AUTH_ITSS	
ICS Selection	
Expected behaviour	
rith	
the AA in 'operational' state	
nsure 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 algoritm	

TP ld	SECPKI_ITSS_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
Summary	the EC's verification public key
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration PICS Selection	CFG_AUTH_ITSS
PICS Selection	Forward a d hack as do un
	Expected behaviour
ensure that	
when	
	ed to request new Authorization Ticket (AT)
then	
	EtsiTs103097Data to the AA
	Ts102941Data
5	
	g ecSignature
	ing structure of type EtsiTs103097Data-SignedExternalPayload
	aining signer
	dicating HashedId8 of EC certificate
	aining signature
Inc	dicating signature over sharedATRequest calculated with EC verificationKey
TP ld	SECPKI_ITSS_AUTH_15_BV
	Check that the encrypted ecSignature of the Authorization request is encrypted using the
_	EA encryptionKey
Summary	Check that the encrypted ecSignature of the Authorization request was done from the
	EtsiTs103097Data-SignedExternalPayload structure
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITSS

Configuration	CFG_AUTH_ITSS		
PICS Selection	PICS_PKI_AUTH_PRIVACY=TRUE		
	Expected behaviour		
with			
the AA in 'operational' sta	te		
and the EA in 'operationa	l' state		
authorized with CERT_	EA certificate		
ensure that			
when			
the IUT is triggered to r	request new Authorization Ticket (AT)		
then			
the IUT sends a EtsiTs	103097Data to the AA		
containing EtsiTs102	2941Data		
	containing authorizationRequest		
	containing ecSignature		
containing encryptedEcSignature			
containing recipients			
containing only one element of type RecipientInfo			
containing certRecipInfo			
containing recipientId			
indicating HashedId8 of the CERT_EA			
and containing encKey			
indicating encryption key of supported type			
	and containing cypertext		
containing encrypted representation of structure EtsiTs103097Data-SignedExternalPayload			

TP ld	SECPKI_ITSS_AUTH_16_BV
Summary	Check that the ecSignature of the Authorization request is not encrypted
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITSS
PICS Selection	PICS_PKI_AUTH_PRIVACY=FALSE
	Expected behaviour
then	request new Authorization Ticket (AT) s103097Data to the AA 2941Data izationRequest ignature

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

TP ld	SECPKI_ITSS_AUTH_18_BV	
	Check that the Authorization request is signed when Prove of Possession is used	
Summary	Check that proper headers is used in Authorization request with POP	
-	Check that the Authorization request with POP is self-signed	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_ITSS	
PICS Selection	PICS_PKI_AUTH_POP=TRUE	
	Expected behaviour	
with		
the AA in 'operational	' state	
ensure that		
when		
the IUT is triggered	to request new Authorization Ticket (AT)	
then		
the IUT sends a Ets	siTs103097Data-Encrypted to the AA	
containing cyphe		
	crypted representation of the EtsiTs103097Data-Signed	
	content.signedData	
containin		
	ing valid hash algorithm	
	aining tbsData	
	ning headerInfo	
	taining psid	
	dicating AID_PKI_CERT_REQUEST	
	containing generationTime	
	not containing any other headers	
and containing signer		
	containing self	
	aining signature	
	ing value calculated over tbsData with the private key	
COFF	espondent to the verificationKey from this message	

TD ! !	
TP ld	SECPKI_ITSS_AUTH_19_BV
Summary	Check that the signing of ecSignature of the Authorization request is permitted by the EC
	certificate
Reference	ETSI TS 102 941 [1], clause B.5
Configuration	CFG_AUTH_ITSS
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT is triggered to	request new Authorization Ticket (AT)
then	
the IUT sends a EtsiTs	103097Data to the AA
containing EtsiTs102	
containing authori	•
containing ecSi	
	tructure of type EtsiTs103097Data-SignedExternalPayload
containing	
	ng Hashedld8 of EC certificate
	ining appPermissions
	taining an item of type PsidSsp
C	ontaining psid
	indicating AID_CERT_REQ
a	nd containing ssp
	containing opaque[0] (version)
	indicating 1
	containing opaque[1] (value)
	indicating 'Enrolment Request' (bit 1) set to 1

5.2.3.2 Authorization response handling

Void.

5.2.4 CTL handling

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

TP ld	SECPKI_ITSS_CTL_02_BV	
Summary	Check that the IUT untrust the RCA when it is deleted from ECTL	
Reference	ETSI TS 102 941 [1], clause 6.3.5	
Configuration	CFG_CTL_ITSS	
PICS Selection		
	Expected behaviour	
with		
the IUT trusting the CER	T_RCA	
the IUT has received the	the IUT has received the TLM CTL	
not containing the CEI	RT_RCA	
ensure that	•	
when		
the IUT received a CA	M	
signed with AT certi	signed with AT certificate	
signed with AA certificate		
signed with CERT_RCA		
then		
the IUT rejects this CA	AM	

TP ld	SECPKI_ITSS_CTL_03_BV	
Summary	Check that the IUT trust the AA when it is received in RCA CTL	
Reference	ETSI TS 102 941 [1], clause 6.3.5	
Configuration	CFG_CTL_ITSS	
PICS Selection		
	Expected behaviour	
with		
the IUT doesn't have the	CERT_AA_NEW	
the IUT has received the	the IUT has received the RCA CTL	
containing the CERT_A		
and signed by CERT_F	and signed by CERT_RCA	
ensure that		
when		
the IUT received a CAM	the IUT received a CAM	
signed with AT certificate		
signed with CERT_AA_NEW digest		
then	-	
the IUT accepts this CA	AM	

TP ld	SECPKI_ITSS_CTL_04_BV
Summary	Check that the IUT requests new ECTL when current one is expired
Reference	ETSI TS 102 941 [1], clause 6.3.5
Configuration	CFG_CTL_ITSS
PICS Selection	
	Expected behaviour
with the IUT already downloa containing nextUpdat indicating timestan and containing CPOO ensure that when the T1 < CURRENT then the IUT sends a requ	te np T1 C URL

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

5.2.5 CRL handling

Void.

5.3 EA behaviour

5.3.1 Enrolment request handling

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

TP ld	SECPKI_EA_ENR_RCV_02_BI	
Summary	Check that EA does not accept Enrolment rekeying request when enrolment is not	
Summary	permitted by signing certificate.	
eference ETSI TS 102 941 [1], clause B.5		
Configuration	CFG_ENR_EA	
PICS Selection		
	Expected behaviour	
ensure that		
when		
	nrolmentRequestMessage	
	oted EtsiTs103097Data-Signed	
containing signer		
containing diges		
5	shedId8 of the certificate CERT	
	containing appPermissions	
	not containing an item of type PsidSsp	
	containing psid	
	ting AID_CERT_REQ ing an item of type PsidSsp	
containi		
	ting AID_CERT_REQ	
	taining ssp	
	ning opaque[0] (version)	
	cating other value than 1	
or containing opaque[1] (value)		
indicating 'Enrolment Request' (bit 1) set to 0		
then		
the IUT answers with a	an EnrolmentResponseMessage	
containing InnerECResponse		
containing respons	containing responseCode	
indicating 'deniedpermissions'		

5.3.2 Enrolment response

TP ld	SECPKI_EA_ENR_01_BV	
Summary	The EnrolmentResponse message shall be encrypted using an ETSI TS 103 097 [2] approved algorithm and the encryption shall be done with the same AES key as the one used by the ITS-S requestor for the encryption of the EnrolmentRequest message.	
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2	
Configuration	CFG_ENR_EA	
PICS Selection		
	Expected behaviour	
containing encKey containing an er then the IUT answers wit	ensure that when the IUT receives an EnrolmentRequestMessage containing encKey containing an encrypted AES key (SYMKEY) then the IUT answers with an EnrolmentResponseMessage containing cipherText	

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

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

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

TP ld	SECPKI_EA_ENR_05_BV
Summary	Within the headerInfo of the tbsData, the psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [i.2] and the generationTime shall be present.
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
then	n EnrolmentResponseMessage as an answer for an EnrolmentRequestMessage
the IUT sends a	n EtsiTs103097Data-Encrypted structure
containing an e containing the containing	
containing	
	ng AID_CERT_REQ
and contr	aining generationTime

TP ld	SECPKI_EA_ENR_06_BV
Summany	Within the headerInfo of the tbsData, aside from psid and generationTime, all other
Summary	components of the component tbsData.headerInfo not used and absent.
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT sends an Enro	plmentResponseMessage as an answer for an EnrolmentRequestMessage
then	
the IUT sends an Etsi	Ts103097Data-Encrypted structure
containing an encryp	ted EtsiTs103097Data-Signed structure
containing the Data	
containing headerInfo	
containing psid	
and containing generationTime	
and not containing any other component of tbsData.headerInfo	

