



**Intelligent Transport Systems (ITS);
Testing;
Conformance test specifications for ITS PKI management;
Part 3: Abstract Test Suite (ATS) and Protocol Implementation
eXtra Information for Testing (PIXIT)**

https://standards.iteh.ai/standards/etsi/etsi-ts-103-525-3-v1.1.1-2019-03
44f9-b9bd-61f538b6d04/preview

Reference

DTS/ITS-00547

Keywords

ATS, PIXIT, security, testing

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>

Copyright Notification

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

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

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

© ETSI 2019.

All rights reserved.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.

3GPP™ and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.

oneM2M™ logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners.

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

Contents

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.....	7
3 Definition of terms, symbols and abbreviations.....	7
3.1 Terms.....	7
3.2 Symbols.....	7
3.3 Abbreviations	7
4 Contents of the ITS Security Test Suite	8
5 Abstract Test Method	9
5.1 Introduction	9
5.2 Abstract protocol tester	9
5.3 Test Configuration.....	9
5.3.1 Introduction.....	9
5.3.2 PKI infrastructure	9
5.3.2.1 Overview.....	9
5.3.2.2 PKI certificate hierarchy	10
5.3.2.3 Test system settings.....	11
5.3.2.3.1 Test adapter settings	11
5.3.2.3.2 Test Suite Parameters	11
5.3.2.4 Certificate profiles.....	11
5.3.2.5 Certificate generation.....	12
5.3.2.6 Certificate installation.....	13
5.4 Test architecture	13
5.5 Ports and ASPs	13
5.5.1 Introduction.....	13
5.5.2 Primitives of the geoNetworkingPort	13
5.5.3 Primitives of the utPort.....	13
6 External functions	14
7 ATS conventions	14
7.1 Introduction	14
7.2 Testing conventions.....	14
7.2.1 Testing states	14
7.2.1.1 Initial states	14
7.2.1.2 Final state	14
7.3 Naming conventions.....	14
7.3.1 Introduction.....	14
7.3.2 General guidelines	15
7.3.3 ITS specific TTCN-3 naming conventions	16
7.3.4 Usage of Log statements.....	16
7.3.5 Test Case (TC) identifier	17
7.4 On line documentation	17
Annex A (informative): ATS in TTCN-3.....	19
A.1 TTCN-3 files and other related modules.....	19
Annex B (normative): Partial PIXIT pro forma for Security.....	20
B.1 The right to copy	20

B.2	Introduction	20
B.3	Identification summary.....	20
B.4	ATS summary	20
B.5	Test laboratory.....	21
B.6	Client identification.....	21
B.7	SUT	21
B.8	Protocol layer information.....	22
B.8.1	Protocol identification	22
B.8.2	IUT information	22
Annex C (normative):	PCTR pro forma for Security.....	24
C.1	The right to copy	24
C.2	Introduction	24
C.3	Identification summary.....	24
C.3.1	Protocol conformance test report.....	24
C.3.2	IUT identification	24
C.3.3	Testing environment.....	25
C.3.4	Limits and reservation	25
C.3.5	Comments.....	25
C.4	IUT Conformance status	25
C.5	Static conformance summary	26
C.6	Dynamic conformance summary.....	26
C.7	Static conformance review report.....	26
C.8	Test campaign report.....	26
C.9	Observations.....	26
History	27

iteh STANDARD PREVIEW
 (standards.itech.ai)
 Full standard:
<https://standards.itech.ai/catalog/standards/sst/66a2bf25-6162-44f9-b9bd-611538b6d047/etsi-ts-103-525-3-v1.1-2019-03>

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 3 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 parts of the Abstract Test Suite (ATS) for ITS PKI management as defined in ETSI TS 102 941 [2] in accordance with the relevant guidance given in ISO/IEC 9646-7 [i.6]. The objective of the present document is to provide a basis for conformance tests for security communication over GeoNetworking equipment giving a high probability of interoperability between different manufacturers' equipment.

