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



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

Reference

RTS/ITS-00598

Keywords

ITS, security, testing, TSS&TP

ETSI

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

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

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

Important notice

The present document can be downloaded from the ETSI <u>Search & Browse Standards</u> application.

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

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

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

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

Notice of disclaimer & limitation of liability

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

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

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

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

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

Copyright Notification

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 2024. All rights reserved.

Contents

Intelle	ectual Property Rights	5		
Forew	Foreword5			
Moda	l verbs terminology	5		
1	Scope	6		
2	References	6		
2.1	Normative references			
2.2	Informative references			
3	Definition of terms, symbols and abbreviations	7		
3.1	Terms			
3.2	Symbols			
3.3	Abbreviations			
4	Test Suite Structure (TSS)	9		
4.1	Structure for Security tests			
4.2	Test entities and states			
4.2.1	ITS-S states			
4.2.2	EA states	10		
4.2.3	AA states			
4.2.4	RootCA states			
4.2.5	TLM states			
4.3	Test configurations			
4.3.1	Overview			
4.3.2	Enrollment			
4.3.2.1				
4.3.3	Authorization			
4.3.3.1				
4.3.3.2				
4.3.4	Authorization Validation			
4.3.4.1				
4.3.4.2				
4.3.5	Authorization using butterfly key expansion mechanism			
4.3.5.1				
4.3.5.2	Configuration CFG_BFK_AUTH_EA	13		
4.3.5.3	e = = =			
4.3.6	CA certificate generation			
4.3.6.1	∂			
4.3.6.2				
4.3.6.3				
4.3.7	ECTL generation	13		
4.3.7.2				
4.3.7.2	Root CTL generation			
4.3.8.1	•			
4.3.9	CRL generation.			
4.3.9.1				
4.3.10				
4.3.10				
5	Test Purposes (TP)			
5.1	Introduction			
5.1.1	TP definition conventions			
5.1.2	TP Identifier naming conventions			
5.1.3	Rules for the behaviour description			
5.1.4	Sources of TP definitions			
5.1.5	Mnemonics for PICS reference	15		
5.1.6	Certificates content	16		

5.2	ITS-S behaviour	
5.2.0	Overview	
5.2.1	Manufacturing	
5.2.2	Enrolment	
5.2.2.0	Overview	
5.2.2.1	Enrolment request	
5.2.2.2	Enrolment response handling	
5.2.2.3	Enrolment request repetition	
5.2.3	Authorization	
5.2.3.0	Overview	
5.2.3.1	Authorization request	
5.2.3.2	Authorization response handling	
5.2.3.3	Authorization request repetition	
5.2.3.4	Authorization using butterfly key expansion mechanism	
5.2.3.4.1	Overview	
5.2.3.4.2	Butterfly authorization request	
5.2.3.4.3	Butterfly AT download request	
5.2.4	CTL handling	
5.2.5	CTL distribution	
5.2.6	CRL handling	
5.2.7	CRL distribution	
5.3	Common CA behaviour	
5.3.0	Overview	
5.3.1	Certificate validation	
5.3.1.1	Basic certificate content	
5.3.1.2	Check certificate region validity restriction	
5.3.1.3	Check ECC point type of the certificate signature	
5.3.1.4	Check ECC point type of the certificate public keys	
5.3.1.5	Verify certificate signatures	
5.3.1.6	Verify certificate permissions	
5.3.1.7	Check time validity restriction in the chain	
5.4	EA behaviour	
5.4.0	Overview	
5.4.1	Enrolment request handling	
5.4.2	Enrolment response	
5.4.3	Authorization validation request handling	
5.4.4	Authorization validation response	
5.4.5	CA Certificate Request	
5.4.6	Authorization using butterfly key expansion mechanism	
5.4.6.1	Butterfly authorization response	
5.4.6.2	Butterfly certificate request	
5.4.6.3	Authorization certificate download	
5.5	AA behaviour	
5.5.0	Overview	
5.5.1 5.5.2	Authorization request handling	
5.5.2	Authorization validation request Authorization validation response handling	
5.5.4	Authorization response	
5.5.5	CA Certificate Request	
5.5.6	Authorization using butterfly key expansion mechanism	
5.5.6.1	Butterfly certificate response	
5.6	RootCA behaviour	
5.6.0	Overview	
5.6.1	CTL generation	
5.6.2	CRL generation	
5.6.3	CA certificate generation	
5.7	DC behaviour	
5.8	TLM behaviour	
5.8.1	CTL generation	
5.9	CPOC behaviour	
History		

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

DECTTM, **PLUGTESTSTM**, **UMTSTM** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPPTM** and **LTETM** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2MTM** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**[®] and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

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

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

Modal verbs terminology

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

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

1 Scope

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

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

2 References

2.1 Normative references

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

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

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

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

- [1] <u>ETSI TS 102 941 (V2.2.1)</u>: "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2".
- [2] <u>ETSI TS 103 097 (V2.1.1)</u>: "Intelligent Transport Systems (ITS); Security; Security header and certificate formats; Release 2".
- [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: "IEEE Standard for Wireless Access In Vehicular Environments - Security Services for Applications and Management Messages - Amendment 1".
- [4] <u>ETSI TS 103 525-1 (V2.1.1)</u>: "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 1: Protocol Implementation Conformance Statement (PICS); Release 2".
- [5] <u>ETSI TS 103 096-2 (V2.1.1)</u>: "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 2: Test Suite Structure and Test Purposes (TSS & TP); Release 2".
- [6] <u>ETSI TS 103 601 (V2.1.1)</u>: "Intelligent Transport Systems (ITS); Security; Security management messages communication requirements and distribution protocols; Release 2".
- [7] <u>European Commission</u>: "Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)" Release 1.1, June 2018.
- [8] <u>ETSI TS 102 965 (V2.2.1)</u>: "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration; Release 2".

2.2 Informative references

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

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

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

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

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 102 941 [1], ETSI TS 103 097 [2], ETSI TS 103 525-1 [4], ETSI TS 102 965 [8], ISO/IEC 9646-6 [i.5], ISO/IEC 9646-7 [i.6] and the following apply:

AID_CERT_REQ: "Secured certificate request service" ITS-AID

AID_CRL: "CRL service" ITS-AID

AID_CTL: "CTL service" ITS-AID

3.2 Symbols

Void.

3.3 Abbreviations

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

AA	Authorization Authority
AES	Advanced Encryption Standard
AID	Application IDentifier

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

4 Test Suite Structure (TSS)

4.1 Structure for Security tests

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

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

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 the following information elements:
 - Permanent Canonical Identifier (PCI);
 - public/private key pair for cryptographic purposes (canonical key pair);
 - the trust anchor (Root CA) public key certificate and the DC network address;
 - contact information for the EA which will issue certificates for the ITS-S:
 - network address;
 - public key certificate.

- State 'enrolled':
 - ITS-S in 'enrolled' state has successfully performed the enrolment request process.
 - ITS-S in 'enrolled' state is ready to perform an authorization request.
 - ITS-S in 'enrolled' state contains all information elements of the 'initialized' state and additionally:
 - Enrolment Credential (EC) with the condition of being neither expired nor revoked;
 - private key corresponding to the EC public encryption key;
 - private key corresponding to the EC public verification key.
- State 'authorized':
 - ITS-S in 'authorized' state has successfully performed the authorization request process.
 - ITS-S in 'authorized' state contains all information elements of the 'enrolled' state and additionally:
 - one or more Authorization Tickets (AT):
 - being not expired;
 - of which at least one is currently valid;
 - all private keys corresponding to the AT public verification keys;
 - if applicable: all private keys corresponding to the AT public encryption keys.

4.2.2 EA states

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

4.2.3 AA states

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

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

4.2.5 TLM states

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

4.3 Test configurations

4.3.1 Overview

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

4.3.2 Enrollment

4.3.2.1 Configuration CFG_ENR_ITS-S

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

- IUT is configured to be directly entitled to the initial enrolment, as specified in ETSI TS 102 941 [1], clause 6.1.3.0.
- Following information elements shall be provided by IUT for the EA emulated by the TS:
 - Permanent Canonical Identifier (PCI);
 - public key of canonical key pair;
 - profile information.
- TS: EA is emulated by TS.

4.3.2.2 Configuration CFG_ENR_EA

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

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

TS: ITS-S is emulated by the TS.

4.3.3 Authorization

4.3.3.1 Configuration CFG_AUTH_ITS-S

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

- the AA certificate of the emulated AA;
- the EA certificate of the emulated EA;

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

4.3.3.2 Configuration CFG_AUTH_AA

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

• the profile information for the emulated ITS-S.

TS: ITS-S is emulated by the TS:

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

4.3.4 Authorization Validation

4.3.4.1 Configuration CFG_AVALID_AA

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

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

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

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

4.3.4.2 Configuration CFG_AVALID_EA

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

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

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

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

4.3.5 Authorization using butterfly key expansion mechanism

4.3.5.1 Configuration CFG_BFK_AUTH_ITS-S

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

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

TS: AA and EA are emulated by the TS.

4.3.5.2 Configuration CFG_BFK_AUTH_EA

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

13

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

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

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

4.3.5.3 Configuration CFG_BFK_AUTH_AA

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

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

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

• the AA certificate of the IUT.

4.3.6 CA certificate generation

4.3.6.1 Configuration CFG_CAGEN_INIT

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

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

4.3.6.2 Configuration CFG_CAGEN_REKEY

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

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

4.3.6.3 Configuration CFG_CAGEN_RCA

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

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

4.3.7 ECTL generation

4.3.7.1 Configuration CFG_CTLGEN_TLM

IUT: TLM in the operational state.

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

4.3.7.2 Configuration CFG_CTLGEN_CPOC

IUT: CPOC in the operational state.

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

4.3.8 Root CTL generation

4.3.8.1 Configuration CFG_CTLGEN_RCA

IUT: RCA in the operational state.

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

4.3.9 CRL generation

4.3.9.1 Configuration CFG_CRLGEN_RCA

IUT: RCA in the operational state.

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

4.3.10 ITS-S CRL/CTL handling

4.3.10.1 Configuration CFG_CXL_P2P

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

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

Neighbour ITS-S: is emulated by the TS.

RCA: is emulated by the TS.

DC: is emulated by the TS.

5 Test Purposes (TP)

5.1 Introduction

5.1.1 TP definition conventions

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

5.1.2 TP Identifier naming conventions

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

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

Table 2: TP naming convention

5.1.3 Rules for the behaviour description

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

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

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

5.1.4 Sources of TP definitions

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

5.1.5 Mnemonics for PICS reference

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

Mnemonic	PICS item
PICS_SECPKI_IUT_ITS-S	[4] A.2.1
PICS_SECPKI_IUT_EA	[4] A.3.2
PICS_SECPKI_IUT_AA	[4] A.3.3
PICS_SECPKI_IUT_RCA	[4] A.3.4
PICS_SECPKI_IUT_DC	[4] A.3.5
PICS_SECPKI_IUT_TLM	[4] A.3.6
PICS_SECPKI_IUT_CPOC	[4] A.3.7
PICS_SECPKI_ENROLLMENT	[4] A.2.2 or A.4.1
PICS_SECPKI_ENROLLMENT_RETRY	[4] A.2.2.2 or A.4.4
PICS_SECPKI_ENROLLMENT_X509	[4] A.2.2 and A.1.7
PICS_SECPKI_REENROLLMENT	[4] A.2.2.1 or A.4.2
PICS_SECPKI_AUTHORIZATION	[4] A.2.3 or A.5.1
PICS_SECPKI_ AUTHORIZATION _RETRY	[4] A.2.3.3 or A.5.5
PICS_SECPKI_AUTH_PRIVACY	[4] A.2.3.1 or A.5.3
PICS_SECPKI_AUTH_POP	[4] A.2.3.2 or A.5.2
PICS_SECPKI_AUTH_VALIDATION	[4] A.4.3
PICS_SECPKI_AUTH_BFK	[4] A.5.6
PICS_SECPKI_CRL	[4] A.8.5 or A.6.1
PICS_SECPKI_CRL_DOWNLOAD	[4] A.8.6
PICS_SECPKI_CRL_BROADCAST	[4] A.8.9
PICS_SECPKI_CTL	[4] A.8.3 or A.6.2
PICS_SECPKI_CTL_DELTA	[4] A.8.3.1 or A.6.2.1 or A.6.4.1
PICS_SECPKI_CTL_DOWNLOAD	[4] A.8.4
PICS_SECPKI_CTL_BROADCAST	[4] A.8.8
PICS_SECPKI_ECTL	[4] A.8.1 or A.7.1
PICS_SECPKI_ECTL_DELTA	[4] A.8.1.1 or A.7.1.1 or A.7.2.1
PICS_SECPKI_ECTL_DOWNLOAD	[4] A.8.2 or A.7.3
PICS_SECPKI_ECTL_BROADCAST	[4] A.8.7
PICS_SEC_SHA256	[3] S1.2.2.1.1 or S1.3.2.1.1
PICS_SEC_SHA384	[3] \$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
PICS_SEC_IMPLICIT_CERTIFICATES	[3] S1.2.2.8, S1.3.2.7 and S1.3.2.9
PICS_SEC_EXPLICIT_CERTIFICATES	[3] S1.2.2.7, S1.3.2.6 and S1.3.2.8

Table 3: Mnemonics for PICS reference

5.1.6 Certificates content

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

Table 4: Certificates conte	ent
-----------------------------	-----

AA certificate	Content	To be installed on the IUT
CERT_IUT_A_EA	• signer digest of the CERT_IUT_A_CA;	Yes
	application permissions:	
	 CRT_REQ with SSP 0x0107; 	
	 certificate issuing permissions (SSP value/mask): 	
	 CRT_REQ with SSP 0x1C0; 	
	 validation time for 3 years; 	
	no region restriction;	
	assurance level 4;	
	 verification key of type compressed with NIST P256R curve; 	
	 encryption key of type compressed with NIST P256R curve; 	
	• valid signature of type x-only with NIST P256R curve;	
CERT_IUT_A_AA	signer digest of the CERT_IUT_A_CA;	Yes
	application permissions:	
	 CRT_REQ with SSP 0x0132; 	
	 certificate issuing permissions (SSP value/mask): 	
	 CAM with all possible SSP (0x01FFFC / 0xFF0003); 	
	 DENM with all possible SSP (0x01FFFFFF / 0xFF000000); 	
	 SPATEM with all possible SSP (0x01E0 / 0xFF1F); 	
	 MAPEM with all possible SSP (0x01C0 / 0xFF3F); 	
	 IVIM with all possible SSP (0x01000000FFF8 / 	
	0xFF000000007);	
	 SREM with all possible SSP (0x01FFFFE0 / 0xFF00001F); 	
	 SSEM with all possible SSP (0x01 / 0xFF); 	
	 – GPC with all possible SSP (0x01 / 0xFF); 	
	 – GN-MGMT without SSP; 	
	validation time for 3 years;	
	no region restriction;	
	assurance level 4;	
	 verification key of type compressed with NIST P256R curve; 	
	 encryption key of type compressed with NIST P256R curve; 	
	• valid signature of type x-only with NIST P256R curve;	
CERT_IUT_A_CA	• same as CERT_IUT_A_AA;	Yes
CERT_IUT_I_CA	• same as CERT_IUT_A_CA;	Yes
	type implicit;	
	not containing signature;	
	not containing verification key;	
	containing reconstruction value.	

5.2 ITS-S behaviour

5.2.0 Overview

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

PICS_SECPKI_IUT_ITS-S = TRUE

5.2.1 Manufacturing

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

5.2.2 Enrolment

5.2.2.0 Overview

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

PICS_SECPKI_ENROLMENT = TRUE

5.2.2.1 Enrolment request

TP ld	SECPKI_ITS-S_ENR_01_BV		
Summary			
Reference	ETSI TS 102 941 [1], clause 6.1.3		
Configuration	CFG_ENR_ITS-S		
PICS Selection			
	Expected behaviour		
with the IUT being in the 'initialized' state ensure that when the IUT is triggered to request a new Enrolment Credential (EC) certificate then the IUT sends to EA an EnrolmentRequestMessage			

TDL			
TP ld	SECPKI_ITS-S_ENR_02_BV		
	If the enrolment request of the IUT is an initial enrolment request, the itsld (contained in		
Summary	the InnerECRequest) shall be set to the canonical identifier, the signer (contained in the		
,	outer EtsiTs1030971Data-Signed) shall be set to self and the outer signature shall be		
	computed using the canonical private key		
Reference	ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1		
Configuration	CFG_ENR_ITS-S		
PICS Selection			
	Expected behaviour		
with			
the IUT being in the 'initi	alized' state		
ensure that			
when			
	to send an EnrolmentRequestMessage		
then			
	siTs103097Data-Encrypted		
	crypted EtsiTs103097Data-Signed		
containing Et	tsiTs102941Data		
	g enrolmentRequest		
conta	containing InnerEcRequest		
containing itsId			
indicating the canonical identifier of the ITS-S			
	and containing signer		
declared			
and containin			
computed using the canonical private key			

TP ld	SECPKI_ITS-S_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	(contained in the outer EtsiTs1030971Data-Signed) both declared as digest containing the		
	HashedId8 of the EC and the outer signature computed using the current valid EC private		
	key corresponding to the verification public key		
Reference	ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1		
Configuration	CFG_ENR_ITS-S		
PICS Selection	PICS_SECPKI_REENROLMENT		
	Expected behaviour		
with			
the IUT being enrolle	ed with certificate CERT_EC		
ensure that			
when			
the IUT is reques	sted to send an EnrolmentRequestMessage		
then			
the IUT sends an	n EtsiTs103097Data-Encrypted		
	containing an encrypted EtsiTs103097Data-Signed		
containing EtsiTs102941Data			
containing enrolmentRequest			
containing InnerEcRequest			
containing itsld			
declared as digest containing the HashedId8 of the CERT_EC			
and containing signer			
declared as digest containing the HashedId8 of the CERT_EC			
	and containing signature		
comp	computed using the private key corresponding to CERT_EC verification public key		

TP Id	SECPKI_ITS-S_ENR_05_BV	
Summary	If the EC expires, the IUT returns to the state 'initialized'	
Reference	ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1	
Configuration	CFG_ENR_ITS-S	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the 'enre	olled' state	
and the EC of the IUT ex	xpires	
ensure that	·	
when	when	
the IUT is requested	the IUT is requested to send an EnrolmentRequestMessage	
then		
	the IUT sends an EtsiTs103097Data-Encrypted	
containing an end	containing an encrypted EtsiTs103097Data-Signed	
containing EtsiTs102941Data		
containing enrolmentRequest		
	containing InnerEcRequest	
С	containing itsld	
	indicating the canonical identifier of the ITS-S	

TP Id	PId SECPKI_ITS-S_ENR_06_BV	
Summar	For each enrolment request, the ITS-S shall generate a new verification key pair corresponding to an approved signature algorithm as specified in ETSI TS 103 097 [2]	
Referen	ETSI TS 102 941 [1], clause 6.2.3.2.1 ETSI TS 103 097 [2], clause 7	
Configu	ion CFG_ENR_ITS-S	
PICS Se	tion 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:	he first EnrolmentRequestMessage should be an initial request, the following EnrolmentRequestMessages hould be rekeying requests.	

TP ld	SECPKI_ITS-S_ENR_07_BV	
Summary	Within the InnerECRequest, the requestedSubjectAttributes shall not contain a	
	certIssuePermissions field	
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.1	
Configuration	CFG_ENR_ITS-S	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the 'initi	alized' or 'enrolled' state	
ensure that		
when		
the IUT is requested	to send an EnrolmentRequestMessage	
then	then	
	siTs103097Data-Encrypted	
	containing an encrypted EtsiTs103097Data-Signed	
containing EtsiTs102941Data		
containing enrolmentRequest		
containing InnerEcRequest		
containing requestedSubjectAttributes		
	not containing certIssuePermissions	

TP ld	SECPKI ITS-S ENR 08 BV		
	In the headerInfo of the tbsData of the InnerECRequestSignedForPOP all other components of the component tbsdata.headerInfo except generationTime and psid are not		
Summary	used and absent. The psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [8] and the generationTime shall be present		
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.1		
Configuration	CFG_ENR_ITS-S		
PICS Selection			
	Expected behaviour		
with			
the IUT being in th	e 'initialized' or 'enrolled' state		
ensure that			
when	when		
the IUT is requested to send an EnrolmentRequestMessage			
then			
	an EtsiTs103097Data-Encrypted		
containing an encrypted EtsiTs103097Data-Signed			
	ing EtsiTs102941Data		
containing enrolmentRequest			
containing tbsData			
containing headerInfo			
containing psid			
indicating AID_CERT_REQ and containing generationTime			
	and not containing any other component		

PId SECPKI_ITS-S_ENR_09_BV	
Summary	In the headerInfo of the tbsData of the outer EtsiTs103097Data-Signed all other components of the component tbsdata.headerInfo except generationTime and psid are not used and absent. The psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [8] and the generationTime shall be present
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.1
Configuration	CFG_ENR_ITS-S
PICS Selection	
	Expected behaviour
with the IUT being in the 'initialized' or 'enrolled' state ensure that when the IUT is requested to send an EnrolmentRequestMessage then the IUT sends an EtsiTs103097Data-Encrypted	
containing an encrypted EtsiTs103097Data-Signed containing tbsData containing headerInfo containing psid indicating AID_CERT_REQ and containing generationTime and not containing any other component	

TP Id SECPKI_ITS-S_ENR_10_BV	
Summary	The EtsiTs103097Data-Encrypted containing the correctly encrypted ciphertext and a recipients component containing one instance of RecipientInfo of choice certRecipInfo containing the hashedId8 of the EA certificate in recipientId and the encrypted data encryption key in encKey. The data encryption key is encrypted using the public key found in the EA certificate referenced in the recipientId
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.1
Configuration	CFG_ENR_ITS-S
PICS Selection	
	Expected behaviour

ich is encrypted using the symmetric key SYMKEY contained in encKey	

TP ld	SECPKI_ITS-S_ENR_11_BV
Summary	In the inner signed data structure (InnerECRequestSignedForPOP), the signature is computed on the tbsData containing the InnerECRequest using the private key corresponding to the verificationKey, containing in InnerECRequest, to prove the possession of the generated verification key pair
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.1
Configuration	CFG_ENR_ITS-S
PICS Selection	
	Expected behaviour
with the IUT being in the 'initialized' or 'enrolled' state ensure that when the IUT is requested to send an EnrolmentRequestMessage then the IUT sends an EtsiTs103097Data-Encrypted containing an encrypted EtsiTs103097Data-Signed containing EtsiTs102941Data containing enrolmentRequest containing tbsData	
containing InnerEcRequest containing verificationKey (VKEY) containing signature computed on InnerECRequest using the private key corresponding to VKEY contained in InnerECRequest	

PId SECPKI_ITS-S_ENR_12_BV		
Check that signing of Enrolment Request message is permitted by the EC certificate		
Reference ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1, IEEE 1609.2™ [3], clause 6.4.28		
onfiguration CFG_ENR_ITS-S		
PICS Selection PICS_SECPKI_REENROLMENT		
	Expected behaviour	
with		
the IUT being in the 'enre	olled' state	
ensure that		
when		
the IUT is requested	to send an EnrolmentRequestMessage	
then		
	the IUT sends an EtsiTs103097Data-Encrypted	
containing an encrypted EtsiTs103097Data-Signed		
containing sig	containing signer	
containing c		
indicating	indicating HashedId8 of the EC certificate	
contai	containing appPermissions	
	containing an item of type PsidSsp	
containing psid		
indicating AID_CERT_REQ		
and containing ssp		
	containing bitmapSsp [0] (version)	
	indicating 1	
	containing bitmapSsp [1] (value)	
	indicating 'Enrolment Request' (bit 1) set to 1	

23

5.2.2.2 Enrolment response handling

TP ld	SECPKI_ITS-S_ENR_RCV_01_BV	
Summary	If an enrolment request fails, the IUT returns to the state "initialized"	
Reference	ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1	
Configura	tion CFG_ENR_ITS-S	
PICS Sele	ction	
	Expected behaviour	
with		
the IUT	being in the X_STATE	
and the	IUT has sent the EnrolmentRequestMessage	
ensure that	t	
when		
	IUT received the EnrolmentResponseMessage	
	containing a responseCode different than 0	
then		
the	the IUT returns to the X_STATE state	
Variants		
nn	X_STATE	
1	'initialized' state	
2	'enrolled' state	