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

TP ld	SECPKI EA ENR 08 BV		
	The InnerECResponse shall contain the requestHash, which is the left-most 16 octets of		
Summary	the SHA256 digest of the EtsiTs103097Data - Signed structure received in the request and		
-	a responseCode indicating the result of the request.		
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2		
Configuration	CFG_ENR_EA		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the IUT sends an E	the IUT sends an EnrolmentResponseMessage as an answer for an EnrolmentRequestMessage		
then			
	EtsiTs103097Data-Encrypted structure		
containing an end	rypted EtsiTs103097Data-Signed structure		
containing tbsD	containing tbsData		
containing EtsiTS102941Data			
containing InnerECResponse			
containing requestHash			
indicating the left-most 16 octets of the SHA256 digest			
of the EtsiTs103097Data-Signed structure received in the request			
and containing responseCode			

TP ld	SECPKI_EA_ENR_09_BV	
C	If the responseCode is 0, the InnerECResponse shall also contain an (enrolment)	
Summary	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 reques	sted to send an EnrolmentResponseMessage	
containing a re	sponseCode	
indicating 0	indicating 0	
then		
	n EtsiTs103097Data-Encrypted structure	
containing an encrypted EtsiTs103097Data-Signed structure		
containing tbsData		
containing EtsiTS102941Data		
containing InnerECResponse		
containing an enrolment certificate		

TP ld	SECPKI_EA_ENR_10_BV	
0	If the responseCode is different than 0, the InnerECResponse shall not contain a	
Summary	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 reque	sted to send an EnrolmentResponseMessage	
containing a re	esponseCode	
indicating a v	indicating a value different than 0	
then		
	n EtsiTs103097Data-Encrypted structure	
containing an encrypted EtsiTs103097Data-Signed structure		
containing tbsData		
containing EtsiTS102941Data		
containing	containing InnerECResponse	
not containing a certificate		

TP ld			
Summary	ummary Check that signing of Enrolment response message is permitted by the EA certificate.		
Reference	eference ETSI TS 102 941 [1], clause B.5		
Configuration	CFG_ENR_EA		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the IUT sends an Enro	ImentResponseMessage as an answer for an EnrolmentRequestMessage		
then			
	s103097Data-Encrypted structure		
	containing an encrypted EtsiTs103097Data-Signed structure		
	containing signer		
declared as a dige			
	lashedId8 of the EA certificate		
containing appPermissions			
containing an item of type PsidSsp			
containing psid			
indicating AID_CERT_REQ			
and containing ssp			
containing opaque[0] (version)			
	indicating 1		
containing opaque[1] (value) indicating bit 'Enrolment Response' (5) set to 1			
Indica			

TP ld	SECPKI_EA_ENR_12_BV
	Check that generated EC certificate contains only allowed permissions.
	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 EnrolmentResponseMessage
containing a certificat	e (EC_CERT)
then	
the EC_CERT	
containing appPermi	
containing an item	of type PsidSsp
containing psid	
	D_CERT_REQ
and containing	
	paque[0] (version)
indicating 1 containing opaque[1] (value)	
	Enrolment Request' (bit 0) set to 1 Authorization Request' (bit 1) set to 1
	other bits set to 0
	ng an item of type PsidSsp
containing psid	iy an item of type i sloosp
indicating AIE) CTI
and NOT containing an item of type PsidSsp	
containing psid	
indicating AID_CRL	

5.3.3 Authorization validation request handling

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

TP ld	SECPKI_EA_AUTHVAL_RCV_02_BI
C	Check that EA does not accept Authorization Validation Request when SharedAtRequest
Summary	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	
	uthorizationValidationRequestMessage
containing EtsiTs10	
containing ecSigr	
containing sign	
containing di	
	HashedId8 of the certificate EC certificate
	g appPermissions
	itaining an item of type PsidSsp
	icating AID_CERT_REQ
	aining an item of type PsidSsp iining psid
	icating AID_CERT_REQ
	containing ssp
	itaining opaque[0] (version)
	idicating other value than 1
	containing opaque[1] (value)
	dicating 'Authorization Request' (bit 2) set to 0
then	
	an AuthorisationValidationResponseMessage
containing response	i v
indicating 'denied	

5.3.4 Authorization validation response

TP ld	SECPKI_EA_AUTHVAL_01_BV
Summary	The EtsiTs103097Data-Encrypted is built with the component recipients containing one instance of RecipientInfo of choice pskRecipInfo, which contains the HashedId8 of the symmetric key used by the ITS-S to encrypt the AuthorizationRequest message to which the response is built and the component ciphertext containing the encrypted representation of the EtsiTs103097Data-Signed. The encryption uses a ETSI TS 103 097 [2] approved algorithm.
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2 ETSI TS 103 097 [2], clause 7
Configuration	CFG_AVALID_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
	a AuthorizationValidationRequest message
containing encKe	
	encrypted symmetric data encryption key (SYMKEY)
then	
	AuthorizationValidationResponse message
5	Ts103097Data-Encrypted
containing red	
	one instance of RecipientInfo of choice pskRecipInfo
indicating the HashedId8 of SYMKEY	
and containing ciphertext	
5	EtsiTs103097Data-Signed
being end	rypted 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 AuthorizationValidationRequest message

then

the IUT sends a AuthorizationValidationResponse message containing EtsiTs103097Data-Signed

containing EtsiTs102941Data

containing AuthorizationValidationResponse

TP ld	SECPKI_EA_AUTHVAL_03_BV
Summary	The AuthorizationValidationResponse structure contains the requestHash being the left- most 16 octets of the SHA256 digest of the EtsiTs103097Data-Signed structure received in the AuthorizationValidationRequest and a responseCode.
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2
Configuration	CFG_AVALID_EA
PICS Selection	
	Expected behaviour
ensure that when	
the IUT receives	a AuthorizationValidationRequest_message Ts103097Data-Signed structure (REQDSS)
then	
	AuthorizationValidationResponse message iTs103097Data-Signed

ontaining EtsiTs103097Data-Signed containing EtsiTs102941Data containing i

containing AuthorizationValidationResponse

containing requestHash

indicating the left-most 16 octets of the SHA256 digest of REQDSS

and containing responseCode

TP Id	SECPKI EA AUTHVAL 04 BV
Summary	If the responseCode is 0, the AuthorizationValidationResponse structure contains the component confirmedSubjectAttributes with the attributes the EA wishes to confirm, except for certIssuePermissions which is not allowed to be present.
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2
Configuration	CFG_AVALID_EA
PICS Selection	
	Expected behaviour
and the IUT responds containing Authoriza containing respons indicating 0 then the sent Authorization contains an Authorization	horizationValidationRequest message with a AuthorizationValidationResponse message tionValidationResponse ecCode /alidationResponse message ationValidationResponse structure edSubjectAttributes wrtIssuePermissions

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

SECPKI_EA_AUTHVAL_06_BV	
The component version of the EtsiTs102941Data structure is set to v1 (integer value set to 1).	
ETSI TS 102 941 [1], clause 6.2.3.4.2	
CFG_AVALID_EA	
Expected behaviour	
a AuthorizationValidationRequest message	
AuthorizationValidationResponse message ITs103097Data-Signed tsiTs102941Data	
containing version indicating 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 Aut	the IUT receives a AuthorizationValidationRequest message		
then			
the IUT sends a Author	prizationValidationResponse message		
containing EtsiTs103	3097Data-Signed		
containing tbsData	containing tbsData		
containing headerInfo			
containing psid			
indicating AID_CERT_REQ			
and containing	and containing generationTime		
and not containing any other component of tbsdata.headerInfo			

TP ld	SECPKI EA AUTHVAL 08 BV
	EtsiTs103097Data-Signed structure shall contain hashId, tbsData, signer and signature. The hashId shall indicate the hash algorithm to be used as specified in ETSI
Summany	TS 103 097 [2], the signer shall be declared as a digest, containing the HashedId8 of the
Summary	EA certificate and the signature over tbsData shall be computed using the EA private key
Defenses	corresponding to its public/erificationKey found in the referenced EA certificate.
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2
Configuration	CFG_AVALID_EA
PICS Selection	Eurostad habaviour
ensure that	Expected behaviour
when	
	AuthorizationValidationRequest message
then	AutionzationvaluationRequest message
	uthorizationValidationResponse message
	iTs103097Data-Signed structure
containing hash	
	hash algorithm to be used as specified in ETSI TS 103 097 [2]
and containing	
and containing	
declared as a	
	he HashedId8 of the EA certificate
and containing	
computed ove	
	A private key
	inding to the publicVerificationKey found in the referenced EA certificate
concopon	tang to the public volundation to y round in the relevance and the relation of a
TO 11	
TP ld	SECPKI_EA_AUTHVAL_09_BV
Summary	Check that signing of Authorization Validation response message is permitted by the EA
2	certificate.
Reference	ETSI TS 102 941 [1], clause B.5
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
	ed to send an AuthorizationValidationResponseMessage
then	
	EtsiTs103097Data-Encrypted structure
	crypted EtsiTs103097Data-Signed structure
containing signe	
containing dig	
	lashedId8 of the EA certificate
	g appPermissions
	ng an item of type PsidSsp
	ining psid
indic	cating AID_CERT_REQ
	ontaining ssp
	taining opaque[0] (version)
inc	dicating 1

containing opaque[1] (value) indicating 'Authorisation Validation Response' (bit 4) set to 1

