ETSI TS 103 096-3 V1.2.1 (2015-09)

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f00afd63-052f-4487-805c-f10b1d0a0a09/etsi-ts-103-096-3-v1.2.1-2015-09

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)

Reference
RTS/ITS-00530

Keywords
ATS, ITS, testing, security

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f0bfdd63-03cf-448f-b95c-ff6d1cd0a639/etsi-ts-103-096-3-v1.2.1-2015-09

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 only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

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
http://portal.etsi.org/tb/status/status.asp

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.

© European Telecommunications Standards Institute 2015.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks 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 Definitions and abbreviations 7
3.1 Definitions 7
3.2 Abbreviations 7
4 Contents of the ITS Security Test Suite 8
5 Abstract Test Method 8
5.1 Introduction 8
5.2 Abstract protocol tester 8
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 9
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 12
5.3.2.5 Certificate generation 13
5.3.2.6 Certificate installation 13
5.4 Test architecture 14
5.5 Ports and ASPs 14
5.5.1 Introduction 14
5.5.2 Primitives of the geoNetworkingPort 14
5.5.3 Primitives of the utPort 14
6 External functions 15
7 Unimplemented test purposes 16
8 ATS conventions 18
8.1 Introduction 18
8.2 Testing conventions 18
8.2.1 Testing states 18
8.2.1.1 Initial states 18
8.2.1.2 Final state 18
8.3 Naming conventions 18
8.3.1 Introduction 18
8.3.2 General guidelines 18
8.3.3 ITS specific TTCN-3 naming conventions 19
8.3.4 Usage of Log statements 20
8.3.5 Test Case (TC) identifier 20
8.4 On line documentation 21
Annex A (informative): ATS in TTCN-3 22
A.1 TTCN-3 files and other related modules 22
Annex B (normative): Partial PIXIT pro forma for Security 23
B.1 Partial cancellation of copyright 23

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/00bafd63-052f-4487-805c-f10b1cd0a639/etsi-ts-103-096-3-v1.2.1-2015-09

B.2 Introduction 23
B.3 Identification summary 23
B.4 ATS summary 23
B.5 Test laboratory 23
B.6 Client identification 24
B.7 SUT 24
B.8 Protocol layer information 24
B.8.1 Protocol identification 24
B.8.2 IUT information 25

Annex C (normative): PCTR pro forma for Security 26

C.1 Partial cancellation of copyright 26
C.2 Introduction 26
C.3 Identification summary 26
C.3.1 Protocol conformance test report 26
C.3.2 IUT identification 26
C.3.3 Testing environment 26
C.3.4 Limits and reservation 27
C.3.5 Comments 27
C.4 IUT Conformance status 27
C.5 Static conformance summary 27
C.6 Dynamic conformance summary 27
C.7 Static conformance review report 28
C.8 Test campaign report 28
C.9 Observations 32
History 33

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/00afdf63-052f-4487-805c-f10b1cd0a639/etsi-ts-103-096-3-v1.2.1-2015-09

Intellectual Property Rights

IPRs essential or potentially essential to the present document 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 (http://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.

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 covering Conformance test specification for ITS Security as identified below:

Part 1: "Protocol Implementation Conformance Statement (PICS)";

Part 2: "Test Suite Structure and Test Purposes (TSS & TP)";

Part 3: "Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)".

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f00afd63-052f-4487-805c-f10b1cd6e650/etsi-ts-103-096-3-v1.2.1-2015-09

1 Scope

The present document provides parts of the Abstract Test Suite (ATS) for Security as defined in ETSI TS 103 097 [1] in accordance with the relevant guidance given in ISO/IEC 9646-7 [10]. 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 standard for the methodology of conformance testing (ISO/IEC 9646-1 [7] and ISO/IEC 9646-2 [8]) as well as the ETSI rules for conformance testing (ETSI ETS 300 406 [11]) 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 reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://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 103 097 (V1.2.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".

[2] 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)".

[3] 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)".

[4] ETSI TS 103 096-1 (V1.2.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)".

[5] ETSI TS 103 096-2 (V1.2.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 2: Test Suite Structure and Test Purposes (TSS & TP)".

[6] ETSI TR 103 099 (V1.3.1): "Intelligent Transport Systems (ITS); Architecture of conformance validation framework".

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

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

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

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ETSI standard:
https://standards.iteh.ai/catalog/standards/sist/f005fd63-521f-448a-85cc-10b1cd5c3050/etsi-ts-103-096-3-v1.2.1-2015-09

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

[12] OpenSSL Project Toolkit Library V1.0.1j.