TP ld	SECPKI_ITS-S_ENR_RCV_02_BV
Summary	The IUT is capable of parsing and handling of positive EnrolmentResponse messages containing the requested EC. In case of a successful enrolment, the IUT switches to the state 'enrolled'
Reference	ETSI TS 102 941 [1], clauses 6.1.3, 6.2.3.2.1 and 6.2.3.2.2
Configuration	CFG_ENR_ITS-S
PICS Selection	
	Expected behaviour
ensure that when the IUT receive containing a indicatin	nt the EnrolmentRequestMessage s a subsequent EnrolmentResponseMessage as an answer of the EA responseCode
then	

the IUT switches to the 'enrolled' state

TP Id SECPKI_ITS-S_ENR_RCV_03_BE Check that IUT does not use EC for re-enrolment if this usage is not allowed by EC's Summary application permissions (AID) Reference ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1, IEEE 1609.2™ [3], clause 6.4.28 Configuration CFG_ENR_ITS-S PICS Selection PICS_SECPKI_REENROLMENT Expected behaviour with the IUT being in the 'initialized' state and the IUT has sent an EnrolmentRequestMessage and the IUT has received an EnrolmentResponsetMessage containing certificate containing appPermissions not containing an item of type PsidSsp containing psid indicating AID_CERT_REQ ensure that when the IUT is requested to send an EnrolmentRequestMessage then the IUT sends an initial enrolment request

TP ld	SECPKI_ITS-S_ENR_RCV_04_BE	
Summary	Check that IUT does not use EC for re-enrolment if this usage is not allowed by EC's	
	application permissions (SSP)	
Reference ETSI TS 102 941 [1], clauses 6.1.3 and 6.2.3.2.1, IEEE 1609.2™ [3], clause 6.4.28		
Configuration CFG_ENR_ITS-S		
PICS Selection	PICS_SECPKI_REENROLMENT	
	Expected behaviour	
with		
the IUT being in the 'initi		
	EnrolmentRequestMessage	
and the IUT has receive	d an EnrolmentResponsetMessage	
•	containing certificate	
containing appPermissions		
containing an item of type PsidSsp		
containing psid		
indicat	ting AID_CERT_REQ	
and containing ssp		
	containing bitmapSsp[0] (version)	
indicating 1		
and containing bitmapSsp [1] (value)		
indicating 'Enrolment Request' (bit 1) set to 0		
ensure that		
when		
the IUT is requested	to send an EnrolmentRequestMessage	
then	then	
the IUT sends an init	tial enrolment request	

5.2.2.3 Enrolment request repetition

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

• PICS_SECPKI_ENROLMENT_RETRY = TRUE

TP ld	SECPKI_ITS-S_ENR_REP_01_BV
Summary	Check that IUT repeats an enrolment request when response has not been received
Reference	ETSI TS 103 601 [6], clause 5.1.2
Configuration	CFG_ENR_ITS-S
PICS Selection	
	Expected behaviour
and the IUT has no ensure that when the IUT local tir then	e 'initialized' state y sent the Enrolment Request at the time T1 of yet received the Enrolment Response ne is reached the T1 + PIXIT_ENR_TIMEOUT_TH1 to EA an EnrolmentRequestMessage

TP ld	SECPKI_ITS-S_ENR_REP_02_BV
Summary	Check that IUT uses the same message to perform enrolment retry
Reference	ETSI TS 103 601 [6], clause 5.1.2
Configuration	CFG_ENR_ITS-S
PICS Selection	
	Expected behaviour
ensure that when	it the Enrolment Request (<i>M</i>) to re-send an Enrolment Request

TP ld	SECPKI_ITS-S_ENR_REP_03_BV
Summary	Check that IUT stops sending the Enrolment Request message if Enrolment Response
	message has been received
Reference	ETSI TS 103 601 [6], clause 5.1.2
Configuration	CFG_ENR_ITS-S
PICS Selection	
	Expected behaviour
with	
the IUT being in th	ne 'initialized' state
and the IUT has s	ent the Enrolment Request more than 1 time
ensure that	

when

the IUT receives an Enrolment Response

then

the IUT stops sending Enrolment Requests to EA

TP ld	SECPKI_ITS-S_ENR_REP_04_BV
Summary	Check that IUT stops sending the Enrolment Request message if maximum number of
	retry has been reached
Reference	ETSI TS 103 601 [6], clause 5.1.2
Configuration	CFG_ENR_ITS-S
PICS Selection	
	Expected behaviour
with	
the IUT being in th	e 'initialized' state
and the IUT has st	arted sending the Enrolment Request
ensure that	
when	
the IUT sent th	e PIXIT_ENR_MAX_N1 Enrolment Request messages
then	
the IUT stops s	ending Enrolment Requests

TP Id SECPKI_ITS-S_ENR_REP_05_BV Check that IUT stops sending the Enrolment Request message if timeout has been Summary reached Reference ETSI TS 103 601 [6], clause 5.1.2 CFG_ENR_ITS-S Configuration PICS Selection **Expected behaviour** with the IUT being in the 'initialized' state and the IUT has started sending the Enrolment Request at the time T1 ensure that when the IUT local time is reached the T1 + PIXIT_ENR_TIMEOUT_TH2 then the IUT stops sending an Enrolment Request messages

TP ld	SECPKI_ITS-S_ENR_REP_05_BV
Summary	Check that IUT stops sending the Enrolment Request message if sending timeout (TH2)
	has been reached
Reference	ETSI TS 103 601 [6], clause 5.1.2
Configuration	CFG_ENR_ITS-S
PICS Selection	
	Expected behaviour
with	
the IUT being in the 'in	nitialized' state
and the IUT has starte	ed sending the Enrolment Request
ensure that	
when	
the IUT sent the E	nrolment Request messages
then	
the IUT stops send	ding Enrolment Requests

5.2.3 Authorization

5.2.3.0 Overview

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

PICS_SECPKI_AUTHORIZATION = TRUE

5.2.3.1 Authorization request

TP ld	SECPKI_ITS-S_AUTH_01_BV
Summary	Check that the ITS-S sends the AuthorizationRequestMessage to the Authorization
	Authority (AA) to request an authorization ticket
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.0
Configuration	CFG_AUTH_ITS-S
PICS Selection	
	Expected behaviour
with	
the IUT in 'enrolled	l' state
and the AA in 'ope	rational' state
ensure that	
when	
the IUT is trigg	ered to request new Authorization Ticket (AT)
then	
the IUT sends	an EtsiTs103097Data-Encrypted to the AA

TP ld	SECPKI_ITS-S_AUTH_02_BV
Summary	Check that the AuthorizationRequestMessage is encrypted and sent to only one
	Authorization Authority
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITS-S
PICS Selection	
	Expected behaviour
with	
the IUT in 'enrolled	J' state
and the AA in 'ope	rational' state
authorized with	CERT_IUT_A_AA certificate
ensure that	
when	
the IUT is trigg	ered to request new Authorization Ticket (AT)
then	
the IUT sends	an EtsiTs103097Data to the AA
	content.encryptedData.recipients
	ng size 1
	taining the instance of RecipientInfo
	aining certRecipInfo
(containing recipientId indicating HashedId8 of the CERT_IUT_A_AA
· · · · ·	

I P Id	SECPKI_IIS-S_AUTH_03_BV
Summary	Check that the AuthorizationRequestMessage is encrypted using the encryptionKey
	found in the AA certificate referenced in recipientId
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITS-S
PICS Selection	
	Expected behaviour
with	
the IUT in 'enrolled	l' state
and the AA in 'ope	rational' state
authorized with	A certificate
containing e	encryptionKey (AA_ENC_PUB_KEY)
ensure that	
when	
the IUT is trigg	ered to request new Authorization Ticket (AT)
then	
the IUT sends	a EtsiTs103097Data to the AA
containing of	content.encryptedData
containi	ng ciphertext
	aining data
	encrypted using symmetric key
	been decrypted using AA_ENC_PUB_KEY

ECPKI_ITS-S_AUTH_04_BV heck that the authorization requests never reuses the same encryption key and nonce TSI TS 102 941 [1], clause 6.2.3.3.1 FG_AUTH_ITS-S
Expected behaviour
e
one or more Authorization Requests
state
request new Authorization Ticket (AT)
103097Data to the AA
encryptedData
ertext.aes128ccm.nonce
alue not equal to the nonce in N previous messages
recipients[0].certRecipInfo.encKey
ncrypted symmetric key (S_KEY)
g symmetric key not equal to the key was used in N previous messages

TP ld	SECPKI_ITS-S_AUTH_05_BV
Summary	Check that the authorization request protocol version is set to 1
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITS-S
PICS Selection	
	Expected behaviour
with	
the IUT in 'enrolled' stat	te
and the AA in 'operation	nal' state
ensure that	
when	
the IUT is triggered	to request new Authorization Ticket (AT)
then	
the IUT sends a Ets	iTs103097Data to the AA
containing EtsiT	
containing ve	ersion
containin	g indicating 1
containing co	ontent
containin	g authorizationRequest

TP ld	SECPKI_ITS-S_AUTH_06_BV
	Check that for each authorization request the ITS-S generates a new verification key pair
Summary	Check that for each authorization request the ITS-S generates a new encryption key pair
	Check that for each authorization request the ITS-S generates a new hmac-key
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITS-S
PICS Selection	
	Expected behaviour
with	
the IUT in 'enrolled	J' state
and the AA in 'ope	rational' state
ensure that	
when	
	ered to request new Authorization Ticket (AT)
then	
	a EtsiTs103097Data to the AA
	EtsiTs102941Data
	ing authorizationRequest
	taining publicKeys
,	containing verificationKey indicating value not equal to the field verificationKey of N previous messages
	and not containing encryptionKey
	or containing encryptionKey
,	indicating value not equal to the field encryptionKey of N previous messages
and	containing hmacKey
	ndicating value not equal to the field hmacKey of N previous messages
	hosen according to implementations recommendations.

TP ld	SECPKI_ITS-S_AUTH_07_BV		
Summary	Check that ITS-S sends Authorization request with a keyTag field computed as described		
	in ETSI TS 102 941 [1], clause 6.2.3.3.1		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1		
Configuration	CFG_AUTH_ITS-S		
PICS Selection			
	Expected behaviour		
with			
the IUT in 'enrolled' sta	ate		
and the AA in 'operation	inal' state		
ensure that			
when			
the IUT is triggered	the IUT is triggered to request new Authorization Ticket (AT)		
then			
the IUT sends a Et	siTs103097Data to the AA		
containing Etsi	ls102941Data		
containing authorizationRequest			
containing sharedAtRequest			
containing keyTag			
indicating properly calculated value			

TP ld	SECPKI_ITS-S_AUTH_08_BV		
Summary	Check that ITS-S sends Authorization request with eald of EA certificate		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1		
Configuration	CFG_AUTH_ITS-S		
PICS Selection			
	Expected behaviour		
with			
the IUT is enrolled by the	ne EC, signed with the CERT EA certificate		
and the AA in 'operation	nal' stateensure that		
when	when		
the IUT is triggered	the IUT is triggered to request new Authorization Ticket (AT)		
then			
the IUT sends a Ets	iTs103097Data to the AA		
containing EtsiT	s102941Data		
containing a	uthorizationRequest		
containing sharedAtRequest			
containing eald			
indicating HashedId8 of CERT_ EA certificate			

TP ld	SECPKI ITS-S AUTH 09 BV		
Summary	Check that ITS-S sends Authorization request with the certificateFormat equal to 1		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1		
Configuration	CFG_AUTH_ITS-S		
PICS Selection			
	Expected behaviour		
with			
the IUT in 'enrolled' state	9		
and the AA in 'operation	al' state		
ensure that			
when	when		
the IUT is triggered t	o request new Authorization Ticket (AT)		
then			
the IUT sends a Etsi	Ts103097Data to the AA		
containing EtsiTs	:102941Data		
containing au	thorizationRequest		
containing sharedAtRequest			
containing certificateFormat			
indicating 1			

TP Id	SECPKI ITS-S AUTH 10 BV
Summary	Check that ITS-S sends Authorization request certificate attributes are properly set
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITS-S
PICS Selection	
	Expected behaviour
with	
the IUT in 'enrolled' s	tate
and the AA in 'operat	ional' 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 Ets	iTs102941Data
containing	authorizationRequest
contair	ing sharedAtRequest
containing requestedSubjectAttributes	
containing appPermissions	
	and not containing certIssuePermissions

TP ld	SECPKI_ITS-S_AUTH_11_BV		
Summary	Check that ITS-S sends Authorization request containing EC signature calculated over the		
Summary	sharedATRequest using supported hash algorithm		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1		
Configuration	CFG_AUTH_ITS-S		
PICS Selection			
	Expected behaviour		
with			
the IUT in 'enrolled' state	9		
and the AA in 'operation	al' state		
ensure that			
when	when		
88	the IUT is triggered to request new Authorization Ticket (AT)		
then	then		
	the IUT sends a EtsiTs103097Data to the AA		
0	containing EtsiTs102941Data		
•	thorizationRequest		
containing	g ecSignature		
containing structure of type EtsiTs103097Data-SignedExternalPayload			
containing tbsData			
containing payload			
containing extDataHash			
	indicating supported hash algorithm		
and indicating hash of sharedATRequest			

TP ld	SECPKI_ITS-S_AUTH_12_BV		
Summary	Check that the ecSignature psid is set to the proper ITS_AID		
	Check that the ecSignature generation time is present		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1		
Configuration	CFG_AUTH_ITS-S		
PICS Selection			
	Expected behaviour		
with			
the IUT in 'enrolled' stat	e		
and the AA in 'operation	al' state		
ensure that			
when			
	the IUT is triggered to request new Authorization Ticket (AT)		
then			
	Ts103097Data to the AA		
containing EtsiTs			
containing authorizationRequest			
containing ecSignature containing structure of type EtsiTs103097Data-SignedExternalPayload			
containing the Data			
containing headerInfo			
containing psid			
indicating AID_PKI_CERT_REQUEST			
and containing generationTime			
	and not containing any other headers		

TP Id	SECPKI ITS-S AUTH 13 BV		
Summary	Check that ITS-S sends Authorization request containing EC signature with supported		
Caninal y	hash algorithm		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1		
Configuration	CFG_AUTH_ITS-S		
PICS Selection			
	Expected behaviour		
with			
the IUT in 'enrolled' state	e		
and the AA in 'operation	al' state		
ensure that			
when	when		
the IUT is triggered t	the IUT is triggered to request new Authorization Ticket (AT)		
then			
the IUT sends a EtsiTs103097Data to the AA			
containing EtsiTs	containing EtsiTs102941Data		
containing authorizationRequest			
containing ecSignature			
containing structure of type EtsiTs103097Data-SignedExternalPayload			
COI	containing hashId		
indicating supported hash algorithm			

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

TP ld	SECPKI_ITS-S_AUTH_15_BV
Summary	Check that the encrypted ecSignature of the Authorization request is encrypted using the
	EA encryptionKey
	Check that the encrypted ecSignature of the Authorization request was done from the
	EtsiTs103097Data-SignedExternalPayload structure
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITS-S
PICS Selection	PICS_PKI_AUTH_PRIVACY
	Expected behaviour
with	
the IUT in 'enrolled	J' state
and the AA in 'ope	rational' state
and the EA in 'ope	
	n CERT_EA certificate
ensure that	
when	
	ered to request new Authorization Ticket (AT)
then	
	a EtsiTs103097Data to the AA
	EtsiTs102941Data
	ing authorizationRequest
	taining ecSignature
(containing encryptedEcSignature
	containing recipients
	containing only one element of type RecipientInfo containing certRecipInfo
	containing recipientId
	indicating HashedId8 of the CERT EA
	and containing encKey
	indicating encryption key of supported type
	and containing cyphertext
	containing encrypted representation
	of structure EtsiTs103097Data-SignedExternalPayload

=

TP ld	SECPKI_ITS-S_AUTH_16_BV	
Summary	Check that the ecSignature of the Authorization request is not encrypted	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_ITS-S	
PICS Selection	NOT PICS_PKI_AUTH_PRIVACY	
	Expected behaviour	
then the IUT sends containing contair con		

TP Id	SECPKI_ITS-S_AUTH_17_BV
Summary	Check that the Authorization request is not signed when Prove of Possession is not used
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_ITS-S
PICS Selection	NOT PICS_PKI_AUTH_POP
	Expected behaviour
with	
the IUT in 'enrolled	d' state
and the AA in 'ope	arational' state
ensure that	
when	
the IUT is trigg	ered to request new Authorization Ticket (AT)
then	
the IUT sends	a EtsiTs103097Data-Encrypted to the AA
containing encrypted representation of the leee1609Dot2Data	
containing content.unsecuredData	

TP ld	SECPKI_ITS-S_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_ITS-S
PICS Selection	PICS_PKI_AUTH_POP
	Expected behaviour
with	
the IUT in 'enrolled' s	tate
and the AA in 'operat	ional' state
ensure that	
when	
00	ed to request new Authorization Ticket (AT)
then	
	tsiTs103097Data-Encrypted to the AA
containing cyp	
	encrypted representation of the EtsiTs103097Data-Signed
	ing content signedData
	taining hashId
	indicating valid hash algorithm
	I containing tbsData
	containing headerInfo
	containing psid
	indicating AID_PKI_CERT_REQUEST
	and containing generationTime
	and not containing any other headers
	l containing signer
	containing self
and	I containing signature
	indicating value calculated over tbsData with the private key correspondent to the verificationKey from this message
	correspondent to the vehilication key from this message

TP ld	SECPKI ITS-S AUTH 19 BV		
Summary	Check that the signing of ecSignature of the Authorization request is permitted by the EC certificate		
Reference	ETSI TS 102 941 [1], clause B.5		
Configuration	CFG AUTH ITS-S		
PICS Selection			
Expected behaviour			
with	•		
the IUT in 'enrolled' state	9		
and the AA in 'operation	al' state		
ensure that			
when			
	o request new Authorization Ticket (AT)		
then			
	Ts103097Data to the AA		
containing EtsiTs	thorizationRequest		
5	a ecSignature		
	ning structure of type EtsiTs103097Data-SignedExternalPayload		
containing sindclore of type List's 103097 Data-Signed External Ayload			
	indicating HashedId8 of EC certificate		
containing appPermissions			
containing an item of type PsidSsp			
containing psid			
indicating AID_CERT_REQ			
	and containing ssp		
	containing bitmapSsp[0] (version)		
	indicating 1		
	containing bitmapSsp[1] (value)		
	indicating 'Enrolment Request' (bit 1) set to 1		

5.2.3.2 Authorization response handling

Void.

5.2.3.3 Authorization request repetition

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

PICS_SECPKI	_ AUTHORIZATION	$_$ RETRY = TRUE
-------------	-----------------	-------------------

TP ld	SECPKI_ITS-S_AUTH_REP_01_BV		
Summary	Check that IUT repeats an authorization request when response has not been received		
Reference	ETSI TS 103 601 [6], clause 5.2		
Configuration	CFG_AUTH_ITS-S		
PICS Selection			
Expected behaviour			
with			
the IUT being in the 'enrolled' state			
and the IUT already sent the Authorization Request at the time T1			
and the IUT has not yet received the Authorization Response			
ensure that			
when			
the IUT local time is reached the <i>T1</i> + PIXIT_AUTH_TIMEOUT_TH1			
then			
the IUT sends to EA an AuthorizationRequestMessage			

TP ld	SECPKI_ITS-S_AUTH_REP_02_BV
Summary	Check that IUT uses the same message to perform authorization retry
Reference	ETSI TS 103 601 [6], clause 5.1.2
Configuration	CFG_AUTH_ITS-S
PICS Selection	
	Expected behaviour
with the IUT being in the 'enrolled' state and the IUT already sent the Authorization Request (<i>M</i>) to AA ensure that when the IUT is triggered to re-send an AuthorizationRequestMessage to AA then	

the IUT sends **M** to AA

TP Id SECPKI_ITS-S_AUTH_REP_03_BV Summary Check that IUT stops sending the Authorization Request message if Authority Response message has been received	orization
Reference ETSI TS 103 601 [6], clause 5.1.2	
Configuration CFG_AUTH_ITS-S	
PICS Selection	
Expected behaviour	
with	

the IUT being in the 'enrolled' state

and the IUT has sent the Authorization Request more than 1 time

ensure that

when

the IUT receives an Authorization Response

then

the IUT stops sending Authorization Requests to AA

TP ld	SECPKI_ITS-S_AUTH_REP_04_BV
Summary	Check that IUT stops sending the Authorization Request message if maximum number of
	retry has been reached
Reference	ETSI TS 103 601 [6], clause 5.1.2
Configuration	CFG_AUTH_ITS-S
PICS Selection	
	Expected behaviour
with	
the IUT being in th	e 'enrolled' state
and the IUT has started sending the Authorization Request	
ensure that	
when	
the IUT sent the PIXIT_AUTH_MAX_N1 Authorization Request messages	
then	
the IUT stops s	ending Authorization Requests

TP ld	SECPKI_ITS-S_AUTH_REP_05_BV	
Summary	Check that IUT stops sending the Authorization Request message if timeout has been	
	reached	
Reference	ETSI TS 103 601 [6], clause 5.1.2	
Configuration	CFG_AUTH_ITS-S	
PICS Selection		
	Expected behaviour	
with		
the IUT being in the 'e	nrolled' state	
and the IUT has started sending the Authorization Request at the time T1		
ensure that	ensure that	
when		
the IUT local time is reached the T1 + PIXIT_AUTH_TIMEOUT_TH2		
then		
the IUT stops send	ding an Authorization Request messages	

5.2.3.4 Authorization using butterfly key expansion mechanism

5.2.3.4.1 Overview

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

PICS_SECPKI_ AUTH_BFK = TRUE

5.2.3.4.2 Butterfly authorization request

TP ld	SECPKI_ITS-S_ BFK_AUTH_01_BV	
	Check that the ITS-S sends the EtsiTs103097Data to the Enrolment Authority (EA) to	
Summary	request a batch of authorization tickets	
•	Check that this message is encrypted and addressed to a single recipient.	
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.1	
Configuration	CFG_BFK_AUTH_ITS-S	
PICS Selection		
	Expected behaviour	
with	·	
the IUT in 'enrolled'	state	
and the EA in 'opera	ational' state	
authorized with	enrolment certificate CERT_IUT_A_EA	
ensure that		
when		
the IUT is trigge	the IUT is triggered to request a new batch of authorization tickets	
then		
the IUT sends a	EtsiTs103097Data to the EA	
containing content.encryptedData		
	containing recipients	
indicating size 1		
and containing the instance of RecipientInfo		
CC	containing certRecipInfo	
	containing recipientId	
indicating HashedId8 of the CERT_IUT_A_EA		

TP ld	SECPKI_ITS-S_BFK_AUTH_02_BV	
Summary	Check that the ButterflyAuthorizationRequestMessage is signed using the EC certificate	
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.2	
Configuration	CFG_BFK_AUTH_ITS-S	
PICS Selection	NOT PICS_SECPKI_ENROLMENT_X509	
	Expected behaviour	
with		
the IUT in 'enrolled' state	-	
with certificate CER		
	thorized with CERT_IUT_A_EA	
and the EA in 'operation		
	Iment certificate CERT_IUT_A_EA	
ensure that		
when	a request a new batch of outbarization tickate	
then	o request a new batch of authorization tickets	
	Ts103097Data to the EA	
	nt.encryptedData.cipherText	
•	g encrypted representation of EtsiTs103097Data	
	ning signedData	
	ntaining tbsData	
	containing headerInfo	
containing psid		
	indicating AID_PKI_CERT_REQUEST	
and containing generationTime		
and not containing any other field		
and containing payload.data		
indicating EtsiTs102941Data		
	containing version	
indicating '1'		
	and containing content	
	containing butterflyAuthorizationRequest	
	indicating EeRaCertRequest and containing signer	
	containing digest	
	indicating HashedId8 of the CERT_EC	
<u> </u>		

TP ld	SECPKI_ITS-S_BFK_AUTH_02a_BV
Summary	Check that the ButterflyAuthorizationRequestMessage is signed using the X.509 EC
Summary	certificate
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.2
Configuration	CFG_BFK_AUTH_ITS-S
PICS Selection	PICS_SECPKI_ENROLMENT_X509
	Expected behaviour
with	
the IUT in 'enrolled' st	ate
with certificate CE	RT_ENR of form X.509
and the EA in 'operati	
	rolment certificate CERT_IUT_A_EA
ensure that	
when	
00	d to request a new batch of authorization tickets
then	
	tsiTs103097Data to the EA
	tent.encryptedData.cipherText
	ing encrypted representation of EtsiTs103097Data
	taining signedX509CertificateRequest
(containing encoded representation of the SignedX509CertificateRequest
	containing tbsRequest
	indicating the EeRaCertRequest
	containing signer
	containing the DER representation of the CERT_ENR and containing signature
	calculated over the hashes of tbsRequest and signer
	using the private key correspondent to the CERT_ENR

TP ld	SECPKI_ITS-S_BFK_AUTH_03_BV	
Summary	Check that the ButterflyAuthorizationRequestMessage contains all required elements	
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.2	
Configuration	CFG_BFK_AUTH_ITS-S	
PICS Selection		
	Expected behaviour	
with		
the IUT in 'enrolled' state	9	
and the EA is in 'operation	onal' state	
ensure that		
when		
	o request a new batch of Authorization Tickets (AT)	
then		
	EA a EtsiTs103097Data	
containing the Ee		
containing ve		
	indicating '2' and containing generationTime	
	current ITS timestamp	
	g certificateType	
indicating 'explicit" and containing tbsCert		
containing id		
	ing 'none'	
and containing cracald		
indicating '000000'H		
and containing crlSeries		
indicating '0'		
and containing additionalParams		
containing	ı original	
	ing unified	
	quest can be sent by IUT using approaches presented in	
SECPKI_ITS-S_/	AUTH_BFK_02_BV and SECPKI_ITS-S_AUTH_BFK_02a_BV.	