5.3.5 CA Certificate Request

TP Id	SECONI EA CACEDICEN 01 DV
	SECPKI_EA_CACERTGEN_01_BV
Summary	SubCA certificate requests of the EA are transported to the RCA using
Summary	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 reques	sted to send a CACertificateRequestMessage
then	
the II IT sends a	CACertificateRequestMessage

41

the IUT sends a CACertificateRequestMessage across the reference point S10 to the RCA

TP ld	SECPKI_EA_CACERTGEN_02_BV
Summary	The application form should include the digital fingerprint of the CACertificateRequestMessage in printable format. The digital fingerprint of the CACertificateRequestMessage is computed using a ETSI TS 103 097 [2] approved hash algorithm.
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_INIT
PICS Selection	
	Expected behaviour
then the IUT sends a CACe containing a signatu being computed u	o send a CACertificateRequestMessage ertificateRequestMessage

TP ld	SECPKI_EA_CACERTGEN_03_BV
	The hashId shall indicate the hash algorithm to be used as specified in ETSI
0	TS 103 097 [2], the signer is set to 'self' and the signature over the tbsData is computed
Summary	using the private key corresponding to the new verificationKey to be certified (i.e. the
	request is self-signed).
Deference	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 'initia	al' state
ensure that	
when	
	o send a CACertificateRequestMessage
then	
	ertificateRequestMessage
	097Data-Signed structure
containing hashld	
	ash algorithm to be used
and containing sig	jner
indicating 'self' and containing tb	»Dete
	ertificateRequest
containing cac	
containing verification_key (VKEY) and containing signature	
	tbsData using the private key corresponding to the verificationKey (VKEY)

TP ld	SECPKI_EA_CACERTGEN_04_BV	
Summary	An ECC private key is randomly generated, the corresponding public key (verificationKey) is provided to be included in the CaCertificateRequest. An ECC encryption private key is randomly generated, the corresponding public key (encryptionKey) is provided to be included in the CACertificateRequest. CaCertificateRequest.publicKeys shall contain verification_key and encryption_key.	
Reference	ETSI TS 102 941 [1], clause 6.2.1	
Configuration	CFG_CAGEN_INIT	
PICS Selection		
	Expected behaviour	
with the IUT being in the 'initial' state ensure that when the IUT is requested to send a CACertificateRequestMessage then the IUT sends a CACertificateRequestMessage containing CaCertificateRequestMessage containing publicKeys containing publicKeys		

TP ld	SECPKI_EA_CACERTGEN_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
then the IUT sends a C containing EtsiT containing ver	ed to send a CACertificateRequestMessage ACertificateRequestMessage s102941Data

TP ld	SECPKI_EA_CACERTGEN_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 ensure that when			
	ted 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_CACERTGEN_07_BV
Summary	EtsiTs103097Data-Signed.tbsData contains the EtsiTs102941Data as payload and the headerInfo containing psid and generationTime. The psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [i.2] and the generationTime shall be present. All other components of the component tbsdata.headerInfo are not used and absent.
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_INIT
PICS Selection	
	Expected behaviour
with	
the IUT being in the 'init	ial' state
ensure that	
when	
the IUT is requested to send a CACertificateRequestMessage	
then	
	ertificateRequestMessage
containing headerInfo	
containing psid	
indicating SEC_CERT_REQ	
and containing generationTime and not containing any other component of tbsdata.headerInfo	

TP ld	SECPKI_EA_CACERTGEN_08_BV
Summary	If the current private key has reached its end of validity period or is revoked, the SubCA
	shall restart the initial certificate application process.
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_REKEY
PICS Selection	
	Expected behaviour
with	
the IUT being in the	operational' state
ensure that	
when	
the IUT is reques	ted to send a CACertificateRekeyingMessage
and SubCA certif	icate is no longer valid (due to end of validity or revocation)
then	
the ILIT switches	to the "initial' state

the IUT switches to the "initial' state and sends a CACertificateRequestMessage

	SECPKI_EA_CACERTGEN_09_BV For the re-keying application to the RCA (CaCertificateRekeyingMessage), an EtsiTs103097Data-Signed structure is built, containing: hashId, tbsData, signer and
Summary	signature. The hashId shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [2]. The signer declared as a digest, containing the hashedId8 of the EA certificate and the signature over tbsData is computed using the currently valid private key corresponding to the EA certificate (outer signature).
Poforonco	ETSI TS 102 941 [1], clause 6.2.1 ETSI TS 103 097 [2], clause 7
Configuration	CFG_CAGEN_REKEY
PICS Selection	
	Expected behaviour
with the IUT being in the 'operational' state ensure that when the IUT is requested to send a CACertificateRekeyingMessage then the sends a CACertificateRekeyingMessage being an EtsiTs103097Data-Signed structure containing hashId indicating the hash algorithm to be used and containing tbsData and containing signer containing digest indicating HashedId8 of the SubCA certificate (CERT) and containing signature computed over tbsData	

TP ld	SECPKI_EA_CACERTGEN_10_BV	
Summary	The (outer) tbsData of the CACertificateRekeyingMessage shall contain the	
	CaCertificateRequestMessage as payload.	
Reference	ETSI TS 102 941 [1], clause 6.2.1	
Configuration	CFG_CAGEN_REKEY	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the	operational' state	
ensure that		
when		
the IUT is reques	the IUT is requested to send a CACertificateRekeyingMessage	
then		
the sends a CACertificateRekeyingMessage		
containing tbsData		
containing CaCertificateRequestMessage		

TP ld	SECPKI_EA_CACERTGEN_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
ensure that when the IUT is reque then	

Containing tostbala Containing headerInfo containing psid indicating SEC_CERT_REQ and containing generationTime and not containing any other component of tbsdata.headerInfo

TP ld		
Summary	Check that the CaCertificateRekeyingMessage is permitted by CA certificate	
Reference	ETSI TS 102 941 [1], clause 6.2.1	
Configuration	CFG_CAGEN_REKEY	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the 'oper	rational' state	
ensure that		
when		
	send a CACertificateRekeyingMessage	
then		
the sends a CACertific		
5	being an EtsiTs103097Data-Signed structure	
	and containing tbsData	
and containing sig	gner	
containing digest	adde at the CA contificate	
	edId8 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		
	ng opaque[1] (value)	
indicating 'CA Certificate Response' (bit 6) set to 1		

5.4 AA behaviour

5.4.1 Authorization request handling

TP ld	SECPKI_AA_AUTH_RCV_01_BV	
	Check that the AA is able to decrypt the AuthorizationRequest message using the	
	encryption private key corresponding to the recipient certificate	
0	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 Authorization Validation Request message to the	
	correspondent EA.	
Deference		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_AA	
PICS Selection	PICS_PKI_AUTH_POP=TRUE	
with	Expected behaviour	
the AA in 'operational' sta		
authorized with the ce	=	
÷	onKey (AA_ENC_PUB_KEY)	
ensure that		
when		
	e EtsiTs103097Data message	
containing content.e		
containing recipie		
	instance of RecipientInfo	
containing c	ertRecipInfo	
containing	g recipientId	
	ng HashedId8 of the certificate CERT_AA	
and conta	ining encKey	
indicating symmetric key (S_KEY)		
	ypted with the private key correspondent to the AA_ENC_PUB_KEY	
	/phertext (ENC_DATA)	
containing encrypted representation of the EtsiTs103097Data-Signed		
containing encrypted representation of the Elsi's rosos a bata-signed		
containing		
	ng valid hash algorithm	
and containi		
containing		
and containing tbsData (SIGNED_DATA)		
containing payload		
containing EtsiTs102941Data		
containing content.authorizationRequest		
containing publicKeys.verificationKey (V_KEY)		
and containing hmacKey (HMAC)		
and containing sharedAtRequest		
containing keyTag (KEY_TAG)		
and containing eald (EA_ID)		
indicating HashedId8 of the known EA certificate		
and containi	ng signature (SIGNATURE)	
then		
the IUT is able to decr		
using the private key		
corresponding to the AA_ENC_PUB_KEY		
and the IUT is able to decrypt the cypthertext ENC_DATA		
using the S_KEY		
	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 Authorization Validation Request message to the EA		
	identified by the EA_ID	

46

TP ld	SECPKI_AA_AUTH_RCV_02_BV	
	Check that the AA is able to decrypt the AuthorizationRequest message using the	
	encryption private key corresponding to the recipient certificate	
Summary	Check that the AA is able to verify the request authenticity using the hmacKey verification	
-	Check that the AA sends the AuthorizationValidationRequest message to the	
	correspondent EA.	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_AA	
PICS Selection	PICS_PKI_AUTH_POP=FALSE	
	Expected behaviour	
with		
the AA in 'operational		
	certificate CERT_AA	
	ptionKey (AA_ENC_PUB_KEY)	
ensure that		
when		
	the EtsiTs103097Data message	
	nt.encryptedData	
	containing recipients	
	containing the instance of RecipientInfo	
containing certRecipInfo		
containing recipientId		
indicating HashedId8 of the certificate CERT_AA		
	and containing encKey	
	cating symmetric key (S_KEY)	
encrypted with the private key correspondent to the AA_ENC_PUB_KEY		
and containing cyphertext (ENC_DATA) containing EtsiTs102941Data		
containing content.authorizationRequest		
containing content.authorizationizequest containing hmacKey (HMAC)		
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 cypthertext ENC_DATA		
using the S_KEY		
	to verify integrity of HMAC and KEY_TAG	
and the IUT sends the AuthorizationValidationRequest message to the EA		
identified by the EA_ID		

