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

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

Reference
DTS/ITS-00546

Keywords
ITS, security, testing, TSS&TP

ETSI

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

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

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

Important notice

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

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

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

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

Contents

Intellectual Property Rights 5
Foreword 5
Modal verbs terminology 5
1 Scope 6
2 References 6
2.1 Normative references 6
2.2 Informative references 6
3 Definition of terms, symbols and abbreviations 7
3.1 Terms 7
3.2 Symbols 7
3.3 Abbreviations 7
4 Test Suite Structure (TSS) 8
4.1 Structure for Security tests 8
4.2 Test entities and states 8
4.2.1 ITS-S states 8
4.2.2 EA states 9
4.2.3 AA states 9
4.2.4 RootCA states 9
4.2.5 TLM states 9
4.3 Test configurations 10
4.3.1 Overview 10
4.3.2 Enrolment 10
4.3.2.1 Configuration CFG_ENR_ITSS 10
4.3.2.2 Configuration CFG_ENR_EA 10
4.3.3 Authorization 10
4.3.3.1 Configuration CFG_AUTH_ITSS 10
4.3.3.2 Configuration CFG_AUTH_AA 10
4.3.4 Authorization Validation 11
4.3.4.1 Configuration CFG_AVALID_AA 11
4.3.4.2 Configuration CFG_AVALID_EA 11
4.3.5 CA certificate generation 11
4.3.5.1 Configuration CFG_CAGEN_INIT 11
4.3.5.2 Configuration CFG_CAGEN_REKEY 11
4.3.5.3 Configuration CFG_CAGEN_RCA 11
4.3.6 ECTL generation 11
4.3.6.1 Configuration CFG_CTLGEN_TLM 11
4.3.6.2 Configuration CFG_CTLGEN_CPOC 12
4.3.7 Root CTL generation 12
4.3.7.1 Configuration CFG_CTLGEN_RCA 12
4.3.8 CRL generation 12
4.3.8.1 Configuration CFG_CRLGEN_RCA 12
5 Test Purposes (TP) 12
5.1 Introduction 12
5.1.1 TP definition conventions 12
5.1.2 TP Identifier naming conventions 12
5.1.3 Rules for the behaviour description 13
5.1.4 Sources of TP definitions 13
5.1.5 Mnemonics for PICS reference 13
5.2 ITS-S behaviour 14
5.2.0 Overview 14
5.2.1 Manufacturing 14
5.2.2 Enrolment 14
5.2.2.0 Overview 14
5.2.2.1 Enrolment request 14

5.2.2.2 Enrolment response handling 20
5.2.3 Authorization 20
5.2.3.0 Overview 20
5.2.3.1 Authorization request 21
5.2.3.2 Authorization response handling 28
5.2.4 CTL handling 29
5.2.5 CRL handling 30
5.3 EA behaviour 30
5.3.1 Enrolment request handling 30
5.3.2 Enrolment response 31
5.3.3 Authorization validation request handling 36
5.3.4 Authorization validation response 37
5.3.5 CA Certificate Request 41
5.4 AA behaviour 46
5.4.1 Authorization request handling 46
5.4.2 Authorization validation request 50
5.4.3 Authorization validation response handling 54
5.4.4 Authorization response 55
5.4.5 CA Certificate Request 59
5.5 RootCA behaviour 64
5.5.1 CTL generation 64
5.5.2 CRL generation 74
5.5.3 CA certificate generation 78
5.6 DC behaviour 80
5.7 TLM behavior 81
5.7.1 CTL generation 81
5.8 CPOC behavior 87
History 88

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

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

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

Modal verbs terminology

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

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

1 Scope

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

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

2 References

2.1 Normative references

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

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

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

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

[1] ETSI TS 102 941 (V1.3.1): "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management".

[2] ETSI TS 103 097 (V1.3.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".

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

[4] ETSI TS 103 525-1 (V1.1.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 1: Protocol Implementation Conformance Statement (PICS)".

2.2 Informative references

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

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

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

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

[i.2] ETSI TS 102 965 (V1.3.1): "Intelligent Transport Systems (ITS); Application Object Identifier (ITS-AID); Registration".

[i.3] ISO/IEC 9646-1 (1994): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 1: General concepts".

[i.4] ISO/IEC 9646-2 (1994): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 2: Abstract Test Suite specification".

[i.5] ISO/IEC 9646-6 (1994): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 6: Protocol profile test specification".

[i.6] ISO/IEC 9646-7 (1995): "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 7: Implementation Conformance Statements".

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

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

AID_CERT_REQ	"Secured certificate request service" ITS-AID
AID_CTL	"CTL service" ITS-AID
AID_CRL	"CRL service" ITS-AID

3.2 Symbols

Void.