TP ld	SECPKI_ITS-S_BFK_AUTH_04_BV
Summary	Check that the ButterflyAuthorizationRequestMessage contains newlly generated
Summary	caterpillar public key
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.2
Configuration	CFG_BFK_AUTH_ITS-S
PICS Selection	
	Expected behaviour
with	
the IUT in 'authorized' s	tate
and the IUT already ser	nt one or more Butterfly Authorization Requests
and the EA is in 'operat	
ensure that	
when	
the IUT is triggered	to request a new batch of Authorization Tickets (AT)
then	
the IUT sends to the	e EA an EtsiTs103097Data message
containing the E	eRaCertRequest
containin	g tbsCert
conta	ining verifyKeyIndicator
co	ntaining verificationKey
containing public key	
	not equal to the key was used in a previously sent Butterfly Authorization Requests
and conta	aining additionalParams
conta	ining original
co	ntaining signingExpansion
	containing 16 byte string
not equal to the value was used in a previously sent Butterfly Authorization Requests	
and containing encryptionKey	
containing public key	
not equal to the key was used in a previously sent Butterfly Authorization Requests	
containing encryptionExpansion	
containing 16 byte string	
	not equal to the value was used in a previously sent Butterfly Authorization Requests
	ntaining unified
со	ntaining 16 byte string
	not equal to the value was used in a previously sent Butterfly Authorization Requests
NOTE: The EeRaCertR	equest can be sent by IUT using approaches presented in
SECPKI_ITS-S_	AUTH_BFK_02_BV and SECPKI_ITS-S_AUTH_BFK_02a_BV.

TP ld	SECPKI_ITS-S_BFK_CERTDNL_01_BV	
	Check that IUT downloads the AT certificates batch after receiving of positive	
Summary		
Deference	ButterflyAuthorizationResponse message	
Reference	ETSI TS 102 941 [1], clauses 6.2.3.5.3 and 6.2.3.5.6	
Configuration	CFG_BFK_AUTH_ITS-S	
PICS Selection	—	
	Expected behaviour	
with		
the IUT being in the 'enr		
and the EA is in 'operation		
	ButterflyAuthorizationRequestMessage	
ensure that		
when		
	EtsiTs102941Data as an answer of the EA	
	lyAuthorizationResponse	
	indicating RaEeCertInfo	
containing generationTime		
	ing GEN_TIME	
indicating VALUE_I		
and containing requestHash		
indicating REQ_HASH		
and containing nextDITime		
indicating time between GEN_TIME and current time then		
	uttarfly/\tDownloadPaguactMassaga	
the IUT sends the ButterflyAtDownloadRequestMessage containing butterflyAtDownloadRequest		
	indicating EeRaDownloadRequest	
	generationTime	
	ing value more than GEN_TIME	
	ining filename	
	ing string REQ_HASH + "_" + VALUE_I + ".zip"	
indibat		

5.2.3.4.3 Butterfly AT download request

5.2.4 CTL handling

TP ld	SECPKI ITS-S CTL 01 BV	
Summary	Check that the IUT trusts the new RCA from the received ECTL	
Reference	ETSI TS 102 941 [1], clause 6.3.5	
Configuration	CFG_CXL_P2P	
PICS Selection		
	Expected behaviour	
with	·	
the IUT does not trust	the CERT_RCA_NEW	
and the IUT has receiv	ved the TLM CTL	
containing the CEF	containing the CERT RCA NEW	
ensure that	5 = =	
when	when	
the IUT received a	the IUT received a CAM	
signed with AT	signed with AT certificate	
signed with AA certificate		
signed with CERT_RCA_NEW		
then		
the IUT accepts th	is CAM	

TP ld	SECPKI_ITS-S_CTL_02_BV	
Summary	Check that the IUT distrusts the RCA when it is deleted from ECTL	
Reference	ETSI TS 102 941 [1], clause 6.3.5	
Configuration	CFG_CXL_P2P	
PICS Selection		
	Expected behaviour	
With		
the IUT trusting the C	ERT_RCA	
and the IUT has recei	ved the TLM CTL	
not containing the	not containing the CERT_RCA	
ensure that		
when		
the IUT received a		
signed with AT	signed with AT certificate	
signed with AA certificate		
signed with CERT_RCA		
then		
the IUT rejects this	s CAM	

TP ld	SECPKI_ITS-S_CTL_03_BV	
Summary	Check that the IUT trust the AA when it is received in RCA CTL	
Reference	ETSI TS 102 941 [1], clause 6.3.5	
Configuration	CFG_CXL_P2P	
PICS Selection		
	Expected behaviour	
with		
the IUT trusting the CEF	RT_RCA	
and the IUT does not have the CERT_AA_NEW		
and the IUT has receive		
containing the CERT	containing the CERT_AA_NEW	
and issued by CERT_RCA		
ensure that		
when		
the IUT received a CAM		
signed with AT certificate		
signed with CERT_AA_NEW digest		
then		
the IUT accepts this CAM		

TP ld	SECPKI_ITS-S_CTL_04_BV
Summary	Check that the IUT requests new ECTL when current one is expired
Reference	ETSI TS 102 941 [1], clause 6.3.5
Configuration	CFG_CXL_P2P
PICS Selection	
	Expected behaviour
with the IUT already downloc containing nextUpd indicating times and containing CP ensure that when the T1 < CURREN then the IUT sends a re	date stamp T1 OC URL

TP ld	SECPKI_ITS-S_CTL_05_BV
Summary	Check that the IUT requests new RCA CTL when current one is expired
Reference	ETSI TS 102 941 [1], clause 6.3.5
Configuration	CFG_CXL_P2P
PICS Selection	
	Expected behaviour
with the IUT already downloa containing nextUpda indicating timesta and containing RCA ensure that when the T1 < CURRENT then the IUT sends a requ	ite amp T1 DC URL

5.2.5 CTL distribution

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

PICS_SECPKI_ECTL_BROADCAST = TRUE or PICS_SECPKI_CTL_BROADCAST = TRUE

TP ld	SECPKI_ITS-S_CTLDIST_01_BV
Check that the IUT retransmits the newly received Delta CTL	
Reference	ETSI TS 103 601 [6], clause 4.2.1.4
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-05.2
	Expected behaviour
with	
the IUT is configured	to redistribute the Delta CTL
and the IUT does not	contain an CTL information
ensure that	
when	
the IUT has receiv	ved the Delta CTL
then	
the IUT is started	to broadcast the received Delta CTL
NOTE: This TP is app	lied for both: ECTL and RootCA CTL handling behaviour.
TP ld	SECPKI_ITS-S_CTLDIST_02_BV
Summary Check that the IUT retransmits the updated Delta CTL	

Summary	Check that the IUT retransmits the updated Delta CTL		
Reference	ETSI TS 103 601 [6], clause 4.2.1.4		
Configuration	CFG_CXL_P2P		
PICS Selection	UC-SEC-05.2		
	Expected behaviour		
with			
the IUT is configured to I	redistribute the Delta CTL		
and the IUT contains an CTL information			
containing ctlSequence (SN)			
ensure that			
when			
the IUT has received	the Delta CTL		
containing ctlSequence			
indicating value greater than SN			
then			
the IUT is started to broadcast the received Delta CTL			
NOTE: This TP is applied	d for both: ECTL and RootCA CTL handling behaviour.		

IP	ld	SECPKI_ITS-S_CTLDIST_03_BV	
Sui	mmary	Check that the IUT is using the proper BTP port to broadcast the Delta CTL	
	ierence	ETSI TS 103 601 [6], clause 5.4.4	
Со	nfiguration	CFG_CXL_P2P	
	S Selection	UC-SEC-05.2, X_PICS	
		Expected behaviou	r
with	า	•	
	the IUT is configured to	o support P2P X_DISTRIBUTION distribution	on
		ved the Delta X_DISTRIBUTION message	
	sure that		
	when		
		to broadcast the Delta X DISTRIBUTION	message
	then		moocago
	the IUT sends the J	X MESSAGE	
		—	
	using the BTP r		
	using the BTP p	Permutation table	
X	using the BTP p		X PICS
X A	· · · ·	Permutation table	
	X_DISTRIBUTION	Permutation table	X_PICS PICS_SECPKI_ECTL_BROADCAST
A	X_DISTRIBUTION ECTL	Permutation table X_MESSAGE TlmCertificateTrustListMessage	X_PICS
Α	X_DISTRIBUTION ECTL	Permutation table X_MESSAGE TlmCertificateTrustListMessage	X_PICS PICS_SECPKI_ECTL_BROADCAST
A B	X_DISTRIBUTION ECTL RootCA CTL	Permutation table X_MESSAGE TlmCertificateTrustListMessage	X_PICS PICS_SECPKI_ECTL_BROADCAST
А В ТР	X_DISTRIBUTION ECTL RootCA CTL	Permutation table X_MESSAGE TlmCertificateTrustListMessage RcaCertificateTrustListMessage SECPKI_ITS-S_CTLDIST_04_BV	X_PICS PICS_SECPKI_ECTL_BROADCAST

Summary [Check that the IUT stops to redistribute the Delta CTL if another node is also sending it			
Reference	ETSI TS 103 601 [6], clause 5.3.1		
Configuration CFG_CXL_P2P			
PICS Selection UC-SEC-05.2			
Expected behaviour			
with			
the IUT is configured to	support P2P Delta X_DISTRIBUTION d	istribution	
and the IUT has started	broadcasting the Delta X_DISTRIBUTIC	DN message	
signed with X_CERT			
and containing ctlSe	equence (SN)		
ensure that			
when	when		
the IUT has received the Delta X_DISTRIBUTION			
signed with <i>X_CERTIFICATE</i>			
and containing ct			
0	indicating value equal or higher than SN		
then			
the IUT stops broadfcasting the Delta X_DISTRIBUTION			
signed with X_CERTIFICATE			
and containing ctlSequence (SN)			
Permutation table			
X X_DISTRIBUTION X	<u>CERTIFICATE</u>	X_PICS	
	CERT_TLM	PICS_SECPKI_ECTL_BROADCAST	
B RootCA CTL C	CERT_IUT_A_RCA	PICS_SECPKI_CTL_BROADCAST	

TP ld	SECPKI_ITS-S_CTLDIST_05_BV
Summary	Check that the IUT requests the Delta CTL using P2P protocol when no CTL information
	available
Reference	ETSI TS 103 601 [6], clause 5.3.4.3
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-06.1
	Expected behaviour
with	
the IUT is configu	red to support P2P Delta CTL distribution
and the IUT conta	ins valid TLM or/and RootCA certificate (<i>CERT</i>)
and the IUT does	not contain any CTL information
ensure that	
when	
the IUT is trigg	pered to request the CTL information for CERT
then	
the IUT starts	sending Secured GN messages
containing	contributedExtensions
contain	ing an item of type ContributedExtensionBlock
con	taining contributorId
	indicating etsiHeaderInfoContributorId (2)
con	taining an item of type EtsiTs102941CtlRequest
	containing issuerId
	indicating HashedID8 of the CERT
	and not containing lastKnownCtlSequence
	applied for both: ECTL and RootCA CTL handling behaviour.

TP ld	SECPKI_ITS-S_CTLDIST_06_BV
Summary	Check that the IUT requests the Delta CTL using P2P protocol when new CTL information
Summary	is required
Reference ETSI TS 103 601 [6], clause 5.3.4.3	
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-06.1
	Expected behaviour
with	
the IUT is configured	to support P2P Delta CTL distribution
	valid TLM or/and RootCA certificate (CERT)
and the IUT contain t	the CERT CTL information
containing ctlSe	-
indicating (SA	<i>ſ</i>)
ensure that	
when	
	ed to request the CTL information, associated with CERT
then	
	nding Secured GN messages
-	ntributedExtensions
	an item of type ContributedExtensionBlock
containing contributorId	
indicating etsiHeaderInfoContributorId (2)	
containing an item of type EtsiTs102941CtlRequest	
containing issuerId	
	indicating HashedID8 of the CERT
	containing lastKnownCtlSequence
	indicating SN
NOTE: This TP is app	plied for both: ECTL and RootCA CTL handling behaviour.

4	7

mary Check that the IUT requests the Delta CTL using P2P protocol when CTL information is expired rence ETSI TS 103 601 [6], clause 5.3.6 iguration CFG_CXL_P2P iselection UC-SEC-06.1 Expected behaviour te IUT is configured to support P2P Delta CTL distribution nd the IUT contains valid TLM or/and RootCA certificate (CERT) nd the IUT contains the CERT CTL information containing coll Sequence indicating (SM) re that the IUT receives the Secured GN Message containing contributedExtensions containing contributedExtensions containing an item of type ContributedExtensionBlock containing an item of type ContributedExtensionBlock containing an item of type EtsiTs102941CtIRequest containing an item of type EtsiTs102941CtIRequest containing lastKnownCtISequence indicating value higher than SN tel Ite IUT starts sending Secured GN messages containing an item of type ContributedExtensionBlock containing an item of type ContributedE	TP ld	SECPKI_ITS-S_CTLDIST_07_BV
inary expired rence ETSI TS 103 601 [6], clause 5.3.6 iguration CFG_CXL_P2P Selection UC-SEC-06.1 Expected behaviour	Summory	
rence ETSI TS 103 601 [6], clause 5.3.6 iguration CFG_CXL_P2P i Selection UC-SEC-06.1 Expected behaviour re IUT is configured to support P2P Delta CTL distribution nd the IUT contains valid TLM or/and RootCA certificate (<i>CERT</i>) nd the IUT contains the <i>CERT</i> CTL information containing colfsequence indicating (<i>SN</i>) re that then the IUT receives the Secured GN Message containing a nitem of type ContributedExtensionBlock containing contributedExtensions containing an item of type EtsiTs102941Ct1Request containing lastKnownCt1Sequence indicating value higher than <i>SN</i> ren the IUT starts sending Secured GN messages containing contributedExtensions containing an item of type ContributedExtensionBlock containing lastKnownCt1Sequence indicating value higher than <i>SN</i> ren the IUT starts sending Secured GN messages containing contributedExtensions containing on item of type ContributedExtensionBlock containing contributedExtensionS containing an item of type EtsiTs102941Ct1Request containing an item of type EtsiTs102941Ct1Request containin	Summary	
Selection UC-SEC-06.1 Expected behaviour he IUT is configured to support P2P Delta CTL distribution nd the IUT contains valid TLM or/and RootCA certificate (CERT) nd the IUT contains the CERT CTL information containing colspan="2">containing colspan="2">containing colspan="2">containing colspan="2">containing colspan="2">containing colspan="2">contributedExtensions containing an item of type ContributedExtensionBlock containing an item of type ContributedExtensionBlock containing a nitem of type EtsiTs102941CtlRequest containing a nitem of type EtsiTs102941CtlRequest containing lastKnownCtlSequence indicating Value higher than SN nen the IUT starts sending Secured GN messages containing an item of type ContributedExtensionBlock containing an item of type ContributedExtensionBlock containing contributedExtensions containing contributedExtensionBlock containing contributedExtensionBlock containing an item of type ContributedExtensionBlock containing an item of type ContributedExtensionBlock	Reference	
Expected behaviour The IUT is configured to support P2P Delta CTL distribution and the IUT contains valid TLM or/and RootCA certificate (CERT) and the IUT contains the CERT CTL information containing ctlSequence indicating (SN) re that then the IUT receives the Secured GN Message containing an item of type ContributedExtensionBlock containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing a item of type EtsiTs102941CtlRequest containing lastHownCtlSequence indicating Value higher than SN ten the IUT starts sending Secured GN messages containing an item of type ContributedExtensionBlock containing an item of type ContributedExtensionBlock containing a item of type ContributedExtensionBlock containing a starts sending Value higher than SN ten the IUT starts sending Secured GN messages containing an item of type ContributedExtensionBlock containing an item of type EtsiTs102941CtlRequest containing an item of type EtsiTs102941CtlRequest containing an item of type EtsiTs102941CtlRequest containing issuerId	Configuration	CFG_CXL_P2P
he IUT is configured to support P2P Delta CTL distribution and the IUT contains valid TLM or/and RootCA certificate (<i>CERT</i>) and the IUT contains the <i>CERT</i> CTL information containing ctlSequence indicating (<i>SN</i>) re that the IUT receives the Secured GN Message containing contributedExtensions containing an item of type ContributedExtensionBlock containing an item of type ContributedExtensionBlock containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the <i>CERT</i> and containing lastKnownCtlSequence indicating contributedExtensionBlock containing contributedExtension the IUT starts sending Secured GN messages containing contributedExtensionBlock containing contributedExtensionBlock containing issuerId the IUT starts sending Secured GN messages containing contributedExtensionBlock containing an item of type EtsiTs102941CtlRequest containing an item of type EtsiTs102941CtlRequest containing an item of type EtsiTs102941CtlRequest containing issuerId		
nd the IUT contains valid TLM or/and RootCA certificate (<i>CERT</i>) nd the IUT contains the <i>CERT</i> CTL information containing cllSequence indicating (<i>SN</i>) re that then the IUT receives the Secured GN Message containing contributedExtensions containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedIDB of the <i>CERT</i> and containing lastKnownCtlSequence indicating value higher than <i>SN</i> nen the IUT starts sending Secured GN messages containing contributedExtensions containing an item of type ContributedExtensionBlock containing an item of type ContributedExtensionBlock containing contributedExtensions containing an item of type ContributedExtensionBlock containing an item of type EtsiTs102941CtlRequest containing an item of type EtsiTs102941CtlRequest containing an item of type EtsiTs102941CtlRequest containing issuerId		Expected behaviour
nd the IUT contains valid TLM or/and RootCA certificate (<i>CERT</i>) nd the IUT contains the <i>CERT</i> CTL information containing cllSequence indicating (<i>SN</i>) re that then the IUT receives the Secured GN Message containing contributedExtensions containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedIDB of the <i>CERT</i> and containing lastKnownCtlSequence indicating value higher than <i>SN</i> nen the IUT starts sending Secured GN messages containing contributedExtensions containing an item of type ContributedExtensionBlock containing an item of type ContributedExtensionBlock containing contributedExtensions containing an item of type ContributedExtensionBlock containing an item of type EtsiTs102941CtlRequest containing an item of type EtsiTs102941CtlRequest containing an item of type EtsiTs102941CtlRequest containing issuerId	with	
nd the IUT contains the CERT CTL information containing ctlSequence indicating (SN) re that then the IUT receives the Secured GN Message containing contributedExtensions containing contributedExtensionBlock containing an item of type ContributedExtensionBlock containing a nitem of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value higher than SN the IUT starts sending Secured GN messages containing an item of type ContributedExtensionBlock containing contributedExtensions containing an item of type ContributedExtensionBlock containing an item of type ContributedExtensionBlock containing contributedExtensions containing an item of type ContributedExtensionBlock containing an item of type ContributedExtensionBlock containing an item of type EtsiTs102941CtlRequest containing an item of type EtsiTs102941CtlRequest containing issuerId		
<pre>containing ctlSequence indicating (SN) re that then the IUT receives the Secured GN Message containing contributedExtensions containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value higher than SN nen the IUT starts sending Secured GN messages containing contributedExtensions containing contributedExtensionBlock containing an item of type ContributedExtensionBlock containing issuerId</pre>		
<pre>indicating (SN) re that hen the IUT receives the Secured GN Message containing contributedExtensions containing an item of type ContributedExtensionBlock containing etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value higher than SN nen the IUT starts sending Secured GN messages containing an item of type ContributedExtensionBlock containing an item of type EtsiTs102941CtlRequest containing contributedExtensions containing an item of type ContributedExtensionBlock containing an item of type ContributedExtensionBlock containing an item of type ContributedExtensionBlock containing an item of type EtsiTs102941CtlRequest containing an item of type EtsiTs102941CtlRequest containing issuerId</pre>		
re that then the IUT receives the Secured GN Message containing contributedExtensions containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value higher than SN the IUT starts sending Secured GN messages containing contributedExtensions containing contributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId		
<pre>then the IUT receives the Secured GN Message containing contributedExtensions containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value higher than SN the IUT starts sending Secured GN messages containing contributedExtensionBlock containing an item of type EtsiTs102941CtlRequest containing an item of type EtsiTs102941CtlRequest containing an item of type EtsiTs102941CtlRequest containing issuerId</pre>	ensure that	(v)
the IUT receives the Secured GN Message containing contributedExtensions containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value higher than SN nen the IUT starts sending Secured GN messages containing contributedExtensionBlock containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing an item of type EtsiTs102941CtlRequest containing issuerId	when	
<pre>containing contributedExtensions containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value higher than SN nen the IUT starts sending Secured GN messages containing contributedExtensions containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId</pre>		s the Secured GN Message
<pre>containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value higher than SN nen the IUT starts sending Secured GN messages containing contributedExtensions containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId</pre>		
<pre>containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value higher than SN nen the IUT starts sending Secured GN messages containing contributedExtensions containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId</pre>		
containing an item of type EtsiTs102941CtlRequest containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value higher than SN nen the IUT starts sending Secured GN messages containing contributedExtensions containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId		
<pre>containing issuerId indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value higher than SN een the IUT starts sending Secured GN messages containing contributedExtensions containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId</pre>	in	dicating etsiHeaderInfoContributorId (2)
indicating HashedID8 of the CERT and containing lastKnownCtlSequence indicating value higher than SN the IUT starts sending Secured GN messages containing contributedExtensions containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId	conta	ining an item of type EtsiTs102941CtlRequest
and containing lastKnownCtlSequence indicating value higher than <i>SN</i> the IUT starts sending Secured GN messages containing contributedExtensions containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId	CC	ontaining issuerId
indicating value higher than SN nen the IUT starts sending Secured GN messages containing contributedExtensions containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId		indicating HashedID8 of the CERT
<pre>hen the IUT starts sending Secured GN messages containing contributedExtensions containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId</pre>	a	nd containing lastKnownCtlSequence
the IUT starts sending Secured GN messages containing contributedExtensions containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId		indicating value higher than SN
<pre>containing contributedExtensions containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId</pre>	then	
<pre>containing an item of type ContributedExtensionBlock containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId</pre>		· ·
<pre>containing contributorId indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId</pre>	•	
indicating etsiHeaderInfoContributorId (2) containing an item of type EtsiTs102941CtlRequest containing issuerId		
containing an item of type EtsiTs102941CtlRequest containing issuerId	8	
containing issuerId	-	
indicating HaghadTD9 of the CEPT		C
indicating HashedID8 of the CERT		•
and containing lastKnownCtlSequence indicating SN	a	
· ·	NOTE: This TP is a	· ·

48

TP ld	SECPKI_ITS-S_CTLDIST_08_BV
Summary	Check that the IUT starts broadcasting the Delta CTL when request is received using P2P
	protocol
Reference	ETSI TS 103 601 [6], clause 5.3.6
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-06.2
	Expected behaviour
with	
the IUT is configur	ed to support P2P Delta CTL distribution
and the IUT contain	ins valid TLM or/and RootCA certificate (<i>CERT</i>)
	eceived a Delta CTL message (<i>M</i>)
signed using C	CERT CONTRACT
and containing	ctlSequence
indicating (SN)
ensure that	
when	
the IUT receive	es the Secured Message
containing	contributedExtensions
containi	ing an item of type EtsiTs102941CtlRequest
cont	taining issuerId
i	ndicating HashedID8 of the CERT
and	containing lastKnownCtlSequence
	indicating value less than SN
then	•
the IUT starts I	broadcasting the Delta CTL (<i>M</i>)
	applied for both: ECTL and RootCA CTL handling behaviour.

TP ld	SECPKI_ITS-S_CTLDIST_09_BV
Summary	Check that the IUT stops broadcasting the Delta CTL when broadcasting period is expired
Reference	ETSI TS 103 601 [6], clause 5.3.6
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-06.2
	Expected behaviour
with	
the IUT is configured to	support P2P Delta CTL distribution
and the IUT is configure	d to broadcast the Delta CTL during D1 time
and the IUT has started	to broadcast a Delta CTL message
at the time T	v
ensure that	
when	
the IUT local time is	reached the T + D1
then	
the IUT stops broad	casting the Delta CTL
NOTE 1: This TP is applie	d for both: ECTL and RootCA CTL handling behaviour.
NOTE 2: The D1 value sh	

TP ld	SECPKI_ITS-S_CTLDIST_10_BV
Summary	Check that the IUT stops broadcasting the requested Delta CTL when broadcasting period
	is expired
Reference	ETSI TS 103 601 [6], clause 5.3.6
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-06.2
	Expected behaviour
and the IUT is con and the IUT has st at the time T ensure that when the IUT local tir then	ed to support P2P Delta CTL distribution figured to broadcast the requested Delta CTL during $D2$ time arted to broadcast a Delta CTL message me is reached the $T + D2$
the IUT stops b	proadcasting the Delta CTL
	applied for both: ECTL and RootCA CTL handling behaviour.
NOTE 2: The D2 value	ue shall be provided as a PIXIT.