TP ld	SECPKI_AA_AUTH_RCV_03_BI	
Summary	Check that the AA skips the AuthorizationRequest message if it is not addressed to this AA	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_AA	
PICS Selection		
	Expected behaviour	
with		
the AA in 'operational' sta	te	
authorized with the cer	tificate CERT_AA	
containing encryption	nKey (AA_ENC_PUB_KEY)	
ensure that		
when		
the IUT is received the	the IUT is received 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)		
-	<pre>rpted with the private key correspondent to the AA_ENC_PUB_KEY</pre>	
then		
the IUT does not send	the IUT does not send the AuthorizationValidationRequest message	

TP ld	SECPKI_AA_AUTH_RCV_04_BI	
Summary	Check that the AA skips the AuthorizationRequest message if it 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 'operation	al' state	
authorized with th	e certificate CERT_AA	
containing encryptionKey (AA_ENC_PUB_KEY)		
ensure that		
when		
the IUT is receive	d the EtsiTs103097Data message	
containing cont	tent.encryptedData	
containing re	cipients	
containing	the instance of RecipientInfo	
	ing certRecipInfo	
conta	aining recipientId	
inc	dicating value	
	equal to the HashedId8 of the certificate CERT_AA	
and	containing encKey	
inc	dicating symmetric key (S_KEY)	
	encrypted with the OTHER private key than the correspondent to the AA_ENC_PUB_KEY	
then		
the IUT does not	send the AuthorizationValidationRequest message	

TP ld	SECPKI_AA_AUTH_RCV_05_BI
Summary	Check that the AA skips the AuthorizationRequest message if it unable to decrypt the
	cyphertext.
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with	
the AA in 'operation	al' state
authorized with the	he certificate CERT_AA
containing enc	ryptionKey (AA_ENC_PUB_KEY)
ensure that	
when	
the IUT is receive	ed the EtsiTs103097Data message
containing con	ntent.encryptedData
0	ecipients[0].encKey
	encrypted symmetric key (S_KEY)
	ing cyphertext (ENC_DATA)
encrypted with the OTHER key than S_KEY	
then	
	s not send the AuthorizationValidationRequest message to the correspondent EA

TP ld	SECPKI_AA_AUTH_RCV_06_BI		
Summary	Check that the AA rejects the AuthorizationRequest message if it unable to verify the POP		
Summary	signature.		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1		
Configuration	CFG_AUTH_AA		
PICS Selection	PICS_PKI_AUTH_POP=TRUE		
	Expected behaviour		
with			
the AA in 'operational' sta			
authorized with the cer			
• •	containing encryptionKey (AA_ENC_PUB_KEY)		
ensure that			
when			
	the IUT is received the EtsiTs103097Data message		
•	ncryptedData.cyphertext		
5 71	ted representation of the EtsiTs103097Data-Signed (SIGNED_DATA)		
containing cont			
containing tb			
containing			
	ng EtsiTs102941Data aining content.authorizationRequest		
	0		
	containing publicKeys.verificationKey (V_KEY)		
and containing signature (SIGNATURE) indicating value calculated with OTHER key than private key correspondent to V_KEY			
then			
	end the AuthorizationValidationRequest message		
and the IUT sends to the TS the Authorization Response message			
	containing authorizationResponse		
containing requestHash			
indicating the leftmost 16 bits of the SHA256 value			
	calculated over the SIGNED_DATA		
and containing res			
	alue NOT EQUAL to 0		
and not containing			

TP ld	SECPKI_AA_AUTH_RCV_07_BI		
Summary	Check that the AA rejects the Authorizatio	nRequest message if it unable to verify the	
Summary	integrity of the request using hmacKey.		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1		
Configuratio			
PICS Select	ion X_PICS		
	Expected behaviour		
with			
	operational' state		
	red with the certificate CERT_AA		
	ining encryptionKey (AA_ENC_PUB_KEY)		
ensure that			
when	is received the EtsiTs103097Data message		
	ining EtsiTs102941Data		
	ntaining content.authorizationRequest		
	containing hmacKey (HMAC)		
	and containing sharedAtRequest		
	containing keyTag (KEY_TAG)		
	indicating wrong value		
then			
	IUT does not send the AuthorizationValidationRequest m		
	IUT sends to the TS the AuthorizationResponse message		
	ining authorizationResponse		
	ntaining requestHash indicating the leftmost 16 bits of the SHA256 value		
	calculated over the X_HASH_STRUCTURE		
an	and containing responseCode		
	indicating the value NOT EQUAL to 0		
	d not containing certificate		
	Variants		
nn	X_PICS	X_HASH_STRUCTURE	
1	PICS_PKI_AUTH_POP=TRUE	EtsiTs103097Data-Signed	
2	PICS_PKI_AUTH_POP=FALSE	EtsiTs102941Data	

5.4.2 Authorization validation request

TP ld	SECPKI_AA_AUTHVAL_01_BV	
Summary	Check that the AA sends AuthorizationValidationRequest after receiving of the	
	AuthorizationRequest.	
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1	
Configuration	CFG_AUTH_AA	
PICS Selection		
	Expected behaviour	
with		
the EA in 'operational' state		
authorized with CERT	_EA certificate	
ensure that		
when		
the IUT received the AuthorizationRequest		
containing EtsiTs10		
5	nt.authorizationRequest	
containing sha	I	
containing eald (EA_ID)		
indicating HashedId8 of the CERT_EA		
then		
	EtsiTs103097Data message	
to the EA identified by EA_ID		

TPId SECPKI AA AUTHVAL 02 BV			
	SECPKI_AA_AUTHVAL_02_BV		
Summary	Check that the AuthorizationValidationRequest message is encrypted using approved		
-	algorithm and sent to only one Enrolment Authority.		
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1		
Configuration	CFG_AUTH_ITSS		
PICS Selection			
	Expected behaviour		
with			
the EA in 'operational' sta	ite		
authorized with CERT_EA certificate			
ensure that			
when			
the IUT is triggered to a	the IUT is triggered to send the AuthorizationValidationRequest to the EA		
then			
the IUT sends a EtsiTs	s103097Data		
containing content.e	containing content.encryptedData.recipients		
indicating size 1			
and containing the	and containing the instance of RecipientInfo		
containing certRecipInfo			
containing recipientId			
indicating HashedId8 of the CERT_EA			
and containin			
	eciesNistP256		
or containing eciesBrainpoolP256r1			

TDII		
TP ld	SECPKI_AA_AUTHVAL_03_BV	
Summary	Check that the AA sends AuthorizationValidationRequest signed by AA.	
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1	
Configuration	CFG_AUTH_AA	
PICS Selection		
	Expected behaviour	
With		
the AA in 'operational' sta authorized with CERT_ and the EA in 'operationa ensure that	AA certificate	
when		
the IUT is triggered to s	send the AuthorizationValidationRequest to the EA	
then	·	
the IUT sends a EtsiTs103097Data-Encrypted message containing EtsiTs103097Data-Signed containing signedData containing signer		
containing di	gest	
indicating HashedId8 value of the CERT_AA		

52

TP ld	SECPKI_AA_AUTHVAL_04_BV
Summary	Check that the AA sends signed AuthorizationValidationRequest with signature properly
	calculated using approved hash algorithm.
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
With	
the AA in 'operation	al' state
authorized with C	ERT_AA certificate
	ficationKey (AA_PUB_V_KEY)
and the EA in 'opera	
	ERT_EA certificate
ensure that	
when	
	ed to send the AuthorizationValidationRequest to the EA
then	
	EtsiTs103097Data-Encrypted message
	Ts103097Data-Signed
containing s	
containing	
	ng supported hash algorytm (HASH_ALG)
	aining signature
calcula	ted using the HASH_ALG and private key correspondent to the AA_PUB_V_KEY
TP ld	SECPKI_AA_AUTHVAL_05_BV
Cummon /	Check that the AA sends signed AuthorizationValidationRequest using proper signed data
Summary	headers.
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
With	L. L

With
the AA in 'operational' state
authorized with CERT_AA certificate
containing verificationKey (AA_PUB_V_KEY)
and the EA in 'operational' state
authorized with CERT_EA certificate
ensure that
when
the IUT is triggered to send the AuthorizationValidationRequest to the EA
then
the IUT sends a EtsiTs103097Data-Encrypted message
containing EtsiTs103097Data-Signed
containing signedData
containing tbsData
containing headerInfo
containing psid
indicating AID_PKI_CERT_REQUEST
and containing generationTime
and not containing any other headers

