ETSI TS 103 096-3 V1.5.2 (2022-07)

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-005105

Keywords
ATS, ITS, 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 - 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 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 Security as defined in ETSI TS 103 097 [1] 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 in order to guarantee 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 103 097 (V1.4.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".

[2] ETSI TS 102 871-2 (V1.4.1): "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 (V1.4.1): "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 (V1.5.2): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)".

[5] ETSI TS 103 096-2 (V1.5.2): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 2: Test Suite Structure and Test Purposes (TSS & TP)".

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 V1.1.1.

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 [1], ETSI TS 102 871-2 [2], ETSI TS 102 871-3 [3], 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
ASN.1	Abstract Syntax Notation One
AT	Authorization Ticket
ATM	Abstract Test Method
ATS	Abstract Test Suite
BO	Exceptionnal Behaviour
BV	Valid Behaviour
CAM	Cooperative Awareness Message
DEN	Decentralized Environmental Notification
DENM	Decentralized Environmental Notification Message
EN	European Norm
ES	ETSI Standard
GN	GeoNetworking
HSM	Hardware Security Module
HTML	HyperText Markup Language
ISO	International Organization for Standardization
ITS	Intelligent Transport Systems
ITS-S	ITS Station
ITSS	ITS-S data transfer
IUT	Implementation Under Test

NB	Normal Behaviour
OER	Octet Encoding Rules
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
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
XSLT	eXtensible Stylesheet Language Transformations

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/rep/ITS/ttcn/ats_sec_ts103096-3.git. TTCN-3 compilers can be acquired at http://www.ttcn-3.org/.

5 Abstract Test Method

5.1 Introduction

Clause 5 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.

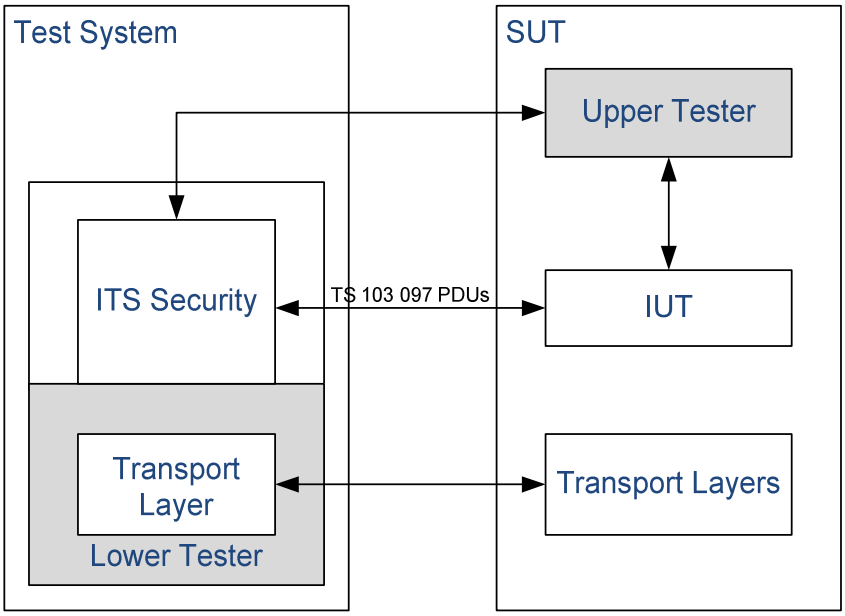

Figure 1: Abstract protocol tester - Security

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.

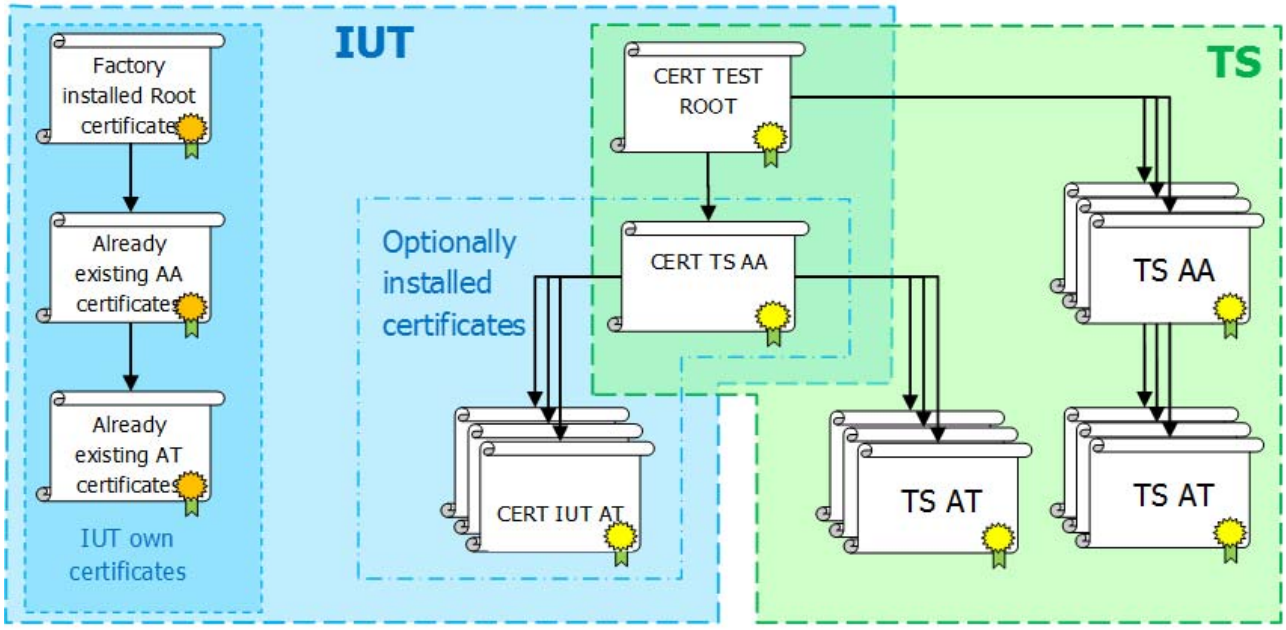

Figure 2: Required PKI certificate hierarchy

The following certificates are required for the test execution:

1) The set of the custom user-generated root certificates, referred as CERT_*_RCA, which are used to sign AA 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 these *_RCA certificates and consider them as trusted. In the case where the IUT cannot install and trust root certificates, no tests can be executed.

2) Further certificates to be installed on the IUT:

   - Option 1: Certificates can be installed onto the IUT. 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, then 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 binary 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
.oer	OER encoder 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 as defined in ETSI TS 103 097 [1]
- Permissions (AID SSP list)
- Geographical Validity Restriction as defined in ETSI TS 103 097 [1]

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 https://forge.etsi.org/rep/ITS/ttcn/ats_sec_ts103096-3.git.

Table 2: TTCN-3 Tool Test Adapter Location

TTCN-3 Tool	Location
TTworkbench	taconfig.xml
TestCastT3	org.etsi.its.tool.elvior.res.ta.properties
Titan	Test suite configuration file

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

The GeoNetworking test suite parameters defined in ETSI TS 102 871-3 [3] shall be applied. In addition the parameters defined in ETSI TS 102 871-2 [2] and in ETSI TS 103 096-2 [5] shall be applied as listed in tables 4 and 5.