The ISO standards 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 102 940: "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management".
- [2] ETSI TS 102 941 (V1.3.1): "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management".
- [3] ETSI TS 103 097 (V1.3.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".
- [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)".
- [5] ETSI TS 103 525-2 (V1.1.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 2: Test Suite Structure and Test Purposes (TSS & TP)".
- [6] ETSI TS 102 871-2 (V1.3.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 2: Test Suite Structure and Test Purposes (TSS & TP)".
- [7] ETSI TS 102 871-3 (V1.3.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking ITS-G5; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)".
- [8] ETSI TS 103 096-2: "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 2: Test Suite Structure and Test Purposes (TSS & TP)".
- [9] ETSI TS 103 096-3: "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)".

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: "Intelligent Transport Systems (ITS); Testing; Framework for conformance and interoperability testing".
- [i.2] ETSI TR 103 099 (V1.4.1): "Intelligent Transport Systems (ITS); Architecture of conformance validation framework".
- [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] OpenSSL Project Toolkit Library V1.0.1j.

NOTE: Available at www.openssl.org.

- [i.9] ETSI ES 201 873-1: "Methods for Testing and Specification (MTS); The Testing and Test Control Notation version 3; Part 1: TTCN-3 Core Language".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 103 097 [3], ETSI TS 103 525-1 [4], ETSI TS 103 525-2 [5], ETSI TS 102 871-3 [87], ISO/IEC 9646-6 [i.5] and ISO/IEC 9646-7 [i.6] apply.

3.2 Symbols

Void.

3.3 Abbreviations

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

AA	Authorization Authority
AID	Application ID
AT	Authorization Ticket

ATM	Abstract Test Method
ATS	Abstract Test Suite
BO	exceptional BehaviOur
BTP	Basic Transport Protocol
BV	Valid Behaviour tests
CAM	Cooperative Awareness Message
CPOC	Central Point Of Contact
CRL	Certificate Revocation List
CTL	Certificate Trust List
DC	Distribution Center
DEN	Decentralized Environmental Notification
DENM	Decentralized Environmental Notification Message
EA	Enrolment Authority
ECTL	European CTL
EN	European Norm
ENR	ENRolment
ES	ETSI Standard
GN	GeoNetworking
HTML	HyperText Markup Language
ISO	International Organization for Standardization
ITS	Intelligent Transport System
ITS-S	ITS-Station
ITSS	ITS-S data transfer
IUT	Implementation Under Test
PCTR	Protocol Conformance Testing Report
PICS	Protocol Implementation Conformance Statement
PIXIT	Partial Protocol Implementation eXtra Information for Testing
PKI	Public Key Infrastructure
PX	PiXit
RCA	Root Certificate Authority
SAP	Service Access Point
SCS	System Conformance Statement
SCTR	Static Conformance Test Report
SSP	Service Specific Permissions
SUT	System Under Test
TC	Test Case
TLM	Trust List Manager
TP	Test Purposes
TR	Technical Report
TS	Test System
TSS	Test Suite Structure
TTCN	Testing and Test Control Notation
UT	Upper Tester
XML	eXtensible Markup Language

4 Contents of the ITS Security Test Suite

The ITS Security test suite contains:

- test implemented in TTCN-3 code;
- certificate profiles and certificate generation tool.

To execute the ITS Security Test Suite a Test Adapter implementation and a TTCN-3 compiler is required. The reference Test Adapter implementation can be found at https://forge.etsi.org/gitlab/ITS/ITS/tags/TS103525-3_v1.1.1. TTCN-3 compilers can be acquired at <http://www.ttcn-3.org>.

5 Abstract Test Method

5.1 Introduction

This clause describes the ATM used to test the ITS-Pki framework.

5.2 Abstract protocol tester

The abstract protocol tester used by the ITS-Pki test suite is described in figure 1. The Test System simulates valid and invalid protocol behaviour and analyses the reaction of the IUT.