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

TP ld	SECPKI_AA_AUTHVAL_07_BV	
Summary	Check that the AA sends AuthorizationValidationRequest with sharedAtRequest and	
	ecSignature as it was requested in the triggering AuthorizationRequest.	
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 'operational' state		
ensure that		
when		
the IUT received the A		
•	containing EtsiTs102941Data	
	nt.authorizationRequest	
	redAtRequest (SHARED_AT_REQUEST)	
and containing ecSignature (EC_SIGNATURE)		
then		
the IUT sends a EtsiTs103097Data-Encrypted message		
containing EtsiTs102941Data		
containing content.authorizationValidationRequest		
containing sharedAtRequest		
	HARED_AT_REQUEST	
and containing		
indicating EC_SIGNATURE		

TP ld		
Summary	Check that signing of Authorization Validation request message is permitted by the AA	
	certificate.	
Reference	ETSI TS 102 941 [1], clause B.5	
Configuration	CFG_AUTH_AA	
PICS Selection		
	Expected behaviour	
ensure that		
when		
the IUT is triggered to s	send the AuthorizationValidationRequest to the EA	
then		
the IUT sends an EtsiTs103097Data-SignedAndEncrypted structure		
containing signer		
declared as a digest		
containing the HashedId8 of the AA certificate		
containing appPermissions		
containing an item of type PsidSsp		
containing psid		
indicating AID_CERT_REQ		
and containing ssp		
containing opaque[0] (version)		
indicating 1		
containing opaque[1] (value)		
indicating 'Enrolment Request' (bit 1) set to 1		

5.4.3 Authorization validation response handling

TP ld	SECPKI_AA_AUTHVAL_RCV_01_BV
Summary	Check that the AA sends AuthorizationResponse after receiving the AuthorizationRequest.
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with the ITSS in 'enrolled' state the EA in 'operational' state and the IUT(AA) in 'operational' state and the IUT had received the AuthorizationRequest from the ITSS and the IUT sent the AuthorizationValidationRequest ensure that when the IUT received the AuthorizationValidationResponseMessage then the IUT sends the EtsiTs103097Data message to the ITSS	

TP ld	SECPKI_AA_AUTHVAL_RCV_02_BI	
Summary	Check that AA does not accept Authorization Validation Response message when this	
	message is signed with certificate without appropriate permissions.	
Reference	ETSI TS 102 941 [1], clause B.5	
Configuration	CFG_AUTH_AA	
PICS Selection		
	Expected behaviour	
with		
the ITSS in 'enrolled' state	e	
the EA in 'operational' sta	ite	
and the IUT(AA) in 'opera		
	I the AuthorizationRequest from the ITSS	
	norizationValidationRequest	
ensure that		
when		
the IUT receives the AuthorizationValidationResponseMessage		
containing signer		
containing digest		
indicating HashedId8 of the certificate		
containing appPermissions		
	not containing an item of type PsidSsp	
containing psid		
indicating AID_CERT_REQ		
or containing an item of type PsidSsp		
containing		
	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		
	an AuthorizationValidationResponseMessage	
containing response		
indicating non-zero value		

5.4.4 Authorization response

TP Id	SECPKI AA AUTH 01 BV		
Summary Check that the AA sends encrypted AuthorizationResponse			
Reference ETSI TS 102 941 [1], clause 6.2.3.3.2			
configuration CFG_AUTH_AA			
PICS Selection			
	Expected behaviour		
with			
the ITSS in 'enrolled' state	e		
has sent the Authorizat	tionRequestMessage		
containing encrypted	denkKey		
containing AES symmetric key (SYM_KEY)			
the EA in 'operational' sta			
ensure that			
when			
the IUT is triggered to s	the IUT is triggered to send the authorization response to the ITSS		
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 ld	SECPKI_AA_AUTH_02_BV		
Summary	Check that the AA sends signed AuthorizationResponse		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2		
Configuration	CFG_AUTH_AA		
PICS Selection			
	Expected behaviour		
with			
the ITSS in 'enrolled	J' state		
and the IUT(AA) in '	operational' state		
authorized with C	ERT_AA certificate		
and the EA in 'opera	and the EA in 'operational' state		
ensure that			
when			
the IUT is triggere	ed to send the authorization response to the ITSS		
then			
the IUT sends the	e 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 AuthorizationResponse with signature properly calculated
	using approved hash algorithm
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with	
the ITSS in 'enrolled' state	9
and the IUT(AA) in 'opera	tional' state
authorized with CERT_	AA certificate
	nKey (AA_PUB_V_KEY)
and the EA in 'operational' state	
ensure that	
when	
the IUT is triggered to s	send the authorization response to the ITSS
then	
and the IUT sends the	EtsiTs103097Data-Encrypted message
containing the EtsiTs	s103097Data-Signed
containing signedData	
containing hashId	
indicating supported hash algorytm (HASH_ALG)	
and containing signature	
calculated us	ing the HASH_ALG and private key correspondent to the AA_PUB_V_KEY

TP ld	SECPKI AA AUTH 04 BV	
Summary	Check that the AA sends signed AuthorizationResponse with signature properly calculated	
	using approved hash algorithm	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2	
Configuration	CFG_AUTH_AA	
PICS Selection		
	Expected behaviour	
with	·	
the ITSS in 'enrolled	J' state	
and the IUT(AA) in '	operational' state	
and the EA in 'operation	ational' state	
ensure that		
when		
the IUT is triggere	ed to send the authorization response to the ITSS	
then		
the IUT sends a E	EtsiTs103097Data-Encrypted message	
containing Etsi	Ts103097Data-Signed	
containing s	ignedData	
containing	g tbsData	
contain	ing headerInfo	
conta	aining psid	
indicating AID_PKI_CERT_REQUEST		
and containing generationTime		
and not containing any other headers		

TP Id	SECPKI_AA_AUTH_05_BV		
Summary		ionResponse with signature properly calculated	
Guinnary	using approved hash algorithm		
Reference		ETSI TS 102 941 [1], clause 6.2.3.3.2	
Configurati			
PICS Select	tion X_PICS		
	Expected behaviour		
with			
	n 'enrolled' state		
	nt the AuthorizationRequestMessage		
	aining EtsiTs102941Data		
cc	ntaining authorizationResponse		
	containing X_DATA_STRUCTURE		
	JT(AA) in 'operational' state		
ensure that	A in 'operational' state		
when			
	is triggered to send the authorization response to the ITSS		
then	is inggered to send the admonzation response to the mod		
	sends a EtsiTs103097Data-Encrypted message		
	aining EtsiTs103097Data-Signed		
	ntaining EtsiTs102941Data		
	containing authorizationResponse		
containing requestHash			
indicating the leftmost 16 bits of the SHA256 value			
calculated over the X_DATA_STRUCTURE			
and containing responseCode			
	Variants		
nn	X_PICS	X_DATA_STRUCTURE	
1	PICS_PKI_AUTH_POP=TRUE	EtsiTs103097Data-Signed	
2	2 PICS_PKI_AUTH_POP=FALSE EtsiTs102941Data		

TP ld	SECPKI_AA_AUTH_06_BV	
Summary	Check that the AA includes the certificate in the positive AuthorizationResponse	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2	
Configuration	CFG_AUTH_AA	
PICS Selection		
	Expected behaviour	
with		
the ITSS in 'enrolled' state has sent the AuthorizationRequestMessage and the IUT(AA) in 'operational' state and the EA in 'operational' state ensure that		
when the IUT is sending to the ITSS the AuthorizationResponseMessage (MSG)		
containing responseCode indicating 0		

then

the message MSG containing certificate

TP Id SECPKI_AA_AUTH_07_BV Summary Check that the AA does not include the certificate in the negative AuthorizationResponse ETSI TS 102 941 [1], clause 6.2.3.3.2 Reference

Configuration	CFG_AUTH_AA		
PICS Selection	ICS Selection		
	Expected behaviour		
with	with		
the ITSS in 'enrolled' state	the ITSS in 'enrolled' state		
has sent the Authoriza	has sent the AuthorizationRequestMessage		
and the IUT(AA) in 'opera	and the IUT(AA) in 'operational' state		
and the EA in 'operationa	and the EA in 'operational' state		
ensure that	ensure that		
when	when		
the IUT is sending to the ITSS the AuthorizationResponseMessage (MSG)			
containing responseCode			
indicating negative value			
then			
the message MSG			
not containing certificate			

mmary C ference E nfiguration C		
ference E nfiguration C	TSI TS 102 941 [1], clause B.5	
nfiguration C		
	ETSI TS 102 941 [1], clause B.5	
	FG_ENR_EA	
S Selection		
	Expected behaviour	
sure that		
vhen		
the IUT sends an Authori	zationResponseMessage as an answer for an AuthorizationReguestMessage	
hen		
the IUT sends an EtsiTs1	03097Data-SignedAndEncrypted structure	
containing signer		
declared as a digest		
	nedId8 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 AuthorizationResponseMessage	
containing a certificat	te (AT_CERT)	
then		
the EC_CERT		
containing appPermi		
	n item of type PsidSsp	
	containing psid	
5	indicating AID_CERT_REQ	
or containing an item of type PsidSsp		
	containing psid	
indicating AID_CERT_REQ		
and containing ssp		
containing opaque[0] (version) indicating 1		
containing opaque[1] (value)		
indicating 00h		
and NOT containing an item of type PsidSsp		
containing psid		
indicating AID_CTL		
and NOT containing an item of type PsidSsp		
containing psid		
indicating AID_CRL		