NOTE: Available at www.openssl.org.

[13] 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".

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 reference 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".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms given in ETSI TS 103 097 [1], ETSI TS 102 871-2 [2], ETSI TS 102 871-3 [3], ISO/IEC 9646-6 [9] and ISO/IEC 9646-7 [10] apply.

3.2 Abbreviations

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

AA	Authorization Authority
AID	Application ID
ASP	Abstract Service Primitive
AT	Authorization Ticket
ATM	Abstract Test Method
ATS	Abstract Test Suite
BO	Inopportune Behaviour tests
BTP	Basic Transport Protocol
BV	Valid Behaviour tests
CAM	Cooperative Awareness Message
CERT	CERTificate testing
DEN	Decentralized Environmental Notification
DENM	Decentralized Environmental Notification Message
EN	European Norm
ES	ETSI Standard
GENMSG	GENeric MeSsaGes
GN	GeoNetworking
HSM	Hardware Security Module
HTML	HyperText Markup Language
ISO	International Organization for Standardization
ITS	Intelligent Transport System
ITSS	ITS-S data transfer
ITS-S	ITS Station
IUT	Implementation Under Test
MSG	Generic messages

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f00afd63-052f-4487-805c-f10b1cd0a039/etsi-ts-103-096-3-v1.2.1-2015-09

NB	Normal Behaviour
PCTR	Protocol Conformance Testing Report
PEM	Privacy Enhanced Mail

NOTE: Standard format for OpenSSL.

PICS	Protocol Implementation Conformance Statement
PIXIT	Partial Protocol Implementation eXtra Information for Testing
PKI	Public Key Infrastructure
PX	PiXit
RCV	ReCeiVing behaviour
SAP	Service Access Point
SCS	System Conformance Statement
SCTR	Static Conformance Test Report
SEC	SECurity
SND	SeNDing behaviour
SSP	Service Specific Permissions
SUT	System Under Test
TC	Test Case
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

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f00afd63-052f-4467-a05c-1f0b1cd0a639/etsi-ts-103-096-3-v1.2.1-2015-09

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 http://forge.etsi.org. 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-Security framework.

5.2 Abstract protocol tester

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

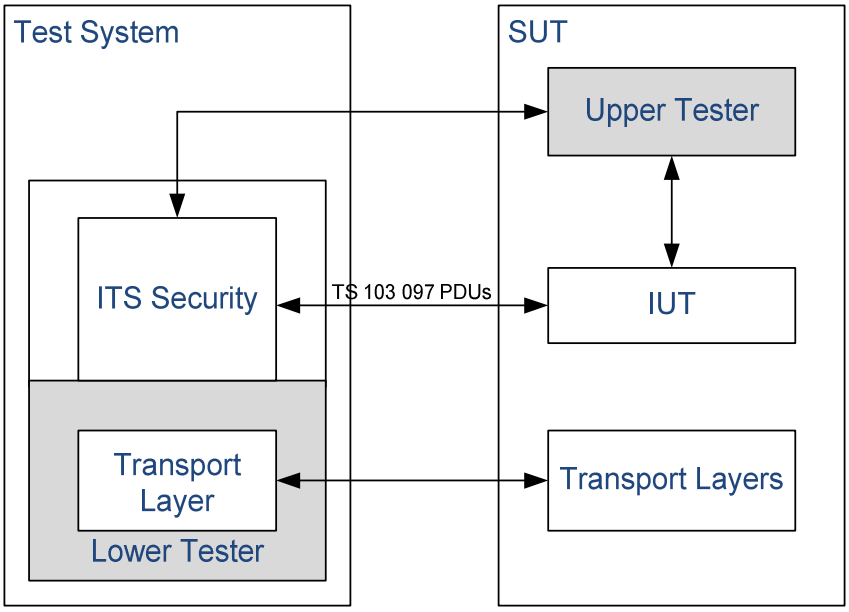

Figure 1: Abstract protocol tester - Security

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f00afd63-05f6-4487-805c-f10b1cd0a639/etsi-ts-103-096-3-v1.2.1-2015-09

5.3 Test Configuration

5.3.1 Introduction

This test suite uses test configurations defined in ETSI TS 102 871-3 [3], i.e. the tester simulates the ITS station implementing the ITS Security framework over GeoNetworking 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 is presented in figure 2.