5.2.6 CRL handling

TP ld	SECPKI_ITS-S_CRL_01_BV
Summary	Check that the IUT accept the received CRL information
Reference	ETSI TS 102 941 [1], clause 5.4.2
Configuration	CFG_CXL_P2P
PICS Selection	
	Expected behaviour
with	
the IUT contains va	alid RootCA certificate (CERT_IUT_A_RCA)
and the IUT has no	of received yet the CRL information issued by the RootCA
ensure that	
when	
the IUT receive	d the CRL information from the DC
then	
the IUT accepts	s the received CRL

TP ld	SECPKI_ITS-S_CRL_02_BV	
Summary	Check that the IUT can handle the revocation of its own AA	
Reference	ETSI TS 102 941 [1], clause 5.4.2	
Configuration	CFG_CXL_P2P	
PICS Selection		
	Expected behaviour	
and the IUT is auth signed with CE ensure that when the IUT receive containing r then	alid RootCA certificate (CERT_IUT_A_RCA) norized using AT certificate RT_IUT_A_B_AA ed the CRL information from the DC evocation of CERT_IUT_A_B_AA ed to 'enrolled' state	

TP ld	SECPKI_ITS-S_CRL_03_BV
Summary	Check that the IUT can handle the revocation of its own EA
Reference	ETSI TS 102 941 [1], clause 5.4.2
Configuration	CFG_CXL_P2P
PICS Selection	
	Expected behaviour
and the IUT been e signed with CE ensure that when the IUT the IUT containing r then	rized' state ns valid RootCA certificate (CERT_IUT_A_RCA) enrolled with EC certificate RT_IUT_A_EA certificate - received the CRL information from the DC revocation of CERT_IUT_A_EA es to the 'initial' state

TP ld	SECPKI_ITS-S_CRL_04_BV
Summary	Check that the IUT can handle the revocation of its own RootCA
Reference	ETSI TS 102 941 [1], clause 5.4.2
Configuration	CFG_CXL_P2P
PICS Selection	
	Expected behaviour
with	
the IUT is in 'authorized'	
and the IUT contains va	lid RootCA certificate (CERT_IUT_A_RCA)
and the IUT been enrolle	ed with EC certificate
signed with EA certif	icate
signed with CER	T_IUT_A_RCA
ensure that	
when	
the IUT the IUT rece	ived the CRL information from the DC
containing revoca	ation of CERT_IUT_A_RCA
then	
the IUT switches to t	he 'initial' state

TP ld	SECPKI_ITS-S_CRL_05_BV
Summony	Check that the IUT skips incoming messages when revoked AA certificate is in the signing
Summary	chain of the current AT certificate
Reference	ETSI TS 102 941 [1], clause 5.4.2
Configuration	CFG_CXL_P2P
PICS Selection	
	Expected behaviour
with	
	lid RootCA certificate (CERT_IUT_A_RCA)
and the IUT has not rec	eived yet the CRL information issued by the RootCA
and the IUT is authorize	d using AT certificate
signed with CERT_I	UT_A_AA
and the IUT contains an	other AA certificate (CERT IUT A B AA)

and the IUT contains another AA certificate (CERT_IUT_A_B_AA) and the IUT has already accepted messages signed with AT certificate signed with CERT_IUT_A_B_AA

and the IUT received the CRL information from the DC containing revocation of CERT_IUT_A_B_AA

ensure that

when the IUT receives a Secured Message

signed with AT certificate

signed with CERT_IUT_A_B_AA

then

the IUT discards this message

5.2.7 CRL distribution

TP ld	SECPKI_ITS-S_CRLDIST_01_BV
Summary	Check that the IUT starts broadcasting the CRL using P2P protocol when CRL information
Summary	is received
Reference	ETSI TS 103 601 [6], clause 5.4.2
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-07.2
	Expected behaviour
with	
the IUT is configured to	support P2P CRL distribution
and the IUT contains va	alid RootCA certificate (CERT_IUT_A_RCA)
and the IUT has not rec	eived yet the CRL information issued by the RootCA
ensure that	
when	
the IUT received the	e CRL information from the DC
containing this	Update (7)
and containing r	extUpdate (N)
then	
the IUT starts broad	casting the received CRL

TP Id	SECPKI_ITS-S_CRLDIST_02_BV
Summary	Check that the IUT is using the proper BTP port to broadcast the CRL
Reference	ETSI TS 103 601 [6], clause 5.4.4
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-07.2
	Expected behaviour
and the IUT contains val and the IUT has not rece ensure that when the IUT is triggered to then	ertificateRevocationListMessage

TP ld	SECPKI_ITS-S_CRLDIST_02_BV
Summary	Check that the IUT stops broadcasting the CRL when distribution time (d1) has been
	expired after receiving of CRL information
Reference	ETSI TS 103 601 [6], clauses 5.4.2 and 5.4.3
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-07.2
	Expected behaviour
with	
the IUT is configu	red to support P2P CRL distribution
and the IUT conta	ins valid RootCA certificate (CERT_IUT_A_RCA)
and the IUT has a	Iready received the CRL information from DC
at the time T	
and the IUT has s	tarted broadcasting the received CRL
and the IUT is cor	nfigured to limit the broadcasting time to <i>D1</i>
ensure that	
when	
the IUT currer	t time is equal or more than T + D1
then	
the IUT stops	broadcasting the CRL
NOTE: The D1 va	ue shall be provided as a PIXIT.

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

TP ld	SECPKI_ITS-S_CRLDIST_04_BV	
	Check that the IUT stops broadcasting the CRL when another station starts to broadcast	
Summary	the same or more recent CRL	
Reference	ETSI TS 103 601 [6], clause 5.4.3	
Configuration	CFG_CXL_P2P	
PICS Selection	UC-SEC-07.2	
	Expected behaviour	
with		
the IUT is configur	ed to support P2P CRL distribution	
and the IUT contai	ns valid RootCA certificate (CERT_IUT_A_RCA)	
and the IUT has al	ready received the CRL	
containing this	Jpdate (T)	
and the IUT has st	and the IUT has started broadcasting the received CRL	
ensure that		
when		
the IUT receives the CRL signed by CERT_IUT_A_RCA		
containing t	containing thisUpdate	
indicatir	indicating the value equal or greater than $\boldsymbol{\tau}$	
then		
the IUT stops broadcasting the CRL		

TP ld	SECPKI_ITS-S_CRLDIST_04_BV
Summary	Check that the IUT skips the lastKnownUpdate field in the P2P CRL request when no CRL
	information has been previously available
Reference	ETSI TS 103 601 [6], clause 5.3.4.2
Configuration	CFG_CXL_P2P
PICS Selection	UC-SEC-08.1
	Expected behaviour
with	
the IUT is configur	ed to support P2P CRL distribution
and the IUT conta	ins valid RootCA certificate (CERT_IUT_A_RCA)
and the IUT has n	ever received a CRL information issued by the RootCA
ensure that	
when	
the IUT is trigg	ered to request the CRL
then	
the IUT starts	sending Secured GN messages
containing	contributedExtensions
contain	ing an item of type ContributedExtensionBlock
cont	aining contributorId
i	ndicating etsiHeaderInfoContributorId (2)
	aining an item of type EtsiTs102941CrlRequest
	containing issuerId
	indicating HashedID8 of the CERT_IUT_A_RCA
	and not containing lastKnownUpdate

TP ld	SECPKI_ITS-S_CRLDIST_05_BV	
	Check that the IUT includes the lastKnownUpdate information in the P2P CRL request if	
	the CRL information was previously available	
Reference	ETSI TS 103 601 [6], clause 5.3.4.2	
Configuration	CFG_CXL_P2P	
PICS Selection	UC-SEC-08.1	
	Expected behaviour	
with		
	to support P2P CRL distribution	
	valid RootCA certificate (CERT_IUT_A_RCA)	
and the IUT has alread	ady received the CRL information issued by the RootCA	
containing thist	Jpdate (7)	
ensure that		
when		
the IUT is triggere	ed to request the CRL	
then		
	nding Secured GN messages	
containing contributedExtensions		
	an item of type ContributedExtensionBlock	
contair	ning contributorId	
indicating etsiHeaderInfoContributorId (2)		
contair	ning an item of type EtsiTs102941CrlRequest	
cor	containing issuerId	
	indicating HashedID8 of the CERT_IUT_A_RCA	
and	containing lastKnownUpdate	
	indicating T	

TP ld	SECPKI_ITS-S_CRLDIST_06_BV	
Summen	Check that the IUT starts broadcasting the CRL using P2P protocol when CRL information	
Summary	has been requested by another ITS station	
Reference	ETSI TS 103 601 [6], clause 5.4.2	
Configuration	CFG_CXL_P2P	
PICS Selection	UC-SEC-08.2	
	Expected behaviour	
with		
the IUT is configured to	support P2P CRL distribution	
and the IUT contains val	lid RootCA certificate (CERT_IUT_A_RCA)	
and the IUT has already	received the CRL information issued by the RootCA	
and the IUT has already	and the IUT has already stopped broadcasting the CRL information	
ensure that		
when		
the IUT received the CRL request information issued by the RootCA		
not containing thislastKnownUpdate		
then		
the IUT starts broade	casting the received CRL	

TP ld	SECPKI_ITS-S_CRLDIST_06_BV	
Summany	Check that the IUT stops broadcasting the CRL when distribution time (d2) has been	
Summary	expired after receiving of CRL request	
Reference	ETSI TS 103 601 [6], clause 5.4.2	
Configuration	CFG_CXL_P2P	
PICS Selection	UC-SEC-08.2	
	Expected behaviour	
with		
the IUT is config	ured to support P2P CRL distribution	
and the IUT cont	ains valid RootCA certificate (CERT IUT A RCA)	
and the IUT has	and the IUT has already received the CRL information request	
at the time T		
and the IUT has	and the IUT has started broadcasting the CRL	
	onfigured to limit the broadcasting time to D2	
ensure that		
when		
WIIGH		
	nt time is equal or more than T+D1	
	nt time is equal or more than T+D1	
the IUT curre	nt time is equal or more than T+D1 broadcasting the CRL	

5.3 Common CA behaviour

5.3.0 Overview

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

PICS_SECPKI_IUT_RCA = TRUE; or

PICS_SECPKI_IUT_AA = TRUE; or

 $PICS_SECPKI_IUT_EA = TRUE.$

5.3.1 Certificate validation

5.3.1.1 Basic certificate content

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

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

TP ld	SECPKI_CA_CERTGEN_02_BV_02
Summary	Check that the CA, been authorized using explicit certificate, is able to issue an implicit certificate
Reference	ETSI TS 103 097 [2], clause 6 IEEE Std 1609.2™ [3], clause 6.4.3
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_IMPLICIT_CERTIFICATES AND PICS_SEC_EXPLICIT_CERTIFICATES
	Expected behaviour
with CA is in 'operationa CA is initialized wit ensure that when	al' state th the explicit certificate (CERT_IUT_A_CA)
the CA is reque	ested to issue the AT certificate ne butterfly key expansion mechanism
then this certificate i containing v indicatir	is of type EtsiTs103097Certificate

indicating 3 containing type indicating 'implicit' and containing toBeSigned containing verifyKeyIndicator containing reconstructionValue and not containing signature

TP ld	SECPKI_CA_CERTGEN_02_BV_03
Summary	Check that the CA, been authorized using implicit certificate, is able to issue an implicit
	certificate
Reference	ETSI TS 103 097 [2], clause 6
Reference	IEEE Std 1609.2 [™] [3], clause 6.4.3
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_IMPLICIT_CERTIFICATES
	Expected behaviour
with	
CA is in 'operation	al' state
CA is initialized wi	th the implicit certificate (CERT_IUT_I_CA)
ensure that	
when	
the CA is requ	ested to issue the AT certificate
using th	ne butterfly key expansion mechanism
then	
this certificate	is of type EtsiTs103097Certificate
containing	version
indicati	ng 3
containing	type
indicati	ng 'implicit'
	ning toBeSigned
contain	ing verifyKeyIndicator
con	taining reconstructionValue
and not co	ntaining signature

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

the CA does not issue the certificate

TRU	
TP ld	SECPKI_CA_CERTGEN_03_BV
Summary	Check that CA issues certificate conformed to ETSI TS 103 097 [2], clause 6
Reference	ETSI TS 103 097 [2], clause 6
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
CA is in 'operational'	state
ensure that	
when	
the CA is issuing	he certificate
then	
this certificate is c	f type EtsiTs103097Certificate
containing toB	eSigned
containing	
indicati	ng 'none' or 'name'
and contai	ning cracald
indicati	ng '000000'H
and containing crlSeries	
indicating '0'D	
	ntaining certRequestPermissions
and not co	ntaining canRequestRollover

TP	d	SECPKI CA (CERTGEN_04_BV_X		
Summary			Check that the issuer of certificates is referenced using digest		
			Check that right digest field is used to reference to the certificate		
Ref	erence		.2™ [3], clause 6.4.3		
PIC	S Selection		CURITY AND X_PICS		
			Expected behavio	ur	
with					
(CA is in 'operational'	state			
i	and CA is authorized	with CA certificate	C_ISSUER		
	ure that				
1	when				
		the explicit certifica	te		
1	hen				
		of type EtsiTs1030	97Certificate		
	containing iss				
		X_DIGEST			
				calculated using X_ALGORITHM	
		erenced to certifica	te C_ISSUER		
	and containin				
		verifyKeyIndicator			
		ning verificationKey	/		
	COI	ntaining X_KEY	Permutation table	~	
Х	V DICEST				
^	X_DIGEST	X_ALGORITHM	X_KEY	X_PICS	
А	sha256AndDigest	SHA-256	ecdsaNistP256 or	PICS_SEC_SHA256	
			ecdsaBrainpoolP256r1	AND PICS_SEC_BRAINPOOL_P256R1	
В	sha384AndDigest	SHA-384	ecdsaBrainpoolP384r1	PICS_SEC_SHA384 AND	
	J			PICS_SEC_BRAINPOOL_P384R1	

5.3.1.2 Check certificate region validity restriction

TP ld	SECPKI_CA_CERTGEN_05_BV		
Summary	Check that the CA is able to issue the certificate with the well-formed circular region validity restriction		
Summary			
Reference	IEEE Std 1609.2 [™] [3], clauses 6.4.20, 6.4.17 and 5.1.2.4		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_CIRCULAR_REGION		
	Expected behaviour		
with			
CA is in 'operationa	al' state		
the CA is authorize	d with CA certificate		
containing toBe	Signed		
containing r	egion		
indicatin	gREGION		
ensure that			
when			
the CA is reque	sted to issue the certificate		
containing o	ircular region restriction		
then			
the CA issues t	he certificate of type EtsiTs103097Certificate		
containing t	oBeSigned		
containi	ng region		
cont	aining circularRegion		
C	ontaining centre		
	indicating a point inside the REGION		
a	nd containing radius		
	indicating a value when all points of the circle are inside the REGION		

TP ld	SECPKI_CA_CERTGEN_06_BV		
Summany	Check that the CA is able to issue the certificate with the well-formed rectangular region validity restriction		
Summary			
Reference	IEEE Std 1609.2 [™] [3], clauses 6.4.20, 6.4.17 and 5.1.2.4		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_RECTANGULAR_REGION		
	Expected behaviour		
with			
CA is in 'operation	al' state		
the CA is authorize	ed with CA certificate		
containing toB			
containing	region		
indicatir	ng REGION		
ensure that			
when			
	ested to issue the certificate		
	rectangular region restriction		
then			
	the certificate of type EtsiTs103097Certificate		
	toBeSigned		
	ng region		
	aining rectangularRegion		
(containing items of type RectangularRegion		
	containing northwest		
	indicating a point inside the REGION		
	and containing southeast		
	indicating a point on the south and east from northwest and inside the REGION		

TP ld	SECPKI_CA_CERTGEN_07_BV			
	Check that CA is able to issue certificate with polygonal region validity restriction where:			
	 the polygonal certificate validity region contains at least three points 			
Summary	 the polygonal certificate validity region does not contain intersections 			
	the polygonal certificate validity region is inside the validity region of the issuing			
	certificate			
Reference	IEEE Std 1609.2 [™] [3], clauses 6.4.21, 6.4.17 and 5.1.2.4			
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_POLYGONAL_REGION			
	Expected behaviour			
with				
CA is in 'operational' sta				
the CA is authorized wit				
containing toBeSign				
containing region				
indicating RE	GION			
ensure that				
when				
•	to issue the certificate			
0	onal region validity restriction			
then	artificate of turne EtaiTe102007Certificate			
containing toBeS	ertificate of type EtsiTs103097Certificate			
containing tobec				
	g polygonalRegion			
	ining more than 2 items of type TwoDLocation			
	dicating points inside the REGION			
	indicating unintercepting segments			

TP ld	SECPKI_CA_CERTGEN_08_BV		
	Check that the CA is able to issue the certificate with identified region validity restriction		
Summary	contains values that correspond to numeric country codes as defined by United Nations		
	Statistics Division [i.8]		
Reference	IEEE Std 1609.2™ [3], clause 6.4.23		
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_IDENTIFIED_REGION		
	Expected behaviour		
with			
CA is in 'operationa			
the CA is authorized			
containing toBe			
containing re			
	REGION		
ensure that			
when			
	sted to issue the certificate		
0	lentified region validity restriction		
	g country or area COUNTRY		
then	an antificate of time Etailor 102007 Cartificate		
containing to	ne certificate of type EtsiTs103097Certificate		
containing to			
	ining identifiedRegion		
	ontaining 1 entry of type IdentifiedRegion		
	containing countryOnly		
	indicating integer representation of the identifier of country or area COUNTRY		
	or containing countryAndRegions		
	containing countryOnly		
	indicating integer representation of the identifier of country or area COUNTRY		
	or containing countryAndSubregions		
	containing country		
	indicating integer representation of the identifier of country or area COUNTRY		

TP ld	SECPKI_CA_CERTGEN_09_BV	
_	Check that the identified region validity restriction of the subordinate certificate is included	
Summary	in the identified region validity restriction of the issuing certificate	
Reference	IEEE Std 1609.2 [™] [3], clauses 6.4.17 and 5.1.2.4	
PICS Selection PICS_GN_SECURITY AND PICS_SEC_IDENTIFIED_REGION		
	Expected behaviour	
with		
the CA is in 'operationa	I' state	
and the CA is authorize		
containing toBeSigr	ned	
containing regio		
	lentifiedRegion	
	ig countryOnly	
	ating COUNTRY	
	ning countryAndRegions	
conta	ining countryOnly	
	dicating COUNTRY	
	containing regions	
	dicating REGIONS ning countryAndSubregions	
	aining country	
	indicating COUNTRY	
	containing regionAndSubregions	
	ndicating REGIONS and SUBREGIONS	
ensure that	······································	
when		
the CA issued the c	ertificate	
containing toBe	Signed	
containing re	egion	
containin	g identifiedRegion	
then		
	type EtsiTs103097Certificate	
containing toBe	•	
containing re		
	ig identifiedRegion	
	dicating value = COUNTRY	
	ntaining countryAndRegions	
	ontaining countryOnly	
	indicating value = COUNTRY	
ar	nd containing regions	
	containing region identifiers contained in REGIONS	
	ntaining countryAndSubregions	
	ontaining country	
	indicating value = COUNTRY	
a	nd containing regionAndSubregions	
	containing region identifiers contained in REGIONS	
	and containing subRegion identifiers contained in SUBREGIONS for every region	

TP Id	1	SECPKI_CA_ CERTGEN_10_BV_ XX
		Check that the certificate signature contains ECC point of type set to either
Sum	nmary	compressed_lsb_y_0, compressed_lsb_y_1 or x_coordinate_only
Defe		
	rence	IEEE Std 1609.2 [™] [3], clauses 6.3.29, 6.3.30 and 6.3.31
PICS	Selection	PICS_GN_SECURITY AND PICS_SEC_EXPLICIT_CERTIFICATES AND X_PICS
		Expected behaviour
with		
th	e CA is in 'operational'	state
ensu	re that	
w	hen	
	the CA issued the ex	olicit certificate
th	en	
	this certificate is of ty	pe EtsiTs103097Certificate
	containing signat	Ire
	containing X_	SIGNATURE
	containing	rSig
	containi	ig x-only
		ning compressed-y-0
		ning compressed-y-1
		Permutation table
XX	X_SIGNATURE	X_PICS
Α	ecdsaNistP256Signatu	re
В	ecdsaBrainpoolP256r1	Signature PICS_SEC_BRAINPOOL_P256R1
	ecdsaBrainpoolP384r1	•

5.3.1.3 Check ECC point type of the certificate signature

5.3.1.4 Check ECC point type of the certificate public keys

TP ld		SECPKI CA CERTGEN 11 BV		
_	-	Check that the certificate verification key contains ECC point of type set to either		
Summa	ry	compressed_lsb_y_0, compressed_lsb_y_1 or uncompressed		
Referen	ice	IEEE Std 1609.2 [™] [3], clause 6.4.38		
PICS Se	election	PICS_GN_SECURITY AND PICS_SEC_EXPLICIT_CERTIFICATES AND X_PICS		
		Expected behaviour		
with		·		
the C	CA is in 'operational'	state		
ensure t	hat			
wher	n			
th	he CA issued the ex	plicit certificate		
then				
th	his certificate is of ty	pe EtsiTs103097Certificate		
	containing toBeS	igned		
	containing ver	rifyKeyIndicator		
	containing	verificationKey		
	contair	ning X_KEY		
		aining uncompressed		
		intaining compressed-y-0		
		intaining compressed-y-1		
		Permutation table		
XX X_	KEY	X_PICS		
A ecc	dsaNistP256			
B ecc	dsaBrainpoolP256r1	PICS_SEC_BRAINPOOL_P256R1		
C ecc	dsaBrainpoolP384r1	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1		

TP lo	J			
IPIC	1	SECPKI_CA_CERTGEN_12_BV		
Sum	mary	Check that the certificate encryption key contains ECC point of type set to either		
Summary		compressed_lsb_y_0, compressed_lsb_y_1 or uncompressed		
Refe	rence	IEEE Std 1609.2™ [3], clause 6.4.38		
PICS	Selection	PICS_GN_SECURITY		
		Expected behaviour		
with				
th	ne CA is in 'operational'	state		
ensu	re that			
w	/hen			
	the CA issued the ce	rtificate		
th	nen			
	this certificate is of ty	/pe EtsiTs103097Certificate		
	containing toBeS	igned		
	containing en	cryptionKey		
	containing	publicKey		
	contai	ning X_KEY		
	cont	aining uncompressed		
	or co	ontaining compressed-y-0		
	or co	ontaining compressed-y-1		
		Permutation table		
XX	X_KEY	X_PICS		
Α	eciesNistP256			
В	eciesBrainpoolP256r1	PICS SEC BRAINPOOL P256R1		

5.3.1.5 Verify certificate signatures

TP Id	S	ECPKI_CA_CERTGEN_13_BV_01		
Summary Check the explicit certificate signature				
Reference				
PICS Selec			EXPLICIT_CERTIFICATES AND X_PICS	
		Expected behaviou		
with				
the CA	is in 'operational' st	ate		
		vith explicit certificate		
	aining toBeSigned			
	containing verifyKe			
	containing verifi			
	containing X	(_KEY		
ensure that				
when		init nortificato		
	CA issued the expli			
then	aartificata is of turo	EtaiTa102007Cartificata		
	containing issuer	e EtsiTs103097Certificate		
	referencing the	cortificato		
	containing to			
		g verifyKeyIndicator		
		aining verificationKey		
		ontaining X_KEY		
		indicating KEY		
	and containing sign			
	containing X_SI			
	verifiable us			
		Permutation table		
XX X_KE	Y	X_SIGNATURE	X_PICS	
A ecdsa	NistP256	ecdsaNistP256Signature		
B ecdsa	BrainpoolP256r1	ecdsaBrainpoolP256r1Signature	PICS_SEC_BRAINPOOL_P256R1	
C ecdsa	BrainpoolP384r1	ecdsaBrainpoolP384r1Signature	PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1	

TP ld	SECPKI_CA_CERTGEN_13_BV_02	
Summary	Check the explicit certificate signature	
Reference	ETSI TS 103 097 [2], clause 6	
PICS Selection	PICS_GN_SECURITY AND PICS_SEC_EXPLICIT_CERTIFICATES AND X_PICS	
	Expected behaviour	
with		
the CA is in 'op	perational' state	
	authorized with explicit certificate	
containing t		
	ing verifyKeyIndicator	
	taining verificationKey	
C	containing X_KEY	
	indicating KEY	
	ued the implicit certificate of type EtsiTs103097Certificate (CERT)	
	ing signature	
and contain		
	cing the certificate	
	taining toBeSigned	
C	containing verifyKeyIndicator	
	containing reconstructionValue	
ensure that	indicating VALUE	
when		
	alculated the digital signature	
	ne private key associated with the CERT	
then		
	ire can be verified using public key	
•	ructed using VALUE and KEY	
	Permutation table	
XX X_KEY	X_PICS	
A ecdsaNistP25		
B ecdsaBrainpo	oolP256r1 PICS_SEC_BRAINPOOL_P256R1	
C ecdsaBrainpoolP384r1 PICS_SEC_SHA384 AND PICS_SEC_BRAINPOOL_P384R1		