59

5.4.5 CA Certificate Request

TP ld	SECPKI_AA_CACERTGEN_01_BV	
0	SubCA certificate requests of the AA are transported to the RCA using	
Summary	CACertificateRequest messages across the reference point S9.	
Reference	ETSI TS 102 941 [1], clause 6.2.1	
Configuration	CFG_CAGEN_INIT	
PICS Selection		
	Expected behaviour	
ensure that		
when		
the IUT is reques	sted to send a CACertificateRequestMessage	
then		
the IUT sends a	CACertificateRequestMessage	
across the refe	erence point S9 to the RCA	

TP ld	SECPKI_AA_CACERTGEN_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
Kelerence	ETSI TS 103 097 [2], clause 7
Configuration	CFG_CAGEN_INIT
PICS Selection	
	Expected behaviour
with	
the IUT being in the	'initial' state
ensure that	
when	
the IUT is reques	ted to send a CACertificateRequestMessage
then	
the IUT sends a	CACertificateRequestMessage
containing a sig	
	ted using a ETSI TS 103 097 [2] approved hash algorithm
and the IUT expo	orts the digital fingerprint (SIG) in a printable format.
-	

TP ld	SECPKI_AA_CACERTGEN_03_BV
Summary	The hashId shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [2], the signer is set to 'self' and the signature over the tbsData is computed using the private key corresponding to the new verificationKey to be certified (i.e. the request is self-signed).
Reference	ETSI TS 102 941 [1], clause 6.2.1 ETSI TS 103 097 [2], clause 7
Configuration	CFG_CAGEN_INIT
PICS Selection	
	Expected behaviour
then the IUT sends a CACe being an EtsiTs1030 containing hashld indicating the ha and containing sig indicating 'self' and containing tbs containing CaCe containing pub containing ve and containing ve	send a CACertificateRequestMessage rtificateRequestMessage 197Data-Signed structure sh algorithm to be used ner Data utificateRequest licKeys erification_key (VKEY)

TP ld	SECPKI_AA_CACERTGEN_04_BV
Summary	An ECC private key is randomly generated, the corresponding public key (verificationKey) is provided to be included in the CaCertificateRequest. An ECC encryption private key is randomly generated, the corresponding public key (encryptionKey) is provided to be included in the CACertificateRequest.
	CaCertificateRequest.publicKeys shall contain verification_key and encryption_key.
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_INIT
PICS Selection	
	Expected behaviour
with the IUT being in the ensure that when	e 'initial' state
	sted to send a CACertificateRequestMessage
then	
containing Ca	CACertificateRequestMessage CertificateRequest

containing publicKeys containing verification_key and containing encryption_key

	-
TP ld	SECPKI_AA_CACERTGEN_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 'init	ial' state
ensure that	
when	
the IUT is requested	to send a CACertificateRequestMessage
then	
the IUT sends a CAC	ertificateRequestMessage
containing EtsiTs1	02941Data
containing versio	n
indicating v1 (ir	nteger value set to 1)

TP ld	SECPKI_AA_CACERTGEN_06_BV
Summary	CaCertificateRequest.requestedSubjectAttributes shall contain the requested certificates
Summary	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 the	'initial' state
ensure that	
when	
the IUT is reques	ted to send a CACertificateRequestMessage
then	
the IUT sends a	CACertificateRequestMessage
containing Ca	CertificateRequest
containing re	questedSubjectAttributes
as specifie	d in ETSI TS 103 097 [2] clause 7.2.4.

TP ld	SECPKI_AA_CACERTGEN_07_BV
Summary	EtsiTs103097Data-Signed.tbsData contains the EtsiTs102941Data as payload and the headerInfo containing psid and generationTime. The psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [i.2] and the generationTime shall be present. All other components of the component tbsdata.headerInfo are not used and absent.
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_INIT
PICS Selection	
	Expected behaviour
with the IUT being in th ensure that when	e 'initial' state
	sted to send a CACertificateRequestMessage
containing he containing	

indicating SEC_CERT_REQ and containing generationTime and not containing any other component of tbsdata.headerInfo

TP ld	SECPKI_AA_CACERTGEN_08_BV
0	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	operational' state
ensure that	
when	
the IUT is reques	sted to send a CACertificateRekeyingMessage
and SubCA certil	ficate is no longer valid (due to end of validity or revocation)
then	
the IUT switches	to the "initial" state
and sends a CA0	CertificateReguestMessage

TP ld	SECPKI_AA_CACERTGEN_09_BV
Summary	For the re-keying application to the RCA (CaCertificateRekeyingMessage), an EtsiTs103097Data-Signed structure is built, containing: hashId, tbsData, signer and signature. The hashId shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [2]. The signer declared as a digest, containing the hashedId8 AA certificate and the signature over tbsData is computed using the currently valid private key corresponding to the AA certificate (outer signature).
Reference	ETSI TS 102 941 [1], clause 6.2.1 ETSI TS 103 097 [2], clause 7
Configuration	CFG_CAGEN_REKEY
PICS Selection	
	Expected behaviour
then the sends a CAC being an EtsiTs containing has indicating th and containing and containing declared as	ted to send a CACertificateRekeyingMessage ertificateRekeyingMessage s103097Data-Signed structure shId e hash algorithm to be used g tbsData g signer digest the hashedId8 of the SubCA certificate (CERT) g signature
	private key corresponding to CERT

TP ld	SECPKI_AA_CACERTGEN_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	
ensure that when the IUT is reque then the sends a CAC containing tbsl	e 'operational' state sted to send a CACertificateRekeyingMessage CertificateRekeyingMessage Data aCertificateRequestMessage

TP ld	SECPKI_AA_CACERTGEN_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	d to send a CACertificateRekeyingMessage tificateRekeyingMessage

containing headerInfo containing psid indicating SEC_CERT_REQ and containing generationTime and not containing any other component of tbsdata.headerInfo

TP ld	SECPKI_AA_CACERTGEN_12_BV
Summary	Check that the CaCertificateRekeyingMessage is permitted by AA certificate.
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_REKEY
PICS Selection	
	Expected behaviour
with	
the IUT being in the	operational' state
ensure that	
when	
	ed to send a CACertificateRekeyingMessage
then	
	rtificateRekeyingMessage
	103097Data-Signed structure
and containing	
and containin	
containing di	
	lashedId8 of the AA certificate g appPermissions
	ing an item of type PsidSsp
	ining psid
	cating AID_CERT_REQ
	ontaining ssp
	taining opaque[0] (version)
	dicating 1
	taining opaque[1] (value)
	dicating 'CA Certificate Response' (bit 6) set to 1

5.5 RootCA behaviour

5.5.1 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.

65

TP ld	SECPKI_RCA_CTLGEN_01_BV
C	Check that the RootCA generates the Full CTL when new EA is about to be added to the
Summary	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 tr	iggered to add new EA certificate (CERT_EA) in the CTL
then	
the IUT issue a	new CTL of type CtlFormat
containing isF	
indicating T	
and containing	g ctlCommands
containing	CtlCommand
containir	ig add
contai	ning ea
	taining eaCertificate
•	ndicating CERT_EA

TP ld	SECPKI_RCA_CTLGEN_02_BV
Summery	Check that the RootCA generates the Delta CTL when new EA is about to be added to the
Summary	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	d to add new EA certificate (CERT_EA) in the CTL
then	
the IUT issue a new C	TL of type CtlFormat
containing isFullCtl	
indicating FALSE	
and containing ctlCc	
containing CtlCon	
containing add	
containing ea	
	eaCertificate
indicatir	ng CERT_EA

TP ld	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
then the IUT issue a new C ⁻ containing isFullCtl indicating TRUE and containing ctlCo not containing Ctl containing add containing ea containing ea	ommands Command

TP ld	SECPKI_RCA_CTLGEN_04_BV
Cummon 4	Check that the RootCA generates the Delta CTL when EA certificate is about to be
Summary	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 trigge	ered to delete EA certificate (CERT_EA) from the CTL
then	
the IUT issue a new	CTL of type CtlFormat
containing isFullC	
indicating FAL	SE
and containing ct	
not containing	CtlCommand
containing d	elete
containing	g cert
indicati	ng Hashedid8 of CERT_EA

TD L	
TP ld	SECPKI_RCA_CTLGEN_05_BV
Summary	Check that the RootCA generates the Full CTL when EA access point 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 triggere	d to add new EA access point URL (URL) to the CTL
then	
the IUT issue a new C	TL of type CtlFormat
containing isFullCtl	
indicating TRUE	
containing ctlComm	ands
containing CtlCor	
containing add	
containing e	a
	g eaCertificate (CERT_EA)
	ining itsAccessPoint
indicati	
	ing any other CtlCommand
containing add	
containing e	
	g eaCertificate
indicati	ng CERT_EA