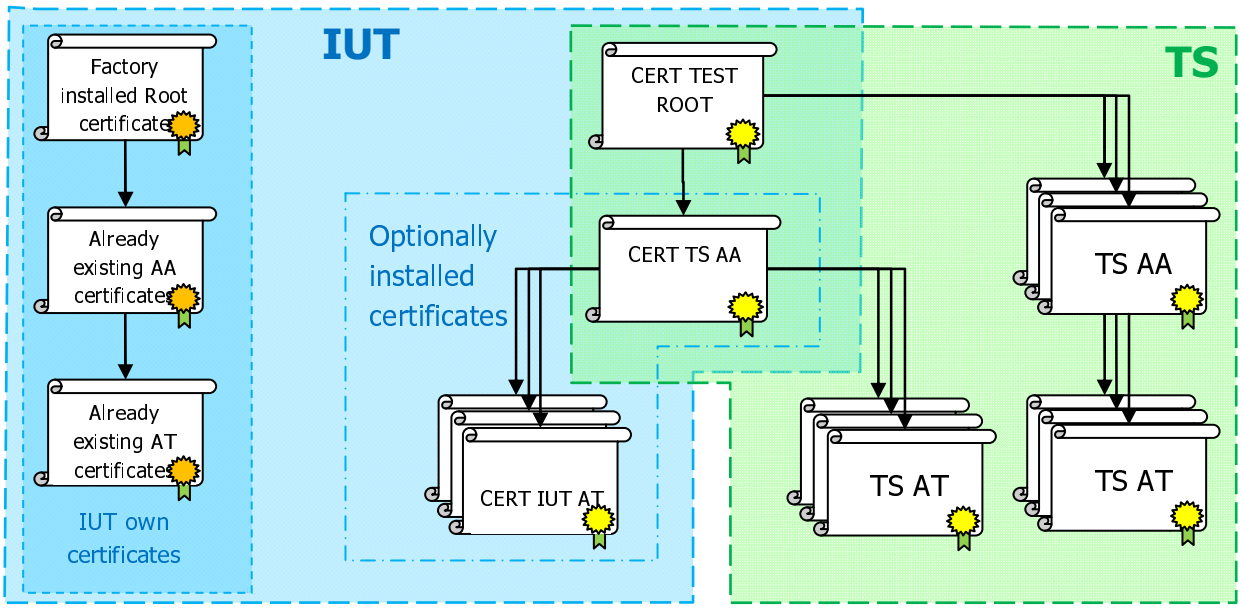

Figure 2: Required PKI certificate hierarchy

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/00afd63-0521-4487-8053-f10b1cd0a639/etsi-ts-103-096-3-v1.2.1-2015-09

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 AA certificates used by the Test System and by the IUT to verify the Test System certificates. For the generation procedure see clause 7.1.4. 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_AA and the set of CERT_IUT_AT) 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 or just their digests 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. Certificate digests can be stored within a file; each file shall have the same name as the corresponding certificate (CERT_IUT_x_AT) and the 'dgs' extension.

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 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, private keys and digest shall be stored as a hexadecimal streams.

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

Table 1: PKI file extensions

File extension	File role
.crt	Certificate
.vkey	Verification private key
.ekey	Encryption private key
.dgs	Digest of certificate (16 bytes)

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

5.3.2.3 Test system settings

5.3.2.3.1 Test adapter settings

A reference Test Adapter has been developed and validated on the TTCN-3 runtime environments as listed in table 2 and can be downloaded at http://forge.etsi.org/.

Table 2: TTCN-3 Tool Test Adapter Location

TTCN-3 Tool	Location
TTworkbench	taconfig.xml
TestCastT3	org.etsi.its.tool.elvior.res.ta.properties

iTeh STANDARD PREVIEW
(standards.iteh.ai)
Full standard:
https://standards.iteh.ai/catalog/standards/sist/f00afd63-0521-4487-805c-f10b1c49a639/etsi-ts-103-096-3-v1.2.1-2015-09

The relevant Test adapter parameters for the Test System security support are listed in table 3.

Table 3: TTCN-3 Tool Test Adapter Parameters

Parameter	Role	Default value
TsSecuredMode	Shall be set to FALSE to be able to test security envelope on TTCN-3 level	false
TsSecuredPath	Secured root path to access certificate files	"data/certificates"
TsSecuredConfiId	Vendor specific configuration identifier. This should be actually a name of the subfolder inside the TsSecuredPath, containing the IUT certificates or digests, e.g. "data/certificates/vendorA"	vendorA

5.3.2.3.2 Test Suite Parameters

Most of test parameters are the same as for GeoNetworking test suite and described in ETSI TS 102 871-3 [3]. Additional security-related parameters and some important GN parameters, PICS and PIXITS, are described in tables 4 and 5 respectively.