5.3.1.6 Verify certificate permissions

TP ld	SECPKI_CA_CERTGEN_14_BV
Summary	Check that all PSID entries of the appPermissions component of the certificate are unique
Reference	IEEE Std 1609.2 [™] [3], clauses 6.4.28 and 5.1.2.4
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the CA is in 'opera	tional' state
ensure that	
when	
the CA issued	the certificate
containing t	oBeSigned
containi	ng appPermissions
then	
this certificate i	s of type EtsiTs103097Certificate
containing t	oBeSigned
containi	ng appPermissions
cont	aining items of type PsidSsp
	containing psid
	indicating unique values in this sequence

TP ld	SECPKI_CA_CERTGEN_15_BV	
Summen	Check that all PSID entries of the appPermissions component of the certificate are also	
Summary	contained in the certIssuePermissions component in the issuing certificate	
Reference	IEEE Std 1609.2™ [3], clauses 6.4.28 and 5.1.2.4	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the CA is in 'operati	ional' state	
ensure that		
when		
the CA issued the		
containing toBeSigned		
containing appPermissions		
then		
	s of type EtsiTs103097Certificate	
containing is		
	ed to the certificate	
	aining toBeSigned	
C	ontaining certIssuePermissions	
	containing items of type PsidGroupPermissions	
	containing eeType	
	indicating app(0)	
	and containing subjectPermissions	
	containing explicit	
containing items of type PsidSspRange		
indicating X_PSID_RANGE_LIST or containing all		
and containing toBeSigned		
containing appPermissions		
containing apprentissions		
	containing psid	
	contained in the X_PSID_RANGE_LIST	
	as a psid	

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

TP ld	SECPKI_CA_CERTGEN_17_BV
Summary	Check that SSP field in each entry of the appPermissions component of the AT certificate
	is equal to or a subset of the SSP Range in the corresponding issuing entry
Reference	IEEE Std 1609.2™ [3], clauses 6.4.28 and 5.1.2.4
PICS Selection	PICS_GN_SECURITY
	Expected behaviour
with	
the CA is in 'operational	l' state
ensure that	
when	
the CA issued the cert	lificate
containing toBeSigr	
containing appPermissions	
then	
this certificate is of type EtsiTs103097Certificate	
containing issuer	
referenced to the	
containing toB	
	ertIssuePermissions
	g items of type PsidGroupPermissions
	ning eeType
	cating app(0)
	ntaining subjectPermissions
	aining explicit
cc	ontaining items of type PsidSspRange
containing psid	
indicating X_PSID_AA	
containing sspRange	
indicating X_SSP_AA [X_PSID_AA]	
or containing all	
containing toBeSigned	
containing appPe	
	ns of type PsidSsp
containing p	
	value equal to X_PSID_AA
containing s	
indicating	value permitted by X_SSP_AA [X_PSID_AA]

TP Id	SECONI CA CEDICEN 18 BV	
	SECPKI_CA_CERTGEN_18_BV	
Summary	Check that the validityPeriod of the subordinate certificate is inside the validityPeriod of the	
	issuing certificate	
Reference	IEEE Std 1609.2™ [3], clause 5.1.2.4	
PICS Selection	PICS_GN_SECURITY	
	Expected behaviour	
with		
the CA is in 'operational' s	state	
and the CA is authorized	with CA certificate	
containing toBeSigned		
containing validityPeriod		
containing start		
indicating X_START_VALIDITY_CA		
containing duration		
indicating X_DURATION_CA		
ensure that		
when		
the IUT issued the certificate		
then		
this certificate is of type EtsiTs103097Certificate		
containing toBeSigned		
containing validityPeriod		
containing start		
indicating X_START_VALIDITY (X_START_VALIDITY >= X_START_VALIDITY_CA)		
containing duration		
indicating value <= X_START_VALIDITY_CA + X_DURATION_CA - X_START_VALIDITY		

5.3.1.7 Check time validity restriction in the chain

5.4 EA behaviour

5.4.0 Overview

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

PICS_SECPKI_IUT_EA = TRUE

5.4.1 Enrolment request handling

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

TP ld	
	SECPKI_EA_ENR_RCV_02_BI Check that EA does not accept Enrolment rekeying request when enrolment is not
Summary	
Deference	permitted by signing certificate
Reference	ETSI TS 102 941 [1], clause B.5
Configuration	CFG_ENR_EA
PICS Selection	E-marked backgroup
	Expected behaviour
with	
the EA is in 'operationa	al' state
ensure that	
when	
	n EnrollmentRequestMessage
	ncrypted EtsiTs103097Data-Signed
containing s containing	
	ng Hashedld8 value
	enced the certificate (CERT)
	ontaining appPermissions
	not containing an item of type PsidSsp
	containing psid
	indicating AID_CERT_REQ
	or containing an item of type PsidSsp
	containing psid
	indicating AID_CERT_REQ
	and containing ssp
	containing opaque[0] (version)
	indicating other value than 1
	or containing opaque[1] (value)
	indicating 'Enrolment Request' (bit 1) set to 0
then	
	th an EnrollmentResponseMessage
containing InnerE	
containing resp	
indicating 'c	leniedpermissions'

TP ld	SECPKI EA ENR RCV 04 BI	
Summary	Enroll an ITS-Station, but the outer signature, created with the canonical private key,	
	cannot be verified with the registered canonical public key	
Reference	ETSI TS 102 941 [1], clause B.5	
Configuration	CFG_ENR_EA	
PICS Selection		
	Expected behaviour	
with		
the EA is in 'opera	the EA is in 'operational' state	
ensure that		
when		
the IUT receives an EnrollmentRequestMessage		
containing an outer signature		
signed with an unknown canonical private key		
then		
the IUT answers with an EnrollmentResponseMessage		
containing InnerECResponse		
containing responseCode		
indicating 'invalidsignature'		
and not containing a certificate		

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

TP Id	SECPKI EA ENR RCV 06 BI	
Summary	Enroll the ITS-Station, but the CSR requests more permissions than the issuer allows,	
	i.e. request for security management SSP bit which is not set in the EA SSP	
Reference	ETSI TS 102 941 [1], clause B.5	
Configuration	CFG_ENR_EA	
PICS Selection		
	Expected behaviour	
with		
the EA is in 'operational'	state	
ensure that		
when		
the IUT receives an EnrollmentRequestMessage		
containing an InnerEcRequest		
9	containing SSP	
	more permissions than EA allows	
then		
the IUT answers with an EnrollmentResponseMessage		
containing InnerECResponse		
containing responseCode		
indicating 'deniedpermissions'		
and not containing a certificate		

TP ld	SECPKI_EA_ENR_RCV_07_BI
Summary	Enroll the ITS-Station, but the CSR requests an AID permission that the issuer does not
	allow
Reference	ETSI TS 102 941 [1], clause B.5
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
with	
the EA is in 'opera	tional' state
ensure that	
when	
the IUT receives an EnrollmentRequestMessage	
	an InnerEcRequest
contain	5
cont	aining an AID permission not authorized by EA
then	
	rs with an EnrollmentResponseMessage
containing InnerECResponse	
containing responseCode	
indicating 'deniedpermissions'	
and not containing a certificate	

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

TP ld	SECPKI_EA_ENR_RCV_09_BI		
Summary	Enroll the ITS-Station, but the start date of the CSR is before the start date of the EA		
Reference	ETSI TS 102 941 [1], clause B.5		
Configuration	CFG_ENR_EA		
PICS Selection			
Expected behaviour			
with			
the EA is in 'operational' state			
ensure that			
when			
the IUT receives an EnrollmentRequestMessage			
containing an InnerEcRequest			
containing ValidityPeriod			
containing start date			
indicating a value less than the start date of the EA			
then			
the IUT answers with an EnrollmentResponseMessage			
containing InnerECResponse			
containing responseCode			
indicating 'deniedpermissions'			
and not containing a certificate			

TP ld	SECPKI_EA_ENR_RCV_10_BI		
Summary	Enroll the ITS-Station, but expiring date of the CSR is after the expiring date of the EA		
Reference	ETSI TS 102 941 [1]		
Configuration	CFG_ENR_EA		
PICS Selection			
Expected behaviour			
with			
the EA is in 'operational'	state		
ensure that			
when			
the IUT receives an	the IUT receives an EnrollmentRequestMessage		
containing an Inn	erEcRequest		
containing Va	containing ValidityPeriod		
indicating a value greater than the ValidityPeriod of the EA			
then	5 <i>y</i>		
the IUT answers with an EnrollmentResponseMessage			
containing InnerECResponse			
containing responseCode			
indicating 'deniedpermissions'			
and not containing a certificate			

TP ld	SECPKI EA ENR RCV 11 BI		
Summary	Enroll the ITS-Station, but the start date of the CSR is after the expiring date of the EA		
Reference	ETSI TS 102 941 [1]		
Configuration	CFG_ENR_EA		
PICS Selection			
Expected behaviour			
with			
the EA is in 'operational' state			
ensure that			
when			
the IUT receives an I	EnrollmentRequestMessage		
containing an InnerEcRequest			
containing ValidityPeriod			
containing start date			
indicating a value greater than the start date of the EA			
then			
the IUT answers with an EnrollmentResponseMessage			
containing InnerECResponse			
containing responseCode			
indicating 'deniedpermissions'			
and not containing a certificate			

TP ld	SECONI EA END DOV 12 DI	
	SECPKI_EA_ENR_RCV_12_BI	
Summary	Enroll the ITS-Station, but the lifetime of the EC would be greater than allowed	
	(considering values in C-ITS CP [7])	
Reference	ETSI TS 102 941 [1] and C-ITS CP [7], clause 7.2	
Configuration	CFG_ENR_EA	
PICS Selection		
Expected behaviour		
with		
the EA is in 'operational' state		
ensure that		
when		
the IUT receives an EnrollmentRequestMessage		
containing an InnerEcRequest		
containing ValidityPeriod		
indicating a value greater than 3 years		
then		
the IUT answers with an EnrollmentResponseMessage		
containing InnerECResponse		
containing responseCode		
indicating 'deniedpermissions'		
and not containing a certificate		

TP ld	SECPKI_EA_ENR_RCV_13_BI		
Summary	Enroll the ITS-Station, but the inner PoP signature in the CSR, created with the EC private		
	key, cannot be verified with the provided public key		
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.1		
Configuration	CFG_ENR_EA		
PICS Selection			
Expected behaviour			
with			
the EA is in 'operational' state			
ensure that			
when			
	s an EnrollmentRequestMessage		
containing an InnerEcRequest			
signed with a private key SIGN_POP_PRIVATE_KEY			
and containing public verification keys			
indicating a value which does not match with the private key SIGN_POP_PRIVATE_KEY			
then			
the IUT answers with an EnrollmentResponseMessage			
containing InnerECResponse			
containing responseCode			
indicating 'invalidsignature'			
and not containing a certificate			

TP ld	SECPKI_EA_ENR_RCV_14_BV		
Summary	Check that EA sends the same response for the repeated EC request		
Reference	ETSI TS 103 601 [6], clause 5.1		
Configuration	CFG_ENR_EA		
PICS Selection	PICS_SECPKI_ENROLLMENT_RETRY		
	Expected behaviour		
with			
the EA is in 'operational'	state		
and the EA already rece	and the EA already received EnrollmentRequestMessage (<i>REQ</i>)		
having checksum (C	having checksum (CS)		
and the EA has sent the	EnrollmentResponseMessage (RES)		
containing responseCode			
indicating OK	indicating OK		
ensure that			
when			
the IUT receives an EnrollmentRequestMessage			
having checksum			
indicating value equal to CS			
then			
the IUT answers with an EnrollmentResponseMessage			
indicating RES	indicating RES		

TP ld	SECPKI_EA_ENR_RCV_15_BV
Summary	Check that EA does not accept enrolment when message generation time is too far in the
	past
Reference	ETSI TS 103 601 [6], clause 5.1.4
Configuration	CFG_ENR_EA
PICS Selection	PICS_SECPKI_ENROLLMENT_RETRY
	Expected behaviour
with	
the EA is in 'operation	tional' state
	<pre>/ received the EnrollmentRequestMessage (REQ)</pre>
	erationTime TG
and having che	ecksum (CS)
ensure that	
when	
the IUT receive	es an EnrollmentRequestMessage
at the mom	ent TR2
indicatir	ng TR2 > TG + PIXIT_EA_ENROLLMENT_TIMEOUT
and having	checksum
indicatir	ng value equal to CS
then	
the IUT answe	s with an EnrollmentResponseMessage
containing i	responseCode
indicatir	ng deniedrequest
NOTE: PIXIT_EA_	ENROLLMENT_TIMEOUT shall be set as a TP parameter.

5.4.2 Enrolment response

TP ld	SECPKI_EA_ENR_01_BV
Summary	The EnrollmentResponse message shall be encrypted using an ETSI TS 103 097 [2] approved algorithm and the encryption shall be done with the same AES key as the one used by the ITS-S requestor for the encryption of the EnrollmentRequest message
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
containing er	es an EnrollmentRequestMessage ncKey an encrypted AES key (SYMKEY)
the IUT answers with an EnrollmentResponseMessage 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 EnrollmentRequest message to which the response is built and containing the component ciphertext, once decrypted, contains an EtsiTs103097Data-Signed structure
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
	es an EnrollmentRequestMessage o send the enrolment response
then	
containing red containing contain and containin	one instance of RecipientInfo of choice pskRecipInfo ng the HashedId8 of the symmetric key used to encrypt the EnrollmentRequestMessage g cipherText
being an e	ncrypted EtsiTs103097Data-Signed structure

TP ld	SECPKI_EA_ENR_04_BV
Summary	The decrypted EtsiTs103097Data-Signed structure shall contain hashld, tbsData, signer and signature. The hashld shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [2], the signer shall be declared as a digest, containing the Hashedld8 of
	the EA certificate and the signature over tbsData shall be computed using the EA private key corresponding to its publicVerificationKey found in the referenced EA certificate
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT sends an	EnrollmentResponseMessage as an answer for an EnrollmentRequestMessage
then	
the IUT sends an	EtsiTs103097Data-Encrypted structure
containing an en	crypted EtsiTs103097Data-Signed structure
containing ha	
	the hash algorithm to be used as specified in ETSI TS 103 097 [2]
and containin	
and containin	
declared a	
	ig the HashedId8 of the EA certificate
and containin	
computed over tbsData	
	e EA private key
corres	sponding to the publicVerificationKey found in the referenced EA certificate

TP ld	SECPKI_EA_ENR_05_BV
	Within the headerInfo of the tbsData, the tbsData field of the decrypted
Summary	EtsiTs103097Data-Signed structure shall contain the psid set to "secured certificate
•	request" as assigned in ETSI TS 102 965 [8] and the generationTime
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT sends	an EnrollmentResponseMessage as an answer for an EnrollmentRequestMessage
then	
the IUT sends	an EtsiTs103097Data-Encrypted structure
containing an	encrypted EtsiTs103097Data-Signed structure
containing	tbsData
containing headerInfo	
containing psid	
	dicating AID_CERT_REQ

and containing generationTime and not containing any other component of tbsData.headerInfo

TP ld	SECPKI_EA_ENR_07_BV
C	The EtsiTS102941Data shall contain the version set to v1 (integer value set to 1) and the
Summary	content set to InnerECResponse
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT sends	an EnrollmentResponseMessage as an answer for an EnrollmentRequestMessage
then	
the IUT sends	an EtsiTs103097Data-Encrypted structure
containing an	encrypted EtsiTs103097Data-Signed structure
containing	tbsData
containi	ng 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-Encrypted structure received in the request
	and a responseCode indicating the result of the request
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT sends	an EnrollmentResponseMessage as an answer for an EnrollmentRequestMessage
then	
	an EtsiTs103097Data-Encrypted structure
containing a	n encrypted EtsiTs103097Data-Signed structure
containing	j tbsData
	ning EtsiTS102941Data
conta	aining InnerECResponse
CC	ontaining requestHash
	indicating the left-most 16 octets of the SHA256 digest
	of the topmost EtsiTs103097Data-Encrypted structure received in the request
ar	nd containing responseCode

TP ld	SECPKI EA ENR 09 BV	
Summary	If the responseCode is 0, the InnerECResponse shall also contain an (enrollment) certificate	
Reference	ETSI TS 102 941 [1], clause 6.2.3.2.2	
Configuration	CFG_ENR_EA	
PICS Selection		
	Expected behaviour	
ensure that		
when		
the IUT is requ	iested to send an EnrollmentResponseMessage	
containing a	containing a responseCode	
indicating	0	
then		
the IUT sends	an EtsiTs103097Data-Encrypted structure	
containing ar	encrypted EtsiTs103097Data-Signed structure	
containing	tbsData	
contain	containing EtsiTS102941Data	
conta	ining InnerECResponse	
containing an enrolment certificate		

TP ld	SECPKI_EA_ENR_10_BV	
Summers.	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	the IUT is requested to send an EnrollmentResponseMessage	
	esponseCode	
indicating a	a value different than 0	
then		
the IUT sends a	an EtsiTs103097Data-Encrypted structure	
containing an	encrypted EtsiTs103097Data-Signed structure	
containing tbsData		
containing EtsiTS102941Data		
contair	ning InnerECResponse	
not containing a certificate		

TP ld	SECPKI_EA_ENR_11_BV	
Summary	ummary Check that signing of enrolment response is permitted by the EA certificate	
Reference	ETSI TS 102 941 [1], clause B.5	
Configuration	CFG_ENR_EA	
PICS Selection		
	Expected behaviour	
ensure that		
when		
the IUT sends an En	rollmentResponseMessage as an answer for an EnrollmentRequestMessage	
then		
	siTs103097Data-Encrypted structure	
containing an encrypted EtsiTs103097Data-Signed structure		
containing signer		
declared as a digest		
containing t	the HashedId8 of the EA certificate	
containing appPermissions		
containing an item of type PsidSsp		
containing psid		
indicating AID_CERT_REQ		
and containing ssp		
containing opaque[0] (version)		
	indicating 1	
	containing opaque[1] (value)	
	indicating bit 'Enrolment Response' (5) set to 1	

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

5.4.3 Authorization validation request handling

TP ld	SECPKI_EA_AUTHVAL_RCV_01_BV
	The authorization validation response shall be sent by the EA to the AA across the
Summary	interface at reference point S4 in response to a received
	AuthorizationValidationRequestMessage
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2
Configuration	CFG_AVALID_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT receive	es an AuthorizationValidationRequestMessage
then	
	a AuthorizationValidationResponseMessage reference point S4 to the AA

TP ld	SECPKI_EA_AUTHVAL_RCV_02_BI
	Check that EA does not accept the authorization validation request when
Summary	SharedAtRequest is signed with certificate without appropriate permissions
Reference	ETSI TS 102 941 [1], clause B.5
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT receives an	AuthorizationValidationRequestMessage
containing EtsiTs	102941Data
containing ecS	ignature
containing s	5
	ng digest
	ting HashedId8 of the certificate EC certificate
	ntaining appPermissions
r	not containing an item of type PsidSsp
	containing psid
	indicating AID_CERT_REQ
C	or containing an item of type PsidSsp
	containing psid
	indicating AID_CERT_REQ
	and containing ssp
	containing opaque[0] (version)
	indicating other value than 1
	or containing opaque[1] (value)
44-5-4	indicating 'Authorization Request' (bit 2) set to 0
then	
	n an AuthorizationValidationResponseMessage
containing respons	
indicating 'denie	eapermissions

5.4.4 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 authorization request to which the response is built and the component ciphertext containing the encrypted representation of the EtsiTs103097Data-Signed. The encryption uses a ETSI TS 103 097 [2] approved algorithm
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2
O and in the second second	ETSI TS 103 097 [2], clause 7
Configuration	CFG_AVALID_EA
PICS Selection	
-	Expected behaviour
ensure that	
when	
	a AuthorizationValidationRequestMessage
containing enck	
	encrypted symmetric data encryption key (SYMKEY)
then	
	AuthorizationValidationResponseMessage
•	iTs103097Data-Encrypted
containing	
	ng one instance of RecipientInfo of choice pskRecipInfo
	ating the HashedId8 of SYMKEY
	ning ciphertext
	ng EtsiTs103097Data-Signed
being	encrypted using SYMKEY and an ETSI TS 103 097 [2] approved algorithm

TP ld	SECPKI_EA_AUTHVAL_02_BV
Summary	To read an authorization validation response, the AA shall receive an EtsiTs103097Data-Encrypted structure, containing a EtsiTs103097Data-Signed structure, containing a EtsiTs102941Data structure, containing an AuthorizationValidationResponse structure
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2
Configuration	CFG_AVALID_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT receives a	a AuthorizationValidationRequestMessage
then	
the IUT sends a A	uthorizationValidationResponseMessage
containing EtsiT	s103097Data-Signed
containing Et	siTs102941Data
containing	authorizationValidationResponse

TP Id	SECPKI_EA_AUTHVAL_03_BV
	The AuthorizationValidationResponse structure contains the requestHash being the
Summary	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	
	a AuthorizationValidationRequestMessage
containing Etsi	Ts103097Data-Signed structure (REQDSS)
then	
the IUT sends a	AuthorizationValidationResponseMessage
containing Ets	iTs103097Data-Signed
containing	EtsiTs102941Data
containir	ng authorizationValidationResponse
conta	ining requestHash
indi	cating the left-most 16 octets of the SHA256 digest of REQDSS
and c	ontaining responseCode

TP ld	SECPKI_EA_AUTHVAL_04_BV
Summary	If the responseCode is 0, the AuthorizationValidationResponse structure contains the component confirmedSubjectAttributes with the attributes the EA wishes to confirm, except
	for certIssuePermissions which is not allowed to be present
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2
Configuration	CFG_AVALID_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT receive	es a AuthorizationValidationRequestMessage
	sponds with a AuthorizationValidationResponseMessage
	uthorizationValidationResponse
	i responseCode
indicati	
then	
	rizationValidationResponseMessage
	authorizationValidationResponse
	g confirmedSubjectAttributes
	Itaining certIssuePermissions
not cor	Italining certissuerennissions

TP Id	SECPKI_EA_AUTHVAL_05_BV
Summary	If the responseCode is different than 0, the AuthorizationValidationResponse structure does not contain the component confirmedSubjectAttributes
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2
Configuration	CFG_AVALID_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT receives a A	uthorizationValidationRequestMessage
and the IUT respond	s with a AuthorizationValidationResponseMessage
containing authoriz	zationValidationResponse
containing resp	onseCode
indicating a v	value different than 0
then	
	nValidationResponseMessage
contains an author	izationValidationResponse
not containing confirmedSubjectAttributes	

TP ld	SECPKI_EA_AUTHVAL_06_BV
Summary	The component version of the EtsiTs102941Data structure is set to v1 (integer value set to 1)
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2
Configuration	CFG_AVALID_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT receive	es a AuthorizationValidationRequestMessage
then	
containing Et containing	a AuthorizationValidationResponseMessage siTs103097Data-Signed j EtsiTs102941Data ing version
	cating v1 (integer value set to 1)

TP ld	SECPKI_EA_AUTHVAL_07_BV
Summary	EtsiTs103097Data-Signed.tbsData contains the EtsiTs102941Data as payload and the headerInfo containing psid and generationTime. The psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [8] and the generationTime shall be present. All other components of the component tbsdata.headerInfo are not used and absent
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2
Configuration	CFG_AVALID_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT receives	a AuthorizationValidationRequestMessage
then	
containing Etsi containing th containin containin indica and con	g headerInfo ng psid ating AID_CERT_REQ taining generationTime
and not	containing any other component of tbsdata.headerInfo

TP ld	SECPKI_EA_AUTHVAL_08_BV
Summary	EtsiTs103097Data-Signed structure shall contain hashId, tbsData, signer and signature. The hashId shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [2], the signer shall be declared as a digest, containing the HashedId8 of the EA certificate and the signature over tbsData shall be computed using the EA private key corresponding to its publicVerificationKey found in the referenced EA certificate
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.2
Configuration	CFG_AVALID_EA
PICS Selection	
	Expected behaviour
then the IUT sends containing an containing indicatir and contai and contai declare contai and contai comput using	es a AuthorizationValidationRequestMessage a AuthorizationValidationResponseMessage EtsiTs103097Data-Signed structure hashId ng the hash algorithm to be used as specified in ETSI TS 103 097 [2] ning tbsData ning signer d as a digest ining the HashedId8 of the EA certificate ning signature ed over tbsData the EA private key responding to the publicVerificationKey found in the referenced EA certificate
TP ld	SECPKI_EA_AUTHVAL_09_BV
0	