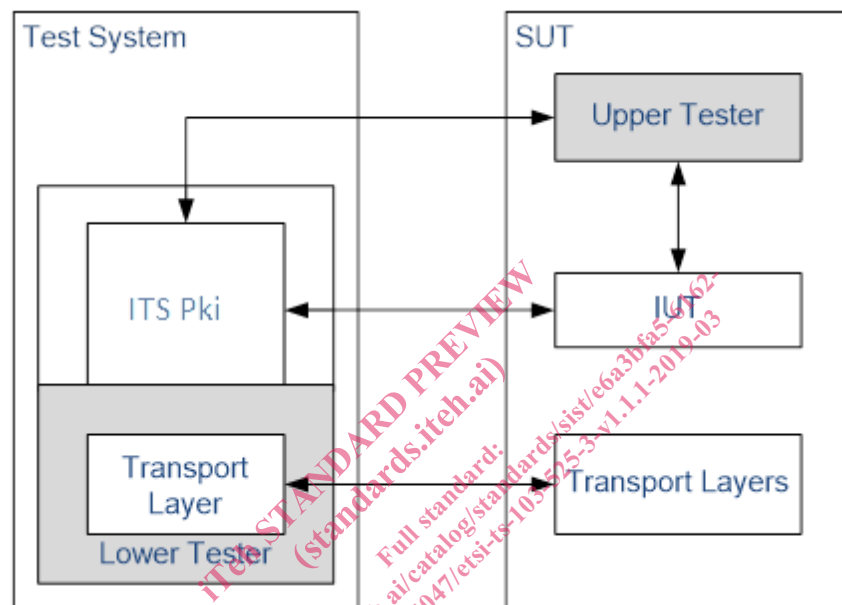


Figure 1: Abstract protocol tester - Pki

5.3 Test Configuration

5.3.1 Introduction

This test suite shall use test configurations as defined in ETSI TS 103 525-2 [5], i.e. the tester simulates the AA implementing the ITS Pki framework over HTTP protocol.

5.3.2 PKI infrastructure

5.3.2.1 Overview

Before executing tests:

- security certificates need to be generated, see clause 5.3.2.5;
- security certificates need to be installed onto the IUT, see clause 5.3.2.6; and
- some Test System settings need to be configured, see clause 5.3.2.3.

5.3.2.2 PKI certificate hierarchy

The required PKI certificate hierarchy of the test infrastructure shall be as specified in ETSI TS 102 940 [1] and ETSI TS 102 941 [2].

The following certificates are required for the test execution:

- 1) The custom user-generated root certificate, referred as `CERT_TEST_ROOT`, is used to sign all CA certificates used by the Test System and by the IUT to verify the Test System certificates. For the generation procedure see clause 5.3.2.5. The IUT shall install this `CERT_TEST_ROOT` certificate and consider it as trusted. In the case where the IUT cannot install the `CERT_TEST_ROOT`, no tests can be executed.
- 2) Further certificates to be installed on the IUT:
 - Option 1: Certificates (`CERT_TS_EA` and `CERT_IUT_AA`) can be installed onto the IUT. Please refer to clause 5.3.2.6 for further details on certificate installation.

If the IUT supports certificate selection using the `UtInitialize Upper Tester` command, than all mandatory tests can be executed and `PICS_CERTIFICATE_SELECTION` shall be set to true.

- Option 2: The IUT can only use its own pre-installed certificates. In this case only a subset of mandatory tests can be executed and `PICS_CERTIFICATE_SELECTION` shall be set to false.

In both cases it is necessary to copy these certificates to the subfolder of the location defined in `PX_CERTIFICATE_POOL_PATH`. The name of the subfolder shall be provided in `PX_IUT_SEC_CONFIG_NAME`.

It is not necessary to install IUT_ROOT and AA certificates onto the Test System when IUT and TS are using different PKIs. The TS trusts any root and AA certificate from the IUT.

A set of certificates and private keys to be used on the Test System side to sign various messages and other Test System certificates. These files are generated by the generation script (see clause 5.3.2.5).

All certificates and private keys shall be stored as hexadecimal streams.

The TS selects certificate using its file name. Table 1 describes file extensions to be used to store certificates and private keys.

Table 1: PKI file extensions

File extension	File role
.cert	Certificate
.vkey	Verification private key
.ekey	Encryption private key

Each Authorization Authority certificate contains:

- Start and End time
- Assurance level
- Permissions (AID list)
- Geographical Validity Restriction

Each Authorization Ticket certificate contains:

- Start and End time
- Assurance level
- Permissions (AID SSP list)
- Geographical Validity Restriction