TP ld	SECPKI_RCA_CTLGEN_06_BV
Summary	Check that the RootCA generates the Delta CTL when EA access point is about to be
	changed.
Reference	ETSI TS 102 941 [1], clauses 6.3.2 and 6.3.4
Configuration	CFG_CTLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	
when	
the RootCA is triggered	d to add new EA access point URL (URL) to the CTL
then	
the IUT issue a new C	TL of type CtlFormat
containing isFullCtl	
indicating FALSE	
containing ctlComm	
containing CtlCon	nmand
containing add	
containing ea	
	eaCertificate (CERT_EA)
	ining itsAccessPoint
indicatir	IG UKL
TP Id	SECPKI_RCA_CTLGEN_07_BV
	Check that the RootCA generates the Full CTL when EA access point URL for AA
Summary	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	
-	d to add new URL for EA-AA communication (URL) to the CTL
then	
the IUT issue a new C	TL of type CtlFormat
containing isFullCtl	
indicating TRUE	
containing ctlComm	ands
containing CtlCon	
containing add	
containing ea	
	eaCertificate (CERT_EA)
	aaAccessPoint
indicatir	
	ng any other CtlCommand
containing add	
containing ea	
	eaCertificate
indicatir	ng CERT_EA

TP ld	SECPKI_RCA_CTLGEN_08_BV
Cummon.	Check that the RootCA generates the Delta CTL when EA access point URL for AA
Summary	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	ered to add new URL for EA-AA communication (URL) to the CTL
then	
the IUT issue a new	w CTL of type CtlFormat
containing isFull	Ctl
indicating FAL	_SE
containing ctlCo	mmands
containing Ctl	Command
containing	
containir	iq ea
contai	ning eaCertificate (CERT_EA)
	ning aaAccessPoint
	cating URL

TP ld	SECPKI RCA CTLGEN 09 BV
0	Check that the RootCA generates the Full CTL when new AA is about to be added to the
Summary	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 trig	gered to add new AA certificate (CERT_AA) in the CTL
then	
the IUT issue a n	ew CTL of type CtlFormat
containing isFu	illCtl
indicating T	
and containing	ctlCommands
containing C	tlCommand
containing	add
contain	ing aa
conta	aining aaCertificate
in	dicating CERT_AA

TP ld	SECPKI_RCA_CTLGEN_10_BV
C	Check that the RootCA generates the Delta CTL when new AA is about to be added to the
Summary	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 trig	gered to add new AA certificate (CERT_AA) in the CTL
then	
	ew CTL of type CtlFormat
containing isF	
indicating F	
	ctlCommands
•	CtlCommand
containin	
contair	5
	aining aaCertificate
in	dicating CERT_AA

TP ld	SECPKI_RCA_CTLGEN_11_BV
	Check that the RootCA generates the Full CTL when AA is about to be deleted from the
Summary	Root CTL.
Reference	ETSI TS 102 941 [1], clause 6.3.2
Configuration	CFG_CTLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	
when	
the RootCA	is triggered to delete AA certificate (CERT_AA) from the CTL
then	
the IUT issue	e a new CTL of type CtlFormat
containing	isFullCtl
	ng TRUE
	ining ctlCommands
	taining CtlCommand
	aining add
	ntaining aa
	containing aaCertificate
	indicating CERT AA
TP ld	SECPKI_RCA_CTLGEN_12_BV

I P Id	SECPKI_RCA_CTLGEN_12_BV
Summary	Check that the RootCA generates the Delta CTL when AA is about to be deleted from the
	Root CTL.
Reference	ETSI TS 102 941 [1], clauses 6.3.2 and 6.3.4
Configuration	CFG_CTLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	
when	
the RootCA is tr	iggered to delete AA certificate (CERT_AA) from the CTL
then	
the IUT issue a	new CTL of type CtlFormat
containing isF	FullCtl
indicating F	ALSE
and containin	g ctlCommands
not contain	ing CtlCommand
containir	ng delete
contai	ning cert
indicating HashedId8 of CERT_AA	

TP ld	SECPKI_RCA_CTLGEN_13_BV
Summary	Check that the RootCA generates the Full CTL when AA access point URL is about to be
	changes.
Reference	ETSI TS 102 941 [1], clause 6.3.2
Configuration	CFG_CTLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	·
when	
the RootCA is trig	gered to add new URL for AA access point (URL) to the CTL
then	
the IUT issue a ne	ew CTL of type CtlFormat
containing isFu	
indicating TF	
containing ctIC	
containing C	
containing	
contain	
	aining aaCertificate
	aining accessPoint
	dicating URL
	ntaining any other CtlCommand
containing	
contain	
	aining aaCertificate
inc	dicating CERT_AA
TP ld	SECPKI_RCA_CTLGEN_14_BV
	Check that the RootCA generates the Delta CTL when AA access point LIRL is about to be

	SECPKI_RCA_CILGEN_14_BV
Summary	Check that the RootCA generates the Delta CTL when AA access point URL is about to be
	changes.
Reference	ETSI TS 102 941 [1], clause 6.3.2
Configuration	CFG_CTLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	·
when	
the RootCA is tr	iggered to add new URL for AA access point (URL) to the CTL
then	
the ILIT issue a	
	new CTL of type CtlFormat
containing isF	
	FullCtl
containing isF indicating T	FullCtl TRUE
containing isF indicating T containing ctl	FullCtl TRUE
containing isF indicating T containing ctl	TullCtl TRUE Commands CtlCommand
containing isF indicating T containing ctl containing containing	TullCtl TRUE Commands CtlCommand
containing isF indicating T containing ctl containing containin containir	FullCtl TRUE Commands CtlCommand ng add
containing isF indicating T containing ctl containing containir contai contai	FullCtl TRUE Commands CtlCommand ng add ning aa

TP ld	SECPKI_RCA_CTLGEN_15_BV
	Check that the RootCA CTL is signed using RootCA verification key
Summary	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 issue	ed the TLM CTL list
containing RootCA	certificate (CERT_RCA)
ensure that	
when	
	ered to issue a new CTL
then	
	v CTL of type RcaCertificateTrustListMessage
containing signed	
containing signer.digest	
	ashedID8 of the RootCA certificate (CERT_RCA)
	appPermissions
	ng an item of type PsidSsp
	ating AID_CTL
	ontaining ssp
	aining opaque[0] (version) licating 1
	8
containing opaque[1] (value) indicating 'TLM entries' (bit 0) set to 0	
indicating 'RCA entries' (bit 1) set to 0	
	licating 'EA entries' (bit 2) set to 1
	licating 'AA entries' (bit 3) set to 1
	licating 'DC entries' (bit 4) set to 1
	3097Data and EtsiTs102941Data envelopes are not yet removed from the analysing message.

TP ld	SECPKI_RCA_CTLGEN_16_BV
Summary	Check that the RCA CTL sequence counter is monotonically increased.
Reference	ETSI TS 102 941 [1], clause 6.3.2
Configuration	CFG_CTLGEN_RCA
PICS Selection	
Expected behaviour	
with the RCA already has issued the previous CTL of type CtlFormat containing ctlSequence indicating N ensure that when the RCA is triggered to issue a new CTL then the IUT issue a new CTL of type CtlFormat containing ctlSequence indicating N+1	

TP ld	SECPKI_RCA_CTLGEN_17_BV	
Summary	Check that the RCA CTL sequence counter is rounded on the value of 256.	
Reference	ETSI TS 102 941 [1], clause 6.3.2	
Configuration	CFG_CTLGEN_RCA	
PICS Selection		
Expected behaviour		
containing ct/Sequenc indicating 255 ensure that when the RCA is triggered to then the IUT issue a new C	ensure that when the RCA is triggered to issue a new CTL then the IUT issue a new CTL of type CtlFormat containing ctlSequence	

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

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

TP ld	SECPKI_RCA_CTLGEN_20_BV	
•	Check that the RCA Delta CTL is generated at the same time as FullCTL.	
Summary	Check that the RCA Delta CTL is a difference between correspondent Full CTL and the	
	previous Full CTL.	
Reference	ETSI TS 102 941 [1], clause 6.3.2	
Configuration	CFG_CTLGEN_RCA	
PICS Selection		
	Expected behaviour	
with		
the RCA already issued t	the previous CTL of type CtlFormat (CTL_FULL_PREV)	
containing isFullCtl		
indicating TRUE		
containing ctlSequenc	e	
indicating N		
ensure that		
when		
the RCA is triggered to	o issue a new CTL	
then		
the IUT issue a new C	TL of type CtlFormat (CTL_FULL)	
containing isFullCtl		
indicating TRUE		
and containing ctISe	equence	
indicating N+1		
and the IUT issue a new CTL of type CtlFormat (CTL_DELTA)		
containing isFullCtl		
indicating FALSE		
and containing ctlSequence		
indicating N+1		
containing ctlComm	containing ctlCommands	
indicating difference between CTL_FULL and CTL_FULL_PREV		

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

TP ld	SECPKI_RCA_CTLGEN_22_BV
Summary	Check that the RCA Full CTL does not contain commands of type 'delete'.
Reference	ETSI TS 102 941 [1], clause 6.3.2
Configuration	CFG_CTLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT is trigge	red to delete the CA from the CTL
then	
the IUT issue a	new CTL of type CtlFormat (CTL_FULL)
containing isF	
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 to	issue a new CTL	
then	then	
the IUT issue a new C	the IUT issue a new CTL of type CtlFormat	
containing isFullCtl	containing isFullCtl	
indicating TRUE		
and containing ctlCo	and containing ctlCommands	
containing at least one ctlCommand		
containing add		
containing url		
indicating URL of the DC of the IUT		
containing cert		
containing the item of type HashedId8		
indicating the HashedId8 of the IUT certificate		