TP ld	SECPKI_EA_AUTHVAL_09_BV
Summary	Check that signing of authorization validation response is permitted by the EA certificate
Reference	ETSI TS 102 941 [1], clause B.5
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT is requ	ested to send an AuthorizationValidationResponseMessage
then	
the IUT sends	an EtsiTs103097Data-Encrypted structure
containing an	encrypted EtsiTs103097Data-Signed structure
containing	signer
contain	ing digest
indica	ting HashedId8 of the EA certificate
COI	ntaining appPermissions
	containing an item of type PsidSsp
	containing psid
	indicating AID_CERT_REQ
	and containing ssp
	containing opaque[0] (version)
	indicating 1
	containing opaque[1] (value)
	indicating 'Authorization Validation Response' (bit 4) set to 1

TP ld	SECPKI_EA_CERTGEN_01_BV
0	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 reque	ested to send a CACertificateRequestMessage
then	
the IUT sends a	a CACertificateRequestMessage
across the r	eference point S10 to the RCA

across the reference point S10 to the RCA

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

TP ld	SECPKI_EA_CERTGEN_03_BV
	The hashId shall indicate the hash algorithm to be used as specified in ETSI
Summary	TS 103 097 [2], the signer is set to 'self' and the signature over the tbsData is computed
	using the private key corresponding to the new verificationKey to be certified (i.e. the
	request is self-signed)
Reference	ETSI TS 102 941 [1], clause 6.2.1
	ETSI TS 103 097 [2], clause 7
Configuration	CFG_CAGEN_INIT
PICS Selection	
	Expected behaviour
with	
the IUT being in the 'initi	ial' state
ensure that	
when	
the IUT is requested	to send a CACertificateRequestMessage
then	
	CertificateRequestMessage
	03097Data-Signed structure
containing has	
	e hash algorithm to be used
and containing	
indicating 'se	
and containing tbsData	
containing the EtsiTs102941Data structure	
containing caCertificateRequest	
containing publicKeys	
containing verification_key (VKEY)	
and containing signature	
computed over tbsData using the private key corresponding to the verificationKey (VKEY)	

TP ld	SECPKI EA CERTGEN 04 BV
Summary	An ECC private key is randomly generated, the corresponding public key (verificationKey) is provided to be included in the CaCertificateRequest An ECC encryption private key is randomly generated, the corresponding public key (encryptionKey) is provided to be included in the CACertificateRequest CaCertificateRequest.publicKeys shall contain verification_key and encryption_key
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_INIT
PICS Selection	
	Expected behaviour
with the IUT being in the ensure that when	
the IUT is requested to send a CACertificateRequestMessage	
then the IUT sends a CACertificateRequestMessage containing caCertificateRequest containing publicKeys containing verification_key and containing encryption_key	

TP ld	SECPKI EA CERTGEN 05 BV		
Summary	The EtsiTs102941Data structure is built with version set to v1 (integer value set to 1)		
Reference	ETSI TS 102 941 [1], clause 6.2.1		
Configuration	CFG_CAGEN_INIT		
PICS Selection			
	Expected behaviour		
with			
the IUT being in the 'initi	al' state		
ensure that			
when			
the IUT is requested	the IUT is requested to send a CACertificateRequestMessage		
then	then		
the IUT sends a CACertificateRequestMessage			
containing EtsiTs102941Data			
containing version			
indicating v1 (integer value set to 1)			

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

TP ld	SECPKI_EA_CERTGEN_07_BV
Summary	EtsiTs103097Data-Signed.tbsData contains the EtsiTs102941Data as payload and the headerInfo containing psid and generationTime. The psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [8] and the generationTime shall be present. All other components of the component tbsdata.headerInfo are not used and absent
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_INIT
PICS Selection	
	Expected behaviour
then the IUT sends a CAO containing heade containing psid indicating SI and containing	to send a CACertificateRequestMessage CertificateRequestMessage erInfo

TP ld	SECPKI_EA_CERTGEN_08_BV
Summary	If the current private key has reached its end of validity period or is revoked, the SubCA
	shall restart the initial certificate application process
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_REKEY
PICS Selection	
	Expected behaviour
with	
the IUT being in th	ne 'operational' state
ensure that	
when	
the IUT is requ	lested to perform a CA certificate rekeying procedure
and SubCA ce	rtificate is no longer valid (due to end of validity or revocation)
then	
the IUT switch	es to the "initial' state
and sends a C	ACertificateRequestMessage

TP ld	SECPKI_EA_CERTGEN_09_BV
Summary	For the re-keying application to the RCA (CaCertificateRekeyingMessage), an EtsiTs103097Data-Signed structure is built, containing: hashId, tbsData, signer and signature. The hashId shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [2]. The signer declared as a digest, containing the hashedId8 of the EA certificate and the signature over tbsData is computed using the currently valid private key corresponding to the EA certificate (outer signature)
Reference	ETSI TS 102 941 [1], clause 6.2.1 ETSI TS 103 097 [2], clause 7
Configuration	CFG_CAGEN_REKEY
PICS Selection	
	Expected behaviour
then the IUT sends a CAC being an EtsiTs100 containing hashl indicating the and containing the and containing s containing dig	to perform a CA certificate rekeying procedure CertificateRekeyingMessage 3097Data-Signed structure Id hash algorithm to be used bsData signer gest fashedId8 of the SubCA certificate (CERT) signature

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

TP ld	SECPKI_EA_CERTGEN_11_BV
Summary	The (outer) tbsData of the CACertificateRekeyingMessage shall contain a headerInfo containing psid and generationTime. The psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [8] and the generationTime shall be present. All other components of the component tbsdata.headerInfo are not used and absent
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_REKEY
PICS Selection	
	Expected behaviour
with	
the IUT being in the	'operational' state
ensure that	
when	
the IUT is reques	ted to perform a CA certificate rekeying procedure
then	
	ertificateRekeyingMessage
containing tbsData	
containing he	
containing psid	
indicating SEC_CERT_REQ	
and containing generationTime	
and not containing any other component of tbsdata.headerInfo	

TP ld	SECPKI_EA_CERTGEN_12_BV
	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 'ope	rational' state
ensure that	
when	
•	to perform a CA certificate rekeying procedure
then	
	icateRekeyingMessage
	097Data-Signed structure
and containing tbsData	
and containing	
containing dig	
indicating HashedId8 of the CA certificate	
containing appPermissions containing an item of type PsidSsp	
containing psid	
indicating AID_CERT_REQ	
and containing ssp	
containing opaque[0] (version)	
indicating 1	
containing opaque[1] (value)	
indicating 'CA Certificate Response' (bit 6) set to 1	

5.4.6 Authorization using butterfly key expansion mechanism

TP ld	SECPKI_EA_BFK_AUTH_01_BV
	Check that the EA sends the butterfly authorization respond message after receiving of the
Summary	butterfly authorization request
•	Check that this message is signed with EA certificate
Reference	ETSI TS 102 941 [1], clauses 6.2.3.5.1 and 6.2.3.5.3
Configuration	CFG_BFK_AUTH_EA
PICS Selection	
	Expected behaviour
with	
the EA in 'operatio	nal' state
authorized with	CERT_EA certificate
and the ITS-S in 'e	nrolled' state
ensure that	
when	
	d the ButterflyAuthorizationRequestMessage
then	
	an EtsiTs103097Data to the ITS-S
	content.signedData
	ng tbsData
	aining headerInfo
C	
	indicating AID_PKI_CERT_REQUEST
	Ind containing generationTime Ind not containing any other field
	containing payload.data
	ndicating EtsiTs102941Data
1	containing version
	indicating '1'
	and containing content
	containing butterflyCertificateResponse
and containing signer	
containing digest	
	indicating HashedId8 of the CERT_EA
and con	taining signature
	lated using CERT_EA verification public key

5.4.6.1 Butterfly authorization response

TP ld	SECPKI_EA_BFK_AUTH_02_BV	
Summary	Check that the butterfly authorization respond message, sent by EA, contains all	
	necessary fields	
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.3	
Configuration	CFG_BFK_AUTH_EA	
PICS Selection		
	Expected behaviour	
with		
the EA in 'operational' st	ate	
authorized with CER	T_EA certificate	
and the ITS-S in 'enrolle	d' state	
ensure that		
when		
the IUT received the	ButterflyAuthorizationRequestMessage (REQ)	
then		
	ITS-S a ButterflyAuthorizationResponseMessage	
	flyCertificateResponse	
	ing RaEeCertInfo	
containing version		
indicating 2		
and containing generationTime		
indicating value between REQ_TIME and the current time		
and containing currentl		
and	d containing requestHash	
	indicating the left-most 16 octets of the SHA256 digest of the REQ	
	d containing nextDITime	
and	d not containing acpcTreeld	

TP ld	SECPKI_EA_BFK_AUTH_03_BV
	Check that the EA sends butterfly certificate request message after receiving of the
	butterfly authorization request
Summary	Check that this message is encrypted for the AA
	Check that this message is signed with the EA certificate
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.4
Configuration	CFG_BFK_AUTH_EA
PICS Selection	
	Expected behaviour
with	
the EA in 'operational'	state
authorized with CE	
and the AA is emulate	
authorized with CE	
	o use emulated AA to generate certificates
ensure that	
when	
the IUT received the	ne ButterflyAuthorizationRequestMessage
containing Etsi	
containing of	content.butterflyAuthorizationRequest
then	
the IUT sends a Et	siTs103097Data to the AA
	ent.encryptedData
containing r	
indicatir	ig size 1
and con	taining the instance of RecipientInfo
	aining certRecipInfo
C	containing recipientId
	indicating HashedId8 of the CERT_AA
	encrypted representation of EtsiTs103097Data
	ng signedData
	aining tbsData
C	containing headerInfo
	containing psid
	indicating AID_PKI_CERT_REQUEST
	and containing payload.data
	indicating EtsiTs102941Data
	containing version
	indicating '1'
	and containing content
	containing butterflyCertificateRequest and containing signer
	containing signer
	indicating HashedId8 of the CERT_EA

5.4.6.2 Butterfly certificate request

n	n	
3	υ	

TP ld	SECPKI_EA_ BFK_ AUTH_04_BV
Summary	Check that the butterfly certificate request message sent by EA to AA contains all required
Summary	elements
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.4
Configuration	CFG_BFK_AUTH_EA
PICS Selection	
	Expected behaviour
with	
the EA in 'operation	nal' state
	CERT_EA certificate
	received the ButterflyAuthorizationRequestMessage
	ha256 message hash MSG_HASH
	responded with ButterflyAuthorizationResponseMessage
containing Etsi	
	outterflyAuthorizationResponse
	ng nextDITime
	ating DNL_TIME
ensure that	
when	
	d the ButterflyAtDownloadRequestMessage
	EtsiTs102941Data
	ng butterflyAtDownloadRequest
	ating EeRaCertRequest ontaining generationTime
C	indicating REQ_TIME
then	
	o the AA the ButterflyCertRequestMessage
	EtsiTs102941Data
	ng content
	aining butterflyCertificateRequest
	ndicating RaAcaCertRequest
	containing version
	indicating 2
	and containing generationTime
	indicating value between REQ_TIME and the current time
	and containing flags
	indicating empty bit string
	and containing certEncKey
	and containing tbsCert
	and not containing linkageInfo

TP ld	SECPKI_EA_BFK_AUTH_05_BV
Summary	Check that the butterfly certificate request message contains expanded cocoon key
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.4
Configuration	CFG BFK AUTH EA
PICS Selection	
	Expected behaviour
with	
the EA in 'operational' st	ate
authorized with CER	T_EA certificate
and the AA in 'operation	al' state
authorized with CER	T_AA certificate
and EA is configured to	use AA of the current configuration to generate certificates
ensure that	
when	
	ButterflyAuthorizationRequestMessage
containing EtsiTs	
	ntent.butterflyAuthorizationRequest
	EeRaCertRequest
	ning tbsCert (TBS_CERT)
	ntaining verification key (CATERPILLAR_KEY)
then the ILIT conde to the	AA the ButterflyCertRequestMessage
containing EtsiTs	
containing co	
	y butterflyCertificateRequest
	ting RaAcaCertReguest
	d containing tbsCert
	containing verificationKey
	containing "cocoon" key
	derived from the CATERPILLAR_KEY

TP ld	SECPKI_EA_BFK_AUTH_06_BV
Summary	Check that the butterfly certificate request message sent by EA to AA contains all required elements
Reference	ETSI TS 102 941 [1], clause 6.2.3.5.4
Configuration	CFG_BFK_AUTH_EA
PICS Selection	
	Expected behaviour
with	
the EA in 'operational' st	ate
authorized with CER	T_EA certificate
and the EA already resp	onded with ButterflyAuthorizationResponseMessage (MSG_RESPONSE)
containing EtsiTs102	2941Data
	flyAuthorizationResponse
containing ne	
	DNL_TIME
and containin	0
indicating	
	g requestHash
	MSG_HASH
	ived from emullated AA one or more ButterflyCertResponse messages
5	rtResponsePrivateSpdu (CERT_RESPONSE)
ensure that	
when	
	ButterflyAtDownloadRequestMessage
containing EtsiTs	
	tterflyAtDownloadRequest
	ning generationTime
	licating DNL_TIME + 1
	ontaining filename licating MSG_HASH + "_" + hex(I_VALUE) + ".zip"
then	
	quested batch of certificates
	x(I_VALUE) + ".info"
	ER encoding of MSG_RESPONSE
	set of files hex(I_VALUE) + "_" + (0N)
	ER encoding of AcaEeCertResponsePrivateSpdu (CERT_RESPONSE)

5.4.6.3 Authorization certificate download

5.5 AA behaviour

5.5.0 Overview

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

```
PICS_SECPKI_IUT_AA = TRUE
```

5.5.1 Authorization request handling

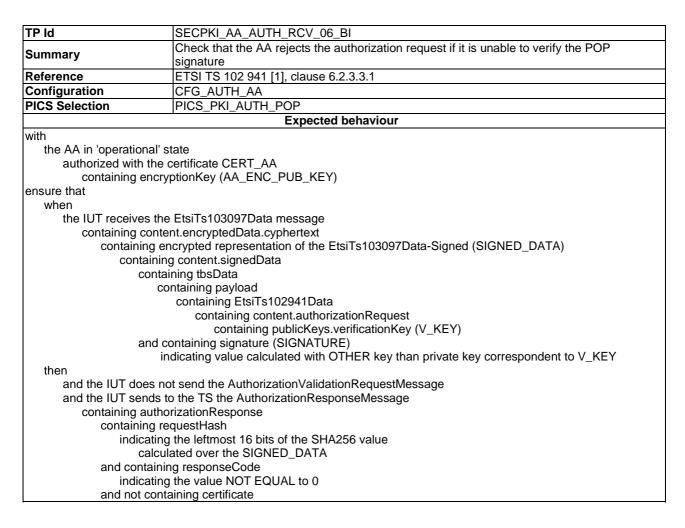
TP ld	SECPKI_AA_AUTH_RCV_01_BV
	Check that the AA is able to decrypt the AuthorizationRequestMessage using the
	encryption private key corresponding to the recipient certificate
-	Check that the AA is able to verify the inner signature
Summary	Check that the AA is able to verify the request authenticity using the hmacKey verification
	Check that the AA sends the Authorization Validation Request message to the
	correspondent EA
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS_PKI_AUTH_POP
	Expected behaviour
with	
the AA in 'operation	nal' state
	the certificate CERT_AA
	encryptionKey (AA_ENC_PUB_KEY)
ensure that	
when	
	s the EtsiTs103097Data-Encrypted message
	content.encryptedData
	ng recipients
	aining the instance of RecipientInfo
	ontaining certRecipInfo
	containing recipientId
	indicating HashedId8 of the certificate CERT_AA
	and containing encKey
	indicating symmetric key (S_KEY)
	encrypted with the private key correspondent to the AA_ENC_PUB_KEY
	taining cyphertext (ENC_DATA)
	aining cyphenext (ENC_DATA) aining encrypted representation of the EtsiTs103097Data-Signed
	ontaining content.signedData
	containing hashld
	indicating valid hash algorithm
a	nd containing signer
	containing self
a	nd 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
	nd containing signature (SIGNATURE)
then	to desput the S KEV
	to decrypt the S_KEY
using the pr	
	onding to the AA_ENC_PUB_KEY
	able to decrypt the cyphertext ENC_DATA
using the S	
	able to verify the signature over the SIGNED_DATA
using the V	
	able to verify integrity of HMAC and KEY_TAG
	nds the AuthorizationValidationRequest message to the EA
identified by	the EA_ID

TP ld	SECPKI_AA_AUTH_RCV_02_BV
	Check that the AA is able to decrypt the AuthorizationRequestMessage using the
	encryption private key corresponding to the recipient certificate
Summary	Check that the AA is able to verify the request authenticity using the hmacKey verification
Summary	Check that the AA sends the Authorization Validation Request message to the
	correspondent EA
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG AUTH AA
PICS Selection	NOT PICS_PKI_AUTH_POP
FICS Selection	Expected behaviour
with	
the AA in 'operational'	atata
	e certificate CERT_AA
	yptionKey (AA_ENC_PUB_KEY)
ensure that	
when	
	e EtsiTs103097Data-Encrypted message
	ent.encryptedData
containing r	ecipients
containir	ng the instance of RecipientInfo
	aining certRecipInfo
C	containing recipientId
	indicating HashedId8 of the certificate CERT_AA
а	and containing encKey
	indicating symmetric key (S_KEY)
	encrypted with the private key correspondent to the AA_ENC_PUB_KEY
	ing cyphertext (ENC_DATA)
	ng EtsiTs102941Data
	aining content.authorizationRequest
	containing hmacKey (HMAC) and containing sharedAtRequest
a	containing keyTag (KEY_TAG)
	and containing eald (EA_ID)
	indicating HashedId8 of the known EA certificate
then	
the IUT is able to d	lecrypt the S KEY
using the privat	
	ing to the AA_ENC_PUB_KEY
	to decrypt the cyphertext ENC_DATA
using the S_KE	
	to verify integrity of HMAC and KEY_TAG
	the AuthorizationValidationRequestMessage to the EA
identified by the	

TP ld	SECPKI_AA_AUTH_RCV_03_BI
Summary	Check that the AA skips the authorization request if it is not addressed to this AA
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with	
the AA in 'operational' st	
authorized with the c	pertificate CERT_AA
containing encryp	ptionKey (AA_ENC_PUB_KEY)
ensure that	
when	
the IUT receives the	EtsiTs103097Data message
containing conter	nt.encryptedData
containing rec	cipients
containing	g only one instance of RecipientInfo
contair	ning certRecipInfo
CO	ntaining recipientId
	indicating value
	NOT equal to the HashedId8 of the certificate CERT_AA
and	d containing encKey
	indicating symmetric key (S_KEY)
	encrypted with the private key correspondent to the AA_ENC_PUB_KEY
then	
the IUT does not sen	nd the AuthorizationValidationRequestMessage

TP ld	SECPKI_AA_AUTH_RCV_04_BI	
Summary	Check that the AA skips the authorization request if it is unable to decrypt the encKey	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_AA	
PICS Selection		
	Expected behaviour	
with		
the AA in 'operational	' state	
authorized with th	e certificate CERT_AA	
containing end	ryptionKey (AA_ENC_PUB_KEY)	
ensure that		
when		
the IUT receives t	he EtsiTs103097Data message	
	tent.encryptedData	
containing	•	
	ing the instance of RecipientInfo	
con	taining certRecipInfo	
	containing recipientId	
	indicating value	
	equal to the HashedId8 of the certificate CERT_AA	
	and containing encKey	
	indicating symmetric key (S_KEY)	
	encrypted with the OTHER private key than the correspondent to the	
	AA_ENC_PUB_KEY	
then		
the IUT does not s	send the AuthorizationValidationRequestMessage	

TP ld	SECPKI_AA_AUTH_RCV_05_BI
Summary	Check that the AA skips the authorization request if it is unable to decrypt the cyphertext
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with	
the AA in 'operational' st	ate
authorized with the c	ertificate CERT AA
containing encry	ptionKey (AA ENC PUB KEY)
ensure that	
when	
the IUT receives the	EtsiTs103097Data message
containing conter	nt.encryptedData
containing red	cipients[0].encKey
	encrypted symmetric key (S_KEY)
	g cyphertext (ENC_DATA)
	with the OTHER key than S_KEY
then	
	t send the AuthorizationValidationRequestMessage to the correspondent EA



TP ld	SECPKI_AA_AUTH_RCV_07_BI		
Summony	Check that the AA rejects the authorization request if it is unable to verify the		
Summary	the request using hmacKey		
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1		
Configuration	CFG_AUTH_AA		
PICS Selection	X_PICS		
	Expected behaviour		
with			
the AA in 'operati	onal' state		
authorized wi	th the certificate CERT_AA		
containing	encryptionKey (AA_ENC_PUB_KEY)		
ensure that			
when			
	ves the EtsiTs103097Data message		
	EtsiTs102941Data		
	ning content.authorizationRequest		
	ntaining hmacKey (HMAC)		
an	d containing sharedAtRequest		
	containing keyTag (KEY_TAG)		
then	indicating wrong value		
	oes not send the AuthorizationValidationRequest me	anessa	
	ends to the TS the Authorization Response Message	Joodgo	
	authorizationResponse		
	ning requestHash		
	licating the leftmost 16 bits of the SHA256 value		
	calculated over the X_HASH_STRUCTURE		
	ontaining responseCode		
ind	licating the value NOT EQUAL to 0		
and no	ot containing certificate		
	Variants		
nn	X_PICS	X_HASH_STRUCTURE	
A	PICS_PKI_AUTH_POP NOT PICS_PKI_AUTH_POP	EtsiTs103097Data-Signed	
1 2		EtsiTs102941Data	

TP Id	SECPKI_AA_AUTH_RCV_08_BI
Summary	Send a correctly encoded AT request, but the ITS-Station is not enrolled at the EA
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS_PKI_AUTH_POP
	Expected behaviour
with	
the AA in 'operational' st	tate
authorized with the c	certificate CERT_AA
containing encry	otionKey (AA_ENC_PUB_KEY)
ensure that	
when	
the IUT receives the AuthorizationRequestMessage	
containing ecSignature	
containing Signer	
indicating an unknown EC hashedId8 value	
then	
and the IUT does not send the AuthorizationValidationRequestMessage	
and the IUT sends to the TS the AuthorizationResponseMessage	
containing authorizationResponse	
containing responseCode	
indicating the value 'unknownits'	
and not containing certificate	

TP ld	SECPKI_AA_AUTH_RCV_09_BI	
Summary	Send an AT request, but the inner signer (valid EC) is not issued by the EA which is known	
	trusted by the AA. The AA trusts only EAs listed on the RCA-CTL	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_AA	
PICS Selection	PICS_PKI_AUTH_POP	
	Expected behaviour	
with		
the AA in 'operationa	al' state	
authorized with t	he certificate CERT_AA	
containing er	ncryptionKey (AA_ENC_PUB_KEY)	
ensure that		
when		
	the AuthorizationRequestMessage	
	containing SharedAtRequest	
	containing eald	
indicating an unknown value		
then		
	and the IUT does not send the AuthorizationValidationRequestMessage	
and the IUT sends to the TS the AuthorizationResponseMessage		
containing authorizationResponse		
containing responseCode		
indicating the value 'its-aa-unknownea'		
and not containing certificate		
TP ld	SECPKI AA AUTH RCV 10 BI	

TP ld	SECPKI_AA_AUTH_RCV_10_BI
Summary	Send an AT request, but the generation time of the POP signature of the CSR is later then
	preloading period of AT certificates
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1, C-ITS CP [7], clause 7.2.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS_PKI_AUTH_POP
	Expected behaviour
with	
the AA in 'operation	al' state
authorized with t	he certificate CERT_AA
	ncryptionKey (AA_ENC_PUB_KEY)
ensure that	
when	
the IUT receives the AuthorizationRequestMessage	
containing POP signature	
containing tbsData	
containing generationTime	
	dicating a value later then PIXIT_AT_PRELOADING_PERIOD in the past
then	
and the IUT does not send the AuthorizationValidationRequestMessage	
and the IUT sends to the TS the AuthorizationResponseMessage	
containing authorizationResponse	
containing responseCode	
indicating the value 'its-aa-outofsyncrequest'	
and not c	ontaining certificate

75.1.1		
TP ld	SECPKI_AA_AUTH_RCV_11_BI	
Summary	Send an AT request, but the generation time of the POP signature of the CSR is in the	
Caminaly	future	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1	
Configuration	CFG_AUTH_AA	
PICS Selection	PICS_PKI_AUTH_POP	
	Expected behaviour	
with		
the AA in 'operational' s	tate	
authorized with the o	authorized with the certificate CERT_AA	
containing encryptionKey (AA_ENC_PUB_KEY)		
ensure that		
when		
the IUT receives the AuthorizationRequestMessage		
containing POP	containing POP signature	
containing tbsData		
containing generationTime		
indicating a value in the future		
then		
and the IUT does not send the AuthorizationValidationRequestMessage		
and the IUT sends to the TS the AuthorizationResponseMessage		
containing authorizationResponse		
containing responseCode		
•	the value 'its-aa-outofsyncrequest'	
and not containing certificate		