3.3 Abbreviations

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

AA	Authorization Authority
AID	Application IDentifier
AID_CAM	ITS Application IDentifier for CAM
AID_DENM	Application Identifier for DENM
AID_GN	Application Identifier for general GeoNetworking messages
AT	Authorization Ticket
ATS	Abstract Test Suite
BO	exceptional BehaviOur
BV	Valid Behaviour
CAM	Co-operative Awareness Messages
CERT	CERTificate
DENM	Decentralized Environmental Notification Message
EA	Enrolment Authority
ECC	Elliptic Curve Cryptography
GN	GeoNetworking
ITS	Intelligent Transportation Systems
ITS-S	Intelligent Transport System - Station
IUT	Implementation Under Test
MSG	MesSaGe
PICS	Protocol Implementation Conformance Statement
SSP	Service Specific Permissions
TP	Test Purposes
TS	Test System
TSS	Test Suite Structure

4 Test Suite Structure (TSS)

4.1 Structure for Security tests

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

Table 1: TSS for Security Management

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

4.2 Test entities and states

4.2.1 ITS-S states

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

        - private key corresponding to the EC public encryption key;
        - private key corresponding to the EC public verification key.

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

4.2.2 EA states

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

4.2.3 AA states

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

4.2.4 RootCA states

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

4.2.5 TLM states

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

4.3 Test configurations

4.3.1 Overview

4.3.2 Enrolment

4.3.2.1 Configuration CFG_ENR_ITSS

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

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

TS: EA is emulated by TS.

4.3.2.2 Configuration CFG_ENR_EA

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

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

TS: ITS-S is emulated by the TS.

4.3.3 Authorization

4.3.3.1 Configuration CFG_AUTH_ITSS

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

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

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

4.3.3.2 Configuration CFG_AUTH_AA

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

- The profile information for the emulated ITS-S.

TS: ITS-S is emulated by the TS:

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

4.3.4 Authorization Validation

4.3.4.1 Configuration CFG_AVALID_AA

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

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

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

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

4.3.4.2 Configuration CFG_AVALID_EA

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

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

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

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

4.3.5 CA certificate generation

4.3.5.1 Configuration CFG_CAGEN_INIT

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

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

4.3.5.2 Configuration CFG_CAGEN_REKEY

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

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

4.3.5.3 Configuration CFG_CAGEN_RCA

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

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

4.3.6 ECTL generation

4.3.6.1 Configuration CFG_CTLGEN_TLM

IUT: TLM in the operational state

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

4.3.6.2 Configuration CFG_CTLGEN_CPOC

IUT: CPOC in the operational state

TS: TS checks generated CTL emulating http client of CPOC

4.3.7 Root CTL generation

4.3.7.1 Configuration CFG_CTLGEN_RCA

IUT: RCA in the operational state

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

4.3.8 CRL generation

4.3.8.1 Configuration CFG_CRLGEN_RCA

IUT: RCA in the operational state

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

5 Test Purposes (TP)

5.1 Introduction

5.1.1 TP definition conventions

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

5.1.2 TP Identifier naming conventions

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

Table 2: TP naming convention

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

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

5.1.3 Rules for the behaviour description

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

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

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

5.1.4 Sources of TP definitions

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

5.1.5 Mnemonics for PICS reference

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

Table 3: Mnemonics for PICS reference

Mnemonic	PICS item
PICS_SECPKI_IUT_ITSS	[4] A.3.1
PICS_SECPKI_IUT_EA	[4] A.4.2
PICS_SECPKI_IUT_AA	[4] A.4.3
PICS_SECPKI_IUT_RCA	[4] A.4.4
PICS_SECPKI_IUT_DC	[4] A.4.5
PICS_SECPKI_IUT_TLM	[4] A.4.6
PICS_SECPKI_IUT_CPOC	[4] A.4.7
PICS_SECPKI_ENROLMENT	[4] A.3.2 or A.5.1
PICS_SECPKI_REENROLMENT	[4] A.3.2.1 or A.5.2
PICS_SECPKI_AUTHORIZATION	[4] A.3.3 or A.6.1
PICS_SECPKI_AUTH_PRIVACY	[4] A.3.3.1 or A.6.3
PICS_SECPKI_AUTH_POP	[4] A.3.3.2 or A.6.2
PICS_SECPKI_AUTH_VALIDATION	[4] A.5.3
PICS_SECPKI_CRL	[4] A.9.5 or A.7.1
PICS_SECPKI_CRL_DOWNLOAD	[4] A.9.6
PICS_SECPKI_CTL	[4] A.9.3 or A.7.2
PICS_SECPKI_CTL_DELTA	[4] A.9.3.1 or A.7.2.1 or A.7.4.1
PICS_SECPKI_CTL_DOWNLOAD	[4] A.9.4
PICS_SECPKI_ECTL	[4] A.9.1 or A.8.1
PICS_SECPKI_DELTA	[4] A.9.1.1 or A.8.1.1 or A.8.2.1
PICS_SECPKI_ECTL_DOWNLOAD	[4] A.9.2 or A.8.3
PICS_SEC_SHA256	[3] S1.2.2.1.1 or S1.3.2.1.1
PICS_SEC_SHA384	[3] S1.2.2.1.2 or S1.3.2.1.2
PICS_SEC_BRAINPOOL_P256R1	[3] S1.2.2.4.1.2 or S1.3.2.4.1.2
PICS_SEC_BRAINPOOL_P384R1	[3] S1.2.2.4.2 or S1.3.2.4.2