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

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

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

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

Foreword

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

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

Modal verbs terminology

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

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

1 Scope

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

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

2 References

2.1 Normative references

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

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

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

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

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

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

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

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

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

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

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

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

2.2 Informative references

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

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

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

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

[i.2] Void.

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

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

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

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

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

[i.8] United Nations Statistics Division: "Standard country or area codes for statistical use (M49)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

AID_CERT_REQ: "Secured certificate request service" ITS-AID

AID_CRL: "CRL service" ITS-AID

AID_CTL: "CTL service" ITS-AID

3.2 Symbols

Void.

3.3 Abbreviations

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

AA	Authorization Authority
AES	Advanced Encryption Standard
AID	Application IDentifier

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

4 Test Suite Structure (TSS)

4.1 Structure for Security tests

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

Table 1: TSS for Security Management

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

4.2 Test entities and states

4.2.1 ITS-S states

- State 'initialized':
  - ITS-S in 'initialized' state is ready to perform the enrolment request.
  - ITS-S in 'initialized' state contains the following information elements:
    - Permanent Canonical Identifier (PCI);
    - public/private key pair for cryptographic purposes (canonical key pair);
    - the trust anchor (Root CA) public key certificate and the DC network address;
    - contact information for the EA which will issue certificates for the ITS-S:
      - network address;
      - public key certificate.

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

4.2.2 EA states

- State 'initial':
  - EA contains the following information elements:
    - the trust anchor (Root CA) public key certificate and the DC network address.
- State 'operational':

  - EA is ready to receive enrolment requests from ITS-S.
  - In addition to information elements enumerated in the 'initial' state, EA in the 'operational' state contains the following information elements:
    - public/private key pairs and EA certificate permitting issuing of enrolment certificates.

4.2.3 AA states

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

4.2.4 RootCA states

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

4.2.5 TLM states

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

4.3 Test configurations

4.3.1 Overview

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

4.3.2 Enrollment

4.3.2.1 Configuration CFG_ENR_ITS-S

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

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

TS: EA is emulated by TS.

4.3.2.2 Configuration CFG_ENR_EA

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

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

TS: ITS-S is emulated by the TS.

4.3.3 Authorization

4.3.3.1 Configuration CFG_AUTH_ITS-S

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

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

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

TS: AA is emulated by the TS.

4.3.3.2 Configuration CFG_AUTH_AA

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

- the profile information for the emulated ITS-S.

TS: ITS-S is emulated by the TS:

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

4.3.4 Authorization Validation

4.3.4.1 Configuration CFG_AVALID_AA

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

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

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

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

4.3.4.2 Configuration CFG_AVALID_EA

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

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

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

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

4.3.5 Authorization using butterfly key expansion mechanism

4.3.5.1 Configuration CFG_BFK_AUTH_ITS-S

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

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

TS: AA and EA are emulated by the TS.

4.3.5.2 Configuration CFG_BFK_AUTH_EA

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

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

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

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

4.3.5.3 Configuration CFG_BFK_AUTH_AA

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

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

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

- the AA certificate of the IUT.

4.3.6 CA certificate generation

4.3.6.1 Configuration CFG_CAGEN_INIT

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

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

4.3.6.2 Configuration CFG_CAGEN_REKEY

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

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

4.3.6.3 Configuration CFG_CAGEN_RCA

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

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

4.3.7 ECTL generation

4.3.7.1 Configuration CFG_CTLGEN_TLM

IUT: TLM in the operational state.

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

4.3.7.2 Configuration CFG_CTLGEN_CPOC

IUT: CPOC in the operational state.

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

4.3.8 Root CTL generation

4.3.8.1 Configuration CFG_CTLGEN_RCA

IUT: RCA in the operational state.

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

4.3.9 CRL generation

4.3.9.1 Configuration CFG_CRLGEN_RCA

IUT: RCA in the operational state.

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

4.3.10 ITS-S CRL/CTL handling

4.3.10.1 Configuration CFG_CXL_P2P

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

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

Neighbour ITS-S: is emulated by the TS.

RCA: is emulated by the TS.

DC: is emulated by the TS.

5 Test Purposes (TP)

5.1 Introduction

5.1.1 TP definition conventions

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

5.1.2 TP Identifier naming conventions

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