TP ld	SECPKI_AA_AUTH_RCV_12_BI
Summary	Send an AT request, but the expiry date of the CSR is before the start date of the EC
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS PKI AUTH POP
	Expected behaviour
with	
the AA in 'operational'	state
•	e certificate CERT_AA
containing enci	ryptionKey (AA_ENC_PUB_KEY)
ensure that	
when	
the IUT receives the AuthorizationRequestMessage	
containing SharedAtRequest	
containing requested Subjec Attributes	
containing ValidityPeriod	
indicating a time range ending before the starting time of the EC	
then	
and the IUT does not send the AuthorizationValidationRequestMessage	
and the IUT sends to the TS the AuthorizationResponseMessage	
containing authorizationResponse	
containing responseCode	
indicating the value 'deniedpermissions'	
and not containing certificate	

100	
-----	--

TP ld	SECPKI_AA_AUTH_RCV_13_BI
Summary	Send an AT request, but the start date of the CSR is before the start date of the EC
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS_PKI_AUTH_POP
	Expected behaviour
with	
the AA in 'operatio	nal' state
authorized with	the certificate CERT_AA
containing e	encryptionKey (AA_ENC_PUB_KEY)
ensure that	
when	
	es the AuthorizationRequestMessage
	SharedAtRequest
	ng requestedSubjecAttributes
	aining ValidityPeriod
C	containing start date
	indicating a value less than the start date of the EC
then	an and she with size (in Maline Demonstration Demonstration)
	es not send the AuthorizationValidationRequestMessage
	nds to the TS the AuthorizationResponseMessage
	authorizationResponse ng responseCode
	cating the value 'deniedpermissions'
and not containing certificate	
anu not	
TP ld	SECPKI_AA_AUTH_RCV_14_BI
Current and a	Quark an AT result to the surface data of the QOD is after the surface data of the EQ

TP Id	SECPKI_AA_AUTH_RCV_14_BI
Summary	Send an AT request, but the expiry date of the CSR is after the expiry date of the EC
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS_PKI_AUTH_POP
	Expected behaviour
with	
the AA in 'operational' st	tate
authorized with the c	certificate CERT_AA
containing encryp	otionKey (AA_ENC_PUB_KEY)
ensure that	
when	
the IUT receives the AuthorizationRequestMessage	
containing SharedAtRequest	
containing requestedSubjecAttributes	
containing ValidityPeriod	
	ting a value greater than the ValidityPeriod of the EC
then	t cond the Authorization) (clidation Desugat) Access
and the IUT does not send the AuthorizationValidationRequestMessage	
and the IUT sends to the TS the AuthorizationResponseMessage	
containing authorizationResponse	
containing responseCode	
indicating the value 'deniedpermissions' and not containing certificate	

|--|

TP ld	SECPKI_AA_AUTH_RCV_15_BI
Summary	Send an AT request, but the start date of the CSR is after the expiring date of the EC
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS_PKI_AUTH_POP
	Expected behaviour
with	
the AA in 'operation	nal' state
	the certificate CERT_AA
	encryptionKey (AA_ENC_PUB_KEY)
ensure that	
when	
the IUT receive	s the AuthorizationRequestMessage
	SharedAtRequest
	ng requestedSubjecAttributes
	aining ValidityPeriod
	containing start date
	indicating a value greater than the start date of the EC
then	
	es not send the AuthorizationValidationRequestMessage
	nds to the TS the AuthorizationResponseMessage
	authorizationResponse
	ng responseCode
	ating the value 'deniedpermissions'
	containing certificate
TP ld	SECPKI_AA_AUTH_RCV_16_BI
Summary	Send an AT request, but the expiry date of the CSR is after now + maximum preloading
Summary	period (considering values in C-ITS CP [7])
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.1, C-ITS CP [7], clause 7.2.1
Configuration	CFG_AUTH_AA
PICS Selection	PICS_PKI_AUTH_POP
	Expected behaviour
with	
the AA in 'operation	nal' state
	the certificate CERT_AA
	encryptionKey (AA_ENC_PUB_KEY)
ensure that	
when	
the IUT receive	s the AuthorizationRequestMessage

When		
the IUT receives the AuthorizationRequestMessage		
containing SharedAtRequest		
containing requestedSubjecAttributes		
containing ValidityPeriod		
containing start date		
indicating the current date		
and a duration		
indicating value grater then PIXIT_AT_PRELOADING_PERIOD		
then		
and the IUT does not send the AuthorizationValidationRequestMessage		
and the IUT sends to the TS the AuthorizationResponseMessage		
containing authorizationResponse		
containing responseCode		
indicating the value 'deniedpermissions'		
and not containing certificate		
NOTE: PIXIT_AT_PRELOADING_PERIOD shall be set as a TP parameter.		

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

TP ld	SECPKI_AA_AUTH_RCV_18_BV
Summary	Check that AA does not accept authorization requests when message generation time is
	too far in the past
Reference	ETSI TS 103 601 [6], clause 5.1.4
Configuration	CFG_ENR_AA
PICS Selection	PICS_SECPKI_AUTHORIZATION_RETRY
	Expected behaviour
with	·
the EA is in 'operati	onal' state
and the AA already	received the AuthorizationRequestMessage (<i>REQ</i>)
containing gene	rationTime TG
and having chec	ksum (CS)
ensure that	
when	
the IUT receives	an AuthorizationRequestMessage
at the mome	nt <i>TR2</i>
indicating	g TR2 > TG + PIXIT_AA_AUTH_TIMEOUT
and having c	checksum
indicating	g value equal to CS
then	
the IUT answers	s with an AuthorizationResponseMessage
containing re	esponseCode
indicating	deniedrequest
NOTE: PIXIT_AA_A	UTH_TIMEOUT shall be set as a TP parameter.

TP ld	SECPKI_AA_AUTHVAL_01_BV
Summary	Check that the AA sends authorization validation request after receiving of the
	authorization request
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with	
the EA in 'operational' st	
authorized with CER	T_EA certificate
ensure that	
when	
	AuthorizationRequestMessage
containing EtsiTs	
	ntent.authorizationRequest
	sharedAtRequest
	ning eald (EA_ID)
	licating HashedId8 of the CERT_EA
then	
	ne EtsiTs103097Data message
to the EA identifie	ed by EA_ID
TP ld	SECPKI_AA_AUTHVAL_02_BV
	Check that the AuthorizationValidationRequestMessage is encrypted using approved
Summary	algorithm and sent to only one EA
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with	ato
the EA in 'operational' st authorized with CER	
ensure that	
when	
_	o send the authorization validation request to the EA
then	o sona ano adanonzation validation request to the EA
	Ts103097Data-Encrypted
	nt.encryptedData.recipients
indicating size	
	g the instance of RecipientInfo
	g certRecipInfo
	ning recipientId
	licating HashedId8 of the CERT_EA
and co	ontaining encKey
	ntaining eciesNistP256
	containing eciesBrainpoolP256r1
01	

TP ld	SECPKI_AA_AUTHVAL_03_BV
Summary	Check that the AA sends authorization validation request signed by AA
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with	
the AA in 'operatio	nal' state
authorized with	CERT_AA certificate
and the EA in 'ope	rational' state
ensure that	
when	
the IUT is trigg	ered to send the authorization validation request to the EA
then	
	a EtsiTs103097Data-Encrypted message
	EtsiTs103097Data-Signed
	ng signedData
	aining signer
C	containing digest
	indicating HashedId8 value of the CERT_AA
75.1.1	
TP ld	SECPKI_AA_AUTHVAL_04_BV
Summary	Check that the AA sends signed authorization validation request with signature properly
	calculated using approved hash algorithm

Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with	
the AA in 'operational' st	ate
authorized with CER	T_AA certificate
containing verific	ationKey (AA_PUB_V_KEY)
and the EA in 'operation	al' state
authorized with CER	T_EA certificate
ensure that	
when	
the IUT is triggered t	o send the authorization validation request to the EA
then	
	Ts103097Data-Encrypted message
	103097Data-Signed
containing sig	
containing	
indicating supported hash algorithm (HASH_ALG)	
	ining signature
calcula	ated using the HASH_ALG and private key correspondent to the AA_PUB_V_KEY

TP ld	SECPKI AA AUTHVAL 05 BV
Summary	Check that the AA sends signed AuthorizationValidationRequestMessage using proper
	signed data headers
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with	
the AA in 'operatio	nal' state
authorized with	n CERT_AA certificate
containing	verificationKey (AA_PUB_V_KEY)
and the EA in 'ope	rational' state
authorized with	CERT_EA certificate
ensure that	
when	
	ered to send the authorization validation request to the EA
then	
	a EtsiTs103097Data-Encrypted message
	EtsiTs103097Data-Signed
	ng signedData
	aining 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
-	

TP ld	SECPKI_AA_AUTHVAL_06_BV
Summary	Check that the AA sends AuthorizationValidationRequestMessage version 1
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
then	to send the authorization validation request to the EA Ts103097Data-Encrypted message s102941Data rsion

TP Id	SECPKI AA AUTHVAL 07 BV
	Check that the AA sends the AuthorizationValidationRequestMessage with
Summany	sharedAtRequest and ecSignature as it was requested in the triggering of
Summary	
Deference	authorization request
Reference	ETSI TS 102 941 [1], clause 6.2.3.4.1
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with	
the AA in 'operational' st	tate
and the EA in 'operation	al' state
ensure that	
when	
	AuthorizationRequestMessage
containing EtsiTs	
	ontent.authorizationRequest
	g sharedAtRequest (SHARED_AT_REQUEST)
	aining ecSignature (EC_SIGNATURE)
then	
	Ts103097Data-Encrypted message
containing EtsiTs	
	ntent.authorizationValidationRequest
	g sharedAtRequest
indicating SHARED_AT_REQUEST	
	aining ecSignature
indicat	ting EC_SIGNATURE

TP ld	SECPKI_AA_AUTHVAL_08_BV
Summary	Check that signing of authorization validation request is permitted by the AA certificate
Reference	ETSI TS 102 941 [1], clause B.5
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with	
the AA in 'operation	nal' state
and the EA in 'ope	rational' state
ensure that	
when	
the IUT is trigge	ered to send the authorization validation request to the EA
then	
	an EtsiTs103097Data-SignedAndEncrypted structure
containing	
	d as a digest
	ning the HashedId8 of the AA certificate
CO	ntaining appPermissions
	containing an item of type PsidSsp
	containing psid
	indicating AID_CERT_REQ
	and containing ssp
	containing opaque[0] (version)
	indicating 1
	containing opaque[1] (value)
	indicating 'Enrolment Request' (bit 1) set to 1

5.5.3 Authorization validation response handling

TP ld	SECPKI_AA_AUTHVAL_RCV_01_BV
Summony	Check that the AA sends the authorization response after receiving the
Summary	AuthorizationRequestMessage
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
and the IUT sent the Au ensure that when the IUT received the then	state

TP ld	SECPKI_AA_AUTHVAL_RCV_02_BI
	Check that AA does not accept the authorization validation response when the
Summary	AuthorizationValidationResponseMessage is signed with certificate without appropriate
	permissions
Reference	ETSI TS 102 941 [1], clause B.5
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with	
the ITS-S in 'enrolled' sta	
the EA in 'operational' st	
and the IUT(AA) in 'oper	
	d the AuthorizationRequest from the ITS-S
	thorizationValidationRequest
ensure that	
when	
	AuthorizationValidationResponseMessage
containing signer	
containing diges	
	shedId8 of the certificate
	appPermissions
	aining an item of type PsidSsp
	dicating AID_CERT_REQ
	ntaining an item of type PsidSsp
	ntaining psid
	indicating AID_CERT_REQ d containing ssp
an	containing opaque[0] (version)
	indicating other value than 1
	or containing opaque[1] (value)
	indicating 'AuthorizationValidationResponse' (bit 4) set to 0
then	indicating Automzation validation coponed (bit 4) set to 0
	an AuthorizationValidationResponseMessage
containing respons	
indicating non-z	

5.5.4 Authorization response

TP ld	SECPKI_AA_AUTH_01_BV
Summary	Check that the AA sends encrypted authorization response
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with	
the ITS-S in 'enrolled	J' state
has sent the Auth	norizationRequestMessage
containing en	crypted enkKey
containing	g AES symmetric key (SYM_KEY)
the EA in 'operationa	al' state
ensure that	
when	
	ed to send the authorization response to the ITS-S
then	
	e EtsiTs103097Data-Encrypted message
5	ntent.encryptedData
	g recipients of size 1
	ning the instance of RecipientInfo
COr	ntaining pskRecipInfo
	indicating HashedId8 of the SYM_KEY
	ining cyphertext
encryp	bted using SYM_KEY
TP ld	SECPKI_AA_AUTH_02_BV
Summary	Check that the AA sends signed authorization response

I P Id	SECPKI_AA_AUTH_02_BV
Summary	Check that the AA sends signed authorization response
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
Configuration	CFG_AUTH_AA
PICS Selection	
Expected behaviour	
with	
the ITS-S in 'enrolled' state	
and the IUT(AA) in 'operational' state	
authorized with CERT_AA certificate	
and the EA in 'operational' state	
ensure that	
when	
the IUT is triggered to send the authorization response to the ITS-S	
then	
the IUT sends the EtsiTs103097Data-Encrypted message	
containing the EtsiTs103097Data-Signed	
containing signedData	
containing signer	
containing digest	
indicating HashedId8 value of the CERT_AA	

TP ld	SECPKI_AA_AUTH_03_BV
Summary	Check that the AA sends signed authorization response with signature properly calculated
	using approved hash algorithm
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with	
the ITS-S in 'enroll	led' state
and the IUT(AA) in	n 'operational' state
authorized with	n CERT_AA certificate
containing	verificationKey (AA_PUB_V_KEY)
and the EA in 'ope	orational' state
ensure that	
when	
the IUT is trigg	ered to send the authorization response to the ITS-S
then	
	nds the EtsiTs103097Data-Encrypted message
	the EtsiTs103097Data-Signed
	ing signedData
	aining hashId
	ndicating supported hash algorithm (HASH_ALG)
	containing signature
(calculated using the HASH_ALG and private key correspondent to the AA_PUB_V_KEY
TP ld	SECPKI_AA_AUTH_04_BV
Summary	Check that the AA sends signed AuthorizationResponseMessage using valid ITS AID and
	only allowed headers.
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
Configuration	CFG_AUTH_AA

Configuration	CFG_AUTH_AA	
PICS Selection		
	Expected behaviour	
with		
the ITS-S in 'enrolled	' state	
and the IUT(AA) in 'o		
and the EA in 'operat	ional' state	
ensure that		
when		
the IUT is triggered to send the authorization response to the ITS-S		
then		
	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_AUTH_05_BV	
Summary		tionResponse with signature properly calculated
Summary	using approved hash algorithm	
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2	
Configuration	CFG_AUTH_AA	
PICS Selection	X_PICS	
	Expected behaviour	
with		
the ITS-S in 'e		
	e AuthorizationRequestMessage	
	ng EtsiTs102941Data	
	aining authorizationResponse	
	containing X_DATA_STRUCTURE	
	A) in 'operational' state	
ensure that	operational' state	
when		
	riggered to send the authorization response to the IT	·S-S
then	nggered to send the dutionzation response to the ri	
	nds a EtsiTs103097Data-Encrypted message	
	ing EtsiTs103097Data-Signed	
	aining EtsiTs102941Data	
(containing authorizationResponse	
	containing requestHash	
	indicating the leftmost 16 bits of the SHA256	
	calculated over the X_DATA_STRUCTUR	E
	and containing responseCode	
	Variants	
nn	X_PICS	X_DATA_STRUCTURE
1	PICS_PKI_AUTH_POP NOT PICS_PKI_AUTH_POP	EtsiTs103097Data-Signed
2		EtsiTs102941Data

TP ld	SECPKI_AA_AUTH_06_BV
Summary	Check that the AA includes the certificate in the positive authorization response
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with	
the ITS-S in 'enrolled' sta and the ITS-S has sent t and the IUT(AA) in 'oper and the EA in 'operation ensure that when	the AuthorizationRequestMessage rational' state
the IUT is sending to containing respor indicating 0	the ITS-S the AuthorizationResponseMessage (MSG) nseCode
then	
the message MSG	
containing certific	cate

TP ld	SECPKI AA AUTH 07 BV
Summary	Check that the AA does not include the certificate in the negative authorization response
Reference	ETSI TS 102 941 [1], clause 6.2.3.3.2
Configuration	CFG_AUTH_AA
PICS Selection	
	Expected behaviour
with	
the ITS-S in 'enrolled'	state
and the ITS-S has se	nt the AuthorizationRequestMessage
and the IUT(AA) in 'o	perational' state
and the EA in 'operati	onal' state
ensure that	
when	
the IUT is sending	to the ITS-S the AuthorizationResponseMessage (MSG)
containing res	ponseCode
indicating r	negative value
then	
the message MSC	
not containing	certificate

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

TP ld	SECPKI AA AUTH 09 BV
Summary	Check that generated AT certificate contains only allowed permissions
Reference	ETSI TS 102 941 [1], clause B.5
Configuration	CFG_ENR_EA
PICS Selection	
	Expected behaviour
ensure that	
when	
the IUT is requested	to send an authorization response
containing a certifie	cate (AT_CERT)
then	
	thorizationResponseMessage
containing author	
	rtificate (AT_CERT)
	appPermissions
	ontaining an item of type PsidSsp
COI	ntaining psid
	indicating AID_CERT_REQ
	taining an item of type PsidSsp
COI	ntaining 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 N	OT containing an item of type PsidSsp
	ntaining psid
	indicating AID_CRL

5.5.5 CA Certificate Request

TP ld	SECPKI_AA_CERTGEN_01_BV		
Summers	SubCA certificate requests of the AA are transported to the RCA using		
Summary	CACertificateRequestMessage structures across the reference point \$9		
Reference	ETSI TS 102 941 [1], clause 6.2.1		
Configuration	CFG_CAGEN_INIT		
PICS Selection			
	Expected behaviour		
ensure that	ensure that		
when			
the IUT is requ	lested to send a CA certificate request		
then			
the IUT sends	a CACertificateRequestMessage		
across the	reference point S9 to the RCA		

TP ld	SECPKI_AA_CERTGEN_02_BV
Summary	The application form should include the digital fingerprint of the CACertificateRequestMessage in printable format. The digital fingerprint of the CACertificateRequestMessage is computed using a ETSI TS 103 097 [2] approved hash algorithm
Reference	ETSI TS 102 941 [1], clause 6.2.1 ETSI TS 103 097 [2], clause 7
Configuration	CFG_CAGEN_INIT
PICS Selection	
	Expected behaviour
then the IUT sends a C containing a sig being compu	ed to send a CA certificaterequest

TP ld	SECPKI_AA_CERTGEN_03_BV
Summary	The hashId shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [2], the signer is set to 'self' and the signature over the tbsData is computed using the private key corresponding to the new verificationKey to be certified (i.e. the request is self-signed)
Reference	ETSI TS 102 941 [1], clause 6.2.1 ETSI TS 103 097 [2], clause 7
Configuration	CFG_CAGEN_INIT
PICS Selection	
	Expected behaviour
with the IUT being in the 'initi	al' state
ensure that	
when	
	to send a CA certificate request
then	
the IUT sends a CAC	CertificateRequestMessage
	03097Data-Signed structure
containing has	nld
	e hash algorithm to be used
and containing	
indicating 'self'	
and containing tbsData	
	aCertificateRequest
	g publicKeys
	ning verification_key (VKEY)
and containing	
computed or	ver tbsData using the private key corresponding to the verificationKey (VKEY)

TP ld	SECPKI_AA_CERTGEN_04_BV
Summary	An ECC private key is randomly generated, the corresponding public key (verificationKey) is provided to be included in the CaCertificateRequestMessage An ECC encryption private key is randomly generated, the corresponding public key
	(encryptionKey) is provided to be included in the CACertificateRequestMessage caCertificateRequest.publicKeys shall contain verification_key and encryption_key
Reference	ETSI TS 102 941 [1], clause 6.2.1
Configuration	CFG_CAGEN_INIT
PICS Selection	
	Expected behaviour
with	
the IUT being in the 'init	tial' state
ensure that	
when	
the IUT is requested	to send a CA certificate request
then	
the IUT sends a CA	CertificateRequestMessage
containing caCe	rtificateRequest
containing pub	licKeys
	verification lieu

containing verification_key and containing encryption_key

TP ld	SECONI AA CERTCEN OF DV		
	SECPKI_AA_CERTGEN_05_BV		
Summary	The EtsiTs102941Data structure is built with version set to v1 (integer value set to 1)		
Reference	ETSI TS 102 941 [1], clause 6.2.1		
Configuration	CFG_CAGEN_INIT		
PICS Selection			
	Expected behaviour		
with			
the IUT being in t	he 'initial' state		
ensure that			
when			
the IUT is req	uested to send a CA certificate request		
then			
the IUT sends a CACertificateRequestMessage			
containing EtsiTs102941Data			
containing version			
	indicating v1 (integer value set to 1)		

TP ld	SECPKI_AA_CERTGEN_06_BV	
Cummons.	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	sted to send a CA certificate request	
then		
the IUT sends a CACertificateRequestMessage		
containing CaCertificateRequest		
containing requestedSubjectAttributes		
as specified in ETSI TS 103 097 [2], clause 7.2.4		

TP ld	SECPKI_AA_CERTGEN_07_BV	
Summary EtsiTs103097Data-Signed.tbsData contains the EtsiTs102941Data as payload and headerInfo containing psid and generationTime. The psid shall be set to "secured certificate request" as assigned in ETSI TS 102 965 [8] and the generationTime sh present. All other components of the component tbsdata.headerInfo are not used a 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	ne 'initial' state	
	uested to send a CA certificate request	
containing containin	a CACertificateRequestMessage headerInfo g psid ting SEC_CERT_REQ	

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

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

TP ld	SECPKI_AA_CERTGEN_09_BV	
Summary	For the re-keying application to the RCA (CaCertificateRekeyingMessage), an EtsiTs103097Data-Signed structure is built, containing: hashId, tbsData, signer and signature. The hashId shall indicate the hash algorithm to be used as specified in ETSI TS 103 097 [2]. The signer declared as a digest, containing the hashedId8 AA certification 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 CA being an Etsi containing indicatin and contain and contain declared indicat	g the hash algorithm to be used ning tbsData ning signer d as digest ting the hashedId8 of the SubCA certificate (CA_CERT)	
compute	ning signature ed over tbsData	
using	the private key corresponding to CA_CERT	

ld SECPKI_AA_CERTGEN_10_BV		
Summary	The (outer) tbsData of the CACertificateRekeyingMessage shall contain the	
i i i i i ai y	CaCertificateRequestMessage as payload	
ference	ETSI TS 102 941 [1], clause 6.2.1	
nfiguration	CFG_CAGEN_REKEY	
CS Selection		
pected behaviour		
h		
the IUT being in the 'op	perational' state	
sure that		
when		
the IUT is requested to perform a CA certificate rekeying procedure		
then		
the sends a CACertificateRekeyingMessage		
containing tbsData		
containing CaCertificateRequestMessage		

TP ld	SECPKI_AA_CERTGEN_11_BV
Summary The (outer) tbsData of the CACertificateRekeyingMessage shall contain a headerIn containing psid and generationTime. The psid shall be set to "secured certificate re as assigned in ETSI TS 102 965 [8] and the generationTime shall be present. All of 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 the sends a CA containing the containing h containin indicat and cont	neaderInfo

TP ld	SECPKI_AA_CERTGEN_12_BV		
Summary			
Reference	e ETSI TS 102 941 [1], clause 6.2.1		
Configuration	CFG_CAGEN_REKEY		
PICS Selection			
	Expected behaviour		
with			
the IUT being in the 'ope	erational' state		
ensure that			
when			
	to perform a CA certificate rekeying procedure		
then			
	ficateRekeyingMessage		
	3097Data-Signed structure		
and containing the			
and containing dia			
containing dig			
	ashedId8 of the currently using AA certificate		
	containing appPermissions		
containing an item of type PsidSsp containing psid			
indicating AID_CERT_REQ			
and containing ssp			
containing opaque[0] (version)			
indicating 1			
containing opaque[1] (value)			
	indicating 'CA Certificate Response' (bit 6) set to 1		
L			