5.5.2 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
then the IUT generates the containing signer containing digest indicating Hashe containing ap containing a containing indicatin and conta	n item of type PsidSsp j psid g AID_CRL
indicat	
NOTE: The EtsiTs10309	7Data and EtsiTs102941Data envelopes are not yet removed from the analysing message

TP ld	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 iter	containing item of type OrlEntry	

containing item of type CrlEntry indicating HashID8 of the CERT_CA

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 th containing the RCA ce		
ensure that		
when	when	
the RootCA is triggered to revoke itself		
then		
the IUT issue a new CRL of type ToBeSignedCrl containing entries		

containing item of type CrlEntry indicating HashID8 of the CERT_RCA

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

TP Id	SECPKI_RCA_CRLGEN_05_BV	
Summary	Check that the RCA issuing a new CRL when previous one is expired	
Reference	ETSI TS 102 941 [1], clause 6.3.3	
Configuration	CFG_CRLGEN_RCA	
PICS Selection		
	Expected behaviour	
with		
the RCA already iss	ued the CRL	
containing nextU	odate	
indicating time	indicating time Tprev	
ensure that	ensure that	
when	when	
the Tprev is less	the Tprev is less than current time (Tcur)	
then	then	
the IUT issue 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 ld	SECPKI_RCA_CRLGEN_06_BV	
Summers	Check that the RootCA is generated the CRL when its own certificate is about to be	
Summary	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	the RootCA is triggered to issue a new CRL	
then	then	
the IUT issue a n	the IUT issue a new CRL of type ToBeSignedCrl	
and containing entries		
does not containing item of type CrlEntry		
indicating HashID8 of other RootCA		

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

TP ld	SECPKI_RCA_CRLGEN_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	ensure that		
when	when		
the RCA is triggered to	the RCA is triggered to issue a new CRL		
then			
the IUT issue a new CRL of type ToBeSignedCrl			
containing version			
indicating 1			

TP ld	SECPKI_RCA_CAGEN_01_BV	
Summary	Check that generated EA certificate contains only allowed permissions	
Reference		
	ETSI TS 102 941 [1], clause B.5	
Configuration	CFG_CAGEN_RCA	
PICS Selection		
	Expected behaviour	
ensure that		
when		
	generate EA certificate	
then		
the IUT generate the c		
containing appPerm		
containing an item containing psid		
	D_CERT_REQ	
and containing		
	ssp paque[0] (version)	
indicating		
	baque[1] (value)	
	'Authorization validation Response' (bit 4) set to 1	
	and indicating 'Enrolment Response' (bit 5) set to 1 and indicating 'CA certificate request' (bit 6) set to 1	
	ting 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 certIssue		
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 ld	SECPKI_RCA_CAGEN_02_BV		
Summary Check that generated AA certificate contains only allowed permissions			
Reference ETSI TS 102 941 [1], clause B.5			
	CFG_CAGEN_RCA		
Configuration PICS Selection			
	Expected behaviour		
ongure that	Expected benaviour		
ensure that when			
_	o generate AA certificate		
then	yenerale AA certificate		
the IUT generate the c	retificate		
containing appPerm			
	n of type PsidSsp		
containing psic			
	D_CERT_REQ		
and containing			
containing o	paque[0] (version)		
indicating			
containing o	paque[1] (value)		
indicating	'Authorization validation Request (bit 2) set to 1		
	ating 'Authorization Response' (bit 3) set to 1		
	ating 'CA certificate request' (bit 6) set to 1		
	ating other bits set to 0		
	ing an item of type PsidSsp		
• •	containing psid		
indicating AI			
	and NOT containing an item of type PsidSsp		
containing psid			
indicating AID_CRL			
containing certIssuePermissions			
containing an item of type PsidGroupPermissions containing eeType			
indicating ap			
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		
	ntaining sspRange		
containing bitmapSspRange			
containing sspBitmask			
indicating FFh			
containing sspValue			
indicating 01h 00h			
and NOT containing an item of type PsidSspRange			
containing psid			
indicating AID_CTL and NOT containing an item of type PsidSsp			
containing psid			
indicating AID_CRL			
Indic			

TP ld	SECPKI_RCA_CAGEN_03_BV	
Summary	Check that generated RootCA certificate contains only allowed permissions	
Reference	ETSI TS 102 941 [1], clause B.5	
Configuration	CFG_CAGEN_RCA	
PICS Selection		
FICS Selection	Expected behaviour	
ensure that		
when		
	o generate AA certificate	
then	<u> </u>	
the IUT generate the c	ertificate	
containing appPerm	issions	
NOT containing a	n item of type PsidSsp	
containing psid		
	D_CERT_REQ	
	n item of type PsidSsp	
containing psid		
indicating AI		
and containing		
indicating		
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		
	n of type PsidGroupPermissions	
containing eeT		
indicating app		
containing subj	ectPermissions	
containing ex		
	gen item of type PsidSspRange	
	containing psid	
	ating AID_CERT_REQ	
	ntaining sspRange	
	aining 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	
	ating AID_CTL	
	containing an item of type PsidSsp	
containing psid		
indica	indicating AID_CRL	

5.6 DC behaviour

TP ld	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	with	
the TLM issued a new CRL		
ensure that		
when		
the ITS-S asked 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 CTL ensure that when the ITS-S asked the IUT for the newly issued CTL then the IUT is answered with this CTL			

5.7 TLM behaviour

5.7.1 CTL generation

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

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

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

TP ld	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	the TLM is triggered to delete RootCA certificate (CERT_RCA) from the CTL		
then	then		
the IUT issue a new C	TL of type CtlFormat		
containing isFullCtl			
indicating FALSE			
and containing ctlCommands			
containing CtlCommand			
containing delete			
containing cert			
indicating HashedId8 of CERT_RCA			

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

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

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

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

TP Id	SECPKI_TLM_ECTLGEN_09_BV		
	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			
the TLM is triggered to	o issue a new CTL		
then			
the IUT issue a new C	TL of type TImCertificateTrustListMessage		
containing signedDa			
containing signer	•		
indicating HashedID8 of the TLM certificate (TLM_CERT)			
	ppPermissions		
containing an item of type PsidSsp			
	containing psid		
indicating AID_CTL			
and containing ssp			
containing opaque[0] (version)			
indicating 1 containing opaque[1] (value)			
indicating 'TLM entries' (bit 0) set to 1			
indicating 'RCA entries' (bit 1) set to 1 indicating 'EA entries' (bit 2) set to 0			
indicating 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.certificateTrustListTIm			
containing ctlCommands			
containing add			
cc	containing tIm		
	containing selfSignedTLMCertificate		
<u> </u>	indicating TLM_CERT		
NOTE: The EtsiTs10309	97Data 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 issued the previous CTL of type CtlFormat containing ctlSequence indicating N ensure that when the TLM is triggered to issue a new CTL then the IUT issue a new CTL of type CtlFormat containing ctlSequence indicating N+1	

TP ld	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			
containing ctlSequence indicating 255	ed the previous CTL of type CtlFormat e		
ensure that			
when			
the TLM is triggered to issue a new CTL			
then			
the IUT issue a new CTL of type CtlFormat			
containing ctlSequence			
indicating 0	indicating 0		

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

TP ld	SECPKI_TLM_ECTLGEN_13_BV	
Summary	Check that the TLM CTL does not have other entries then allowed	
Reference	ETSI TS 102 941 [1], clause 6.3.1	
Configuration	CFG_CTLGEN_TLM	
PICS Selection		
	Expected behaviour	
ensure that when the TLM is triggered to then the IUT issue a new C containing ctlComm not containing an containing add containing ea or containing	TL of type CtlFormat ands y item of type CtlCommand a	

TP Id 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 iss	ued the previous CTL of type CtlFormat (CTL_FULL_PREV)		
containing isFullC			
indicating TRU			
containing ctlSeq	uence		
indicating N			
ensure that			
when			
	red to issue a new CTL		
then			
	ew CTL of type CtlFormat (CTL_FULL)		
containing isFu			
indicating TF			
	and containing ctlSequence		
indicating N-			
	e a new CTL of type CtlFormat (CTL_DELTA)		
containing isFu			
indicating FALSE			
and containing ctlSequence			
indicating N+1			
containing ctlCommands			
indicating di	fference 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 trigger	the IUT is triggered to issue a new CTL			
then				
the IUT issue a new CTL of type CtlFormat				
containing version				
indicating 1				

TP ld	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 triggere	the IUT is triggered to delete the CA from the CTL		
then	then		
the IUT issue a n	ew CTL of type CtlFormat		
containing isFu	ullCtl		
indicating TRUE			
and containing ctlCommands			
NOT containing any item of type CtlCommand			
containing delete			

5.8 CPOC behaviour

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

87

History

	Document history		
V1.1.1	March 2019	Publication	

88