5.5.6 Authorization using butterfly key expansion mechanism

TP ld	SECPKI_AA_BFK_AUTH_01_BV	
	Check that the AA sends the butterfly certificate response message after receiving of the	
Summony	butterfly certificate request	
Summary	Check that this message is encrypted using the same symmetric encryption key as the	
	butterfly certificate request message	
Reference	ETSI TS 102 941 [1], clauses 6.2.3.5.1 and 6.2.3.5.5	
Configuration	CFG_BFK_AUTH_AA	
PICS Selection		
	Expected behaviour	
with	•	
the AA in 'operation	al' state	
	CERT AA certificate	
ensure that		
when		
the IUT received	the ButterflyCertificateRequestMessage	
	ontent.encryptedData.recipients	
	g the instance of RecipientInfo	
	ining certRecipInfo	
	ontaining recipientId	
	indicating HashedId8 of the CERT_AA	
ar	nd containing encKey	
	containing encrypted symmetric encryption key (ENC_KEY)	
then		
the IUT sends to	o the EA a EtsiTs103097Data-Encrypted	
containing co	ontent.encryptedData.recipients	
indicating	g size 1	
and cont	aining the instance of RecipientInfo	
	ining pskRecipInfo	
in	dicating HashedId8 of the ENC_KEY	
TP ld	SECPKI_AA_BFK_AUTH_02_BV	
0	Check that the butterfly certificate response message is signed using AA certificate	
Summary	Check that the message signature is valid	
Reference	ETSI TS 102 941 [1], clauses 6.2.3.5.1 and 6.2.3.5.5	
Configuration	CFG_BFK_AUTH_AA	
PICS Selection		
	Expected behaviour	
with		
the AA in 'operation	al' state	
	CERT_AA certificate	
ensure that		
when		
	EA received the ButterflyCertificateRequestMessage	
then		
	the EA a EtsiTs103097Data-Encrypted	
	ontent.encryptedData.ciperText	
	g EtsiTs103097Data-Signed	
	ining signedData	
CC	ontaining signer	
	containing digest	
indicating HashedId8 value of the CERT_AA		

5.5.6.1 Butterfly certificate response

and containing signature validated using CERT_AA verification public key

TP ld	SECPKI AA BFK AUTH 03 BV	
	Check that the butterfly certificate response message contains all necessary fields	
	Check that the acaResponse in the butterfly certificate response encrypted using valid	
Summary	encryption key	
	Check that the acaResponse in the butterfly certificate response is signed using valid	
	verification key	
Reference	ETSI TS 102 941 [1], clauses 6.2.3.5.1 and 6.2.3.5.5	
Configuration	CFG_BFK_AUTH_AA	
PICS Selection		
	Expected behaviour	
with		
the AA in 'operation		
	CERT_AA certificate	
ensure that		
when		
	d from the EA the ButterflyCertificateRequestMessage (REQ)	
then		
	o the EA a ButterflyCertificateResponseMessage	
	ontent.encryptedData.ciperText	
	ng EtsiTs103097Data-Signed	
	aining signedData.tbsData ontaining headerInfo	
	containing psid	
	indicating AID_PKI_CERT_REQUEST	
	and containing generation Time	
and not containing other fields		
and containing payload		
containing EtsiTs102941Data		
containing butterflyCertificateResponse		
indicating AcaRaCertResponse		
containing version		
indicating 2		
and containing generationTime		
	indicating value between the REQ generation time and the current time	
	and containing requestHash	
	indicating the left-most 16 octets of the SHA256 digest of the REQ	
	and containing acaResponse	
	containing private	
	indicating the AcaEeCertResponsePrivateSpdu	

TP ld	SECPKI_AA_BFK_AUTH_04_BV		
Summary	Check that the butterfly certificate response message contains AT certificate, encrypted with a		
Summary	properly derived key		
Reference	rence ETSI TS 102 941 [1], clauses 6.2.3.5.1 and 6.2.3.5.5		
Configuration	CFG_BFK_AUTH_AA		
PICS Selection			
	Expected behaviour		
with			
the AA in 'operatio	nal' state		
authorized with	n CERT_AA certificate		
ensure that			
when			
	ed from the EA the ButterflyCertificateRequestMessage (REQ)		
	ButterflyCertRequest		
containi	ng certEncKey (ITSS_ENC_KEY)		
then			
	to the EA a ButterflyCertificateResponseMessage		
containing t	the AcaEeCertResponsePrivateSpdu		
	ng content.signedData		
	aining signer.digest		
	ndicating HashedId8 of CERT_AA		
	aining tbsData.payload		
containing leee1609Dot2Data-Encrypted			
containing content.encryptedData.recepients			
	indicating size 1		
and containing the instance of RecipientInfo			
	containing rekRecipInfo		
	containing recipientId		
	indicating HashedId8 of the ITSS_ENC_KEY		

5.6 RootCA behaviour

5.6.0 Overview

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

PICS_SECPKI_IUT_RCA = TRUE

5.6.1 CTL generation

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

1:	21	
----	----	--

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

TP ld	SECPKI_RCA_CTLGEN_02_BV
Summary	Check that the RootCA generates the Delta CTL when new EA is about to be added to the
	Root CTL
Reference	ETSI TS 102 941 [1], clauses 6.3.2 and 6.3.4
Configuration	CFG_CTLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	
when	
the RootCA is	triggered to add new EA certificate (CERT_EA) in the CTL
then	
the IUT issues	a new CTL of type CtlFormat
containing	isFullCtl
	ng FALSE
and contain	ning ctlCommands
contain	ing CtlCommand
con	taining add
	containing ea
	containing eaCertificate
	indicating 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
ensure that	
when	
the RootCA is trigge	ered to delete EA certificate (CERT_EA) from the CTL
then	
the IUT issues a ne	w CTL of type CtlFormat
containing isFull	Ctl
indicating TF	RUE
and containing o	ctlCommands
not containin	g CtlCommand
containin	
conta	ining ea
	ontaining eaCertificate
	indicating CERT_EA

TP ld	SECPKI_RCA_CTLGEN_04_BV
Summary	Check that the RootCA generates the Delta CTL when EA certificate is about to be deleted
Reference	ETSI TS 102 941 [1], clauses 6.3.2 and 6.3.4
Configuration	CFG_CTLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	
when	
the RootCA is trigge	red to delete EA certificate (CERT_EA) from the CTL
then	
the IUT issues a nev	v CTL of type CtlFormat
containing isFull	Ctl
indicating FA	LSE
and containing ct	tlCommands
not containing	g CtlCommand
containing	delete
-	ning cert
inc	licating Hashedid8 of CERT_EA

TP ld	SECPKI_RCA_CTLGEN_05_BV
Summary	Check that the RootCA generates the Full CTL when EA access point is about to be
	changed
Reference	ETSI TS 102 941 [1], clause 6.3.2
Configuration	CFG_CTLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	
when	
the RootCA is trigg	gered to add new EA access point URL (URL) to the CTL
then	
	ew CTL of type CtlFormat
containing isFu	
indicating T	
containing ctlC	
	CtlCommand
contain	
	taining ea
	containing eaCertificate (CERT_EA) and containing itsAccessPoint
	indicating URL
and NOT c	ontaining any other CtlCommand
contain	
	aining ea
	containing eaCertificate
	indicating 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 trigge	ered to add new EA access point URL (URL) to the CTL
then	
the IUT issues a new	w CTL of type CtlFormat
containing isFull	
indicating FA	
containing ctlCo	
containing C	
containin	
	ining ea
	ontaining eaCertificate (CERT_EA)
ar	nd containing itsAccessPoint
	indicating URL
TP ld	SECPKI_RCA_CTLGEN_07_BV
Summers	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	
the RootCA is trigge	ered to add new URL for EA-AA communication (URL) to the CTL
then	
	w CTL of type CtlFormat
containing isFull	
indicating TR	
containing ctlCo	
containing C	
containin	
	ining ea
	ontaining eaCertificate (CERT_EA)
CC	ontaining aaAccessPoint
	indicating URL
	ntaining any other CtlCommand
containin	g add
containin conta	g add ining ea
containin conta	g add

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

TP ld	SECPKI RCA CTLGEN 09 BV
Summary	Check that the RootCA generates the Full CTL when new AA is about to be added to the
	Root CTL
Reference	ETSI TS 102 941 [1], clause 6.3.2
Configuration	CFG_CTLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	
when	
the RootCA is t	riggered to add new AA certificate (CERT_AA) in the CTL
then	
the IUT issues	a new CTL of type CtlFormat
containing i	sFullCtl
indicatir	ng TRUE
and contain	ing ctlCommands
containi	ng CtlCommand
cont	aining add
	containing aa
	containing aaCertificate
	indicating CERT_AA

TP ld	SECPKI_RCA_CTLGEN_10_BV
Summary	Check that the RootCA generates the Delta CTL when new AA is about to be added to the
	Root CTL
Reference	ETSI TS 102 941 [1], clauses 6.3.2 and 6.3.4
Configuration	CFG_CTLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	
when	
the RootCA is	triggered to add new AA certificate (CERT_AA) in the CTL
then	
the IUT issues	a new CTL of type CtlFormat
containing	isFullCtl
	ng FALSE
and contain	ning ctlCommands
contain	ing CtlCommand
con	taining add
	containing aa
	containing aaCertificate
	indicating CERT_AA

125

TP ld	SECPKI_RCA_CTLGEN_11_BV
Summary	Check that the RootCA generates the Full CTL when AA is about to be deleted from the
	Root CTL
Reference	ETSI TS 102 941 [1], clause 6.3.2
Configuration	CFG_CTLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	
when	
the RootCA is t	triggered to delete AA certificate (CERT_AA) from the CTL
then	
	a new CTL of type CtlFormat
containing i	
	ng TRUE
	ning ctlCommands
	taining CtlCommand
	aining add
C	containing aa
	containing aaCertificate
	indicating CERT_AA
TP ld	SECPKI_RCA_CTLGEN_12_BV
Summary	Check that the RootCA generates the Delta CTL when AA is about to be deleted from the Root CTL
Reference	ETSI TS 102 941 [1], clauses 6.3.2 and 6.3.4
Configuration	CFG_CTLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	
when	
the RootCA is t	triggered to delete AA certificate (CERT_AA) from the CTL
then	

en the IUT issues a new CTL of type CtlFormat containing isFullCtl indicating FALSE and containing ctlCommands not containing CtlCommand containing delete containing cert indicating HashedId8 of CERT_AA

126

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	triggered to add new URL for AA access point (URL) to the CTL
then	
the IUT issues	a new CTL of type CtlFormat
containing i	
	ng TRUE
	ctlCommands
	ing CtlCommand
cont	taining add
(containing aa
	containing aaCertificate
	containing accessPoint
	indicating URL
	T containing any other CtlCommand
	taining add
(containing aa
	containing aaCertificate
	indicating CERT_AA
TP ld	SECPKI_RCA_CTLGEN_14_BV
	Check that the RootCA generates the Delta CTL when AA access point URL is about to b

TP ld	SECPKI_RCA_CTLGEN_14_BV
Summary	Check that the RootCA generates the Delta CTL when AA access point URL is about to be
	changed
Reference	ETSI TS 102 941 [1], clause 6.3.2
Configuration	CFG_CTLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	
when	
the RootCA is	triggered to add new URL for AA access point (URL) to the CTL
then	
the IUT issues	a new CTL of type CtlFormat
containing	isFullCtl
indicati	ng TRUE
containing	ctlCommands
contain	ing CtlCommand
con	taining add
	containing aa
	containing aaCertificate
	containing access Daint
	containing accessPoint

TP ld	SECPKI_RCA_CTLGEN_15_BV
Summony	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 is	ssued the TLM CTL list
containing Roc	otCA certificate (CERT_RCA)
ensure that	
when	
	triggered to issue a new CTL
then	
	a new CTL of type RcaCertificateTrustListMessage
	signedData
	ing signer.digest
	ting HashedID8 of the RootCA certificate (CERT_RCA)
	ntaining appPermissions containing an item of type PsidSsp
	containing psid
	indicating AID_CTL
	and containing ssp
	containing opaque[0] (version)
	indicating 1
	containing opaque[1] (value)
	indicating 'TLM entries' (bit 0) set to 0
	indicating 'RCA entries' (bit 1) set to 0
	indicating 'EA entries' (bit 2) set to 1
	indicating 'AA entries' (bit 3) set to 1
	indicating 'DC entries' (bit 4) set to 1
NOTE: The EtsiTs	103097Data 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 I	nas issued the previous CTL of type CtlFormat		
containing ctlS			
indicating	indicating N		
ensure that	5		
when	when		
the RCA is tric	the RCA is triggered to issue a new CTL		
then	•		
the IUT issues a new CTL of type CtlFormat			
	containing ctlSequence		
indicati			

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 ctlSequer indicating 255 ensure that when the RCA is triggered then	to issue a new CTL v CTL of type CtlFormat

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	ensure that		
when	when		
the RCA is triggered to issue a new CTL at time T1			
then			
the IUT issues a new CTL of type CtlFormat			
containing nextUpdate			
indicating timestamp greater then T1			

TP 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	when		
the RCA is trigge	ered to issue a new CTL		
then	then		
the IUT issues a	the IUT issues a new CTL of type CtlFormat		
containing ctl	containing ctlCommands		
not containing any item of type CtlCommand			
containing add			
containing tIm			
or containing rca			

TP ld	SECPKI_RCA_CTLGEN_20_BV		
	Check that the RCA Delta CTL is generated at the same time as FullCTL		
Summary	Check that the RCA Delta CTL is a difference between correspondent Full CTL and the		
	previous Full CTL		
Reference	ETSI TS 102 941 [1], clause 6.3.2		
Configuration	CFG_CTLGEN_RCA		
PICS Selection			
	Expected behaviour		
with			
the RCA already issued	the previous CTL of type CtlFormat (CTL_FULL_PREV)		
containing isFullCtl			
indicating TRUE			
containing ctlSequer	ICE		
indicating N			
ensure that			
when			
the RCA is triggered	to issue a new CTL		
then			
	v CTL of type CtlFormat (CTL_FULL)		
containing isFull			
indicating TR			
•	and containing ctlSequence		
indicating N+1			
and the IUT issues a new CTL of type CtlFormat (CTL_DELTA)			
containing isFullCtl			
indicating FALSE			
and containing ctlSequence			
indicating N+			
containing ctlCon			
indicating diff	erence between CTL_FULL and CTL_FULL_PREV		

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

TP Id	SECPKI_RCA_CTLGEN_22_BV		
Summary	Check that the RCA Full CTL does not contain commands of type 'delete'		
Reference	ETSI TS 102 941 [1], clause 6.3.2		
Configuration	CFG_CTLGEN_RCA		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the IUT is trigg	the IUT is triggered to delete the CA from the CTL		
then	88		
the IUT issues	a new CTL of type CtlFormat (CTL_FULL)		
containing	isFullCtl		
indicati	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	the IUT is triggered to issue a new CTL		
then			
the IUT issues a new	CTL of type CtlFormat		
containing isFullC	containing isFullCtl		
	indicating TRUE		
and containing ctlCommands			
containing at least one ctlCommand			
containing add			
containing url			
indicating URL of the DC of the IUT			
containing cert			
cor	containing the item of type HashedId8		
indicating the HashedId8 of the IUT certificate			

5.6.2 CRL generation

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

TP ld	SECPKI_RCA_CRLGEN_01_BV		
Summary	Check that the RootCA generates the CRL signed with appropriate certificate		
Reference	ETSI TS 102 941 [1], clause 6.3.3		
Configuration	CFG_CRLGEN_RCA		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the RootCA is trigger	red to generate new CRL		
then			
the IUT generates th	e CertificateRevocationListMessage		
containing signer	containing signer		
	containing digest		
indicating Ha	shedId8 of RootCA certificate		
containing appPermissions			
	containing an item of type PsidSsp		
containing psid			
indicating AID_CRL			
and containing ssp			
containing opaque[0] (version)			
indicating 1			
NOTE: The 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 issues	a new CRL of type ToBeSignedCrl

and containing entries containing item of type CrlEntry indicating HashID8 of the CERT_CA

TD	
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 issue	d the CTL
containing the RCA	A certificate CERT_RCA
ensure that	
when	
the RootCA is trigg	pered to revoke itself
then	
the IUT issues a ne	ew CRL of type ToBeSignedCrl
containing entr	ies
containing i	tem of type CrlEntry
indicating HashID8 of the CERT_RCA	

Check that the CRL of the RCA is timestamped	
ETSI TS 102 941 [1], clause 6.3.3	
CFG_CRLGEN_RCA	
Expected behaviour	
ggered to issue a new CRL at the time T1	
new CRL of type ToBeSignedCrl isUpdate	
i	ETSI TS 102 941 [1], clause 6.3.3 CFG_CRLGEN_RCA Expected behaviour ggered to issue a new CRL at the time T1 new CRL of type ToBeSignedCrl

TP ld	SECPKI_RCA_CRLGEN_05_BV
Summary	Check that the RCA issues a new CRL when the previous one is expired
Reference	ETSI TS 102 941 [1], clause 6.3.3
Configuration	CFG_CRLGEN_RCA
PICS Selection	
	Expected behaviour
with	
the RCA already issue	d the CRL
containing nextUpc	ate
indicating time	l prev
ensure that	
when	
the Tprev is less th	an current time (Tcur)
then	
the IUT issues a ne	ew CRL of type ToBeSignedCrl
containing thisl	Jpdate
indicating tir	nestamp greater or equal to the Tcur
and containing	nextUpdate
indicating tir	nestamp greater than Tcur and greater than thisUpdate

TP ld	SECPKI_RCA_CRLGEN_06_BV
Summary	Check that the RootCA generates the CRL when its own certificate is about to be revoked
Reference	ETSI TS 102 941 [1], clause 6.3.3
Configuration	CFG_CRLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	
when	
the RootCA is	triggered to issue a new CRL
then	
the IUT issues	a new CRL of type ToBeSignedCrl
containing	entries
does no	ot containing item of type CrIEntry
indicating HashID8 of other RootCA	

TP Id	SECPKI_RCA_CRLGEN_07_BV
Summary	Check that the RootCA generates the CRL when CA certificate is about to be revoked
Reference	ETSI TS 102 941 [1], clause 6.3.3
Configuration	CFG_CRLGEN_RCA
PICS Selection	
	Expected behaviour
ensure that	
when	
the RootCA is trigge	ared to issue a new CRL
then	
the IUT issues a new	N CRL of type ToBeSignedCrl
and containing e	ntries
does not containing item of type CrIEntry	
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	
when	
the RCA is trigg	gered to issue a new CRL
then	
the IUT issues	a new CRL of type ToBeSignedCrl
containing v	
indicatin	g 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	
	ted to generate EA certificate
then	
the IUT generate	
containing ap	
	g an item of type PsidSsp
	ning psid
	licating AID_CERT_REQ
	ontaining ssp
COF	ntaining opaque[0] (version)
	indicating 1
COL	ntaining opaque[1] (value)
	indicating 'Authorization validation Response' (bit 4) set to 1 and indicating 'Enrolment Response' (bit 5) set to 1
	and indicating 'CA certificate request' (bit 6) set to 1
	and indicating other bits set to 0
and NOT	containing an item of type PsidSsp
	ning psid
	licating AID_CTL
	containing an item of type PsidSsp
	ning psid
	licating AID_CRL
	rtIssuePermissions
	an item of type PsidGroupPermissions
	ning eeType
	licating app
	ning subjectPermissions
	ntaining 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
Configuration	CFG_CAGEN_RCA
PICS Selection	Europeted helessieur
	Expected behaviour
ensure that	
when	to concrete AA partificate
then	I to generate AA certificate
	no cortificato
the IUT generates th containing appP	
	n item of type PsidSsp
containin	
	ting AID_CERT_REQ
	aining ssp
	ining opaque[0] (version)
	dicating 1
	ining opaque[1] (value)
ind	dicating 'Authorization validation Request (bit 2) set to 1
	d indicating 'Authorization Response' (bit 3) set to 1
	id indicating 'CA certificate request' (bit 6) set to 1
and indicating other bits set to 0	
and NOT containing an item of type PsidSsp	
containin	
indicating AID_CTL	
	ntaining an item of type PsidSsp
containin	ting AID_CRL
containing certls	
	n item of type PsidGroupPermissions
containin	
	ting app
	g subjectPermissions
	ining explicit
N	OT containing en item of type PsidSspRange
	containing psid
	indicating AID_CERT_REQ
or	containing en item of type PsidSspRange
	containing psid
	indicating AID_CERT_REQ
and containing sspRange	
containing bitmapSspRange containing sspBitmask	
	indicating FFh
	containing sspValue
	indicating 01h 00h
ar	Id NOT containing an item of type PsidSspRange
	containing psid
	indicating AID_CTL
ar	Id NOT containing an item of type PsidSsp
	containing psid
	indicating AID_CRL

135

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		
	Expected behaviour	
ensure that		
when		
	to generate RootCA certificate	
then		
the IUT generates th	ne certificate	
containing appPe		
	ng an item of type PsidSsp	
containing	g psid	
indica	ting AID_CERT_REQ	
	ig an item of type PsidSsp	
containing		
	ting AID_CTL	
	ining ssp of length 2	
	dicating 01h 38h	
	ng an item of type PsidSsp	
containing	ting AID_CRL	
	•	
	and containing ssp of length 1 containing opaque[0] (version)	
	indicating 1	
	ertIssuePermissions	
5	item of type PsidGroupPermissions	
containing		
indicating app		
containing subjectPermissions		
containing explicit		
containing en item of type PsidSspRange		
containing psid		
indicating AID_CERT_REQ		
	and containing sspRange	
containing bitmapSspRange		
containing sspBitmask of length 2		
indicating FFh FFh containing sspValue of length 2		
indicating 01h FEh		
and NOT containing an item of type PsidSspRange		
containing psid		
	indicating AID_CTL	
an	d NOT containing an item of type PsidSsp	
	containing psid	
	indicating AID_CRL	

5.7 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		
the TLM issued a new CRL		
ensure that		
when	when	
the ITS-S asks the IUT for the newly issued CRL		
then		
the IUT is answered with this CRL		

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

5.8 TLM behaviour

5.8.1 CTL generation

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

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

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

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 trigg	gered to delete RootCA certificate (CERT_RCA) from the CTL
then	
the IUT issues	a new CTL of type CtlFormat
containing i	sFullCtl
indicatir	ng 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 delete RootCA certificate (CERT_RCA) from the CTL
then	
the IUT issues a new CTL of type CtlFormat	
containing isFullCtl	
indicating FAI	LSE
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 trigg	pered to add new the TLM certificate (CERT_TLM) in the CTL
then	
the IUT issues	a new CTL of type CtlFormat
containing i	sFullCtl
indicatir	IN TRUE
	ing ctlCommands
not containing CtlCommand	
	aining 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	d to add new the TLM certificate (CERT_TLM) in the CTL
then	
the IUT issues a new CTL of type CtlFormat	
containing isFullCtl	
indicating FA	ALSE
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 issues a nev	v CTL of type CtlFormat	
containing isFull	containing isFullCtl	
indicating TRUE		
and containing cl	tlCommands	
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 change the CPOC URL in the CTL		
then	-		
the IUT issues a new CTL of type CtlFormat			
containing isFullCtl			
indicating FA	LSE		
and containing ctlCommands			
not containin	not containing CtlCommand		
containing add			
containing tlm			
containing accessPoint			
indicating URL			

TP ld	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			
FICS Selection	Expected behaviour		
ensure that			
when			
	d to issue a new CTL		
then			
the IUT issues a ne	w CTL of type TImCertificateTrustListMessage		
containing signe			
containing si	igner.digest		
	g HashedID8 of the TLM certificate (TLM_CERT)		
containing appPermissions			
containing an item of type PsidSsp			
(containing psid		
indicating AID_CTL			
ć	and containing ssp		
	containing opaque[0] (version)		
	indicating 1		
	containing opaque[1] (value) indicating 'TLM entries' (bit 0) set to 1		
	indicating 'RCA entries' (bit 1) set to 1		
	indicating 'EA entries' (bit 2) set to 0		
indicating 'AA entries' (bit 3) set to 0			
indicating 'DC entries' (bit 4) set to 1			
containing th	psData.payload.data		
containing OER-encoded EtsiTs103097Data structure			
containing OER-encoder EtsiTs102941Data structure			
containing content.certificateTrustListTIm			
containing ctlCommands			
	containing add		
	containing tlm		
	containing selfSignedTLMCertificate		
	indicating TLM_CERT		
NOTE: The EtsiTs1030	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 iss containing ctlSequer indicating N ensure that	ued the previous CTL of type CtlFormat nce		
when			
the TLM is triggered to issue a new CTL			
then			
the IUT issues a new CTL of type CtlFormat containing ctlSequence indicating N+1			

TP 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		
containing ctlSeque indicating 255 ensure that when the TLM is triggered then the IUT issues a ne	when the TLM is triggered to issue a new CTL then the IUT issues a new CTL of type CtlFormat containing ctlSequence		

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	ensure that			
when	when			
the TLM is triggered to issue a new CTL at time T1				
then				
the IUT issues a new CTL of type CtlFormat				
containing nextUpdate				
indicating timestamp greater then T1				

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

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

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

TP ld	SECPKI_TLM_ECTLGEN_16_BV		
Summary	nmary Check that the TLM Full CTL does not contain commands of type 'delete'		
Reference			
Configuration	CFG_CTLGEN_TLM		
PICS Selection			
	Expected behaviour		
ensure that			
when			
the IUT is trigg	gered to delete the CA from the CTL		
then			
the IUT issues	s a new CTL of type CtlFormat		
containing	isFullCtl		
indicating TRUE			
and containing ctlCommands			
NOT containing any item of type CtlCommand			
containing delete			

5.9 CPOC behaviour

TP 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 asks the IUT for the newly issued CTL then the IUT is answered with this CTL				

History

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