ETSI TS 103 096-3 V1.1.1 (2013-07)

Intelligent Transport Systems (ITS);
Testing;
Conformance test specification for TS 102 867 and TS 102 941;
Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)

Reference

DTS/ITS-0050020

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

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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:
http://portal.etsi.org/chaircor/ETSI_support.asp

Contents

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:

TS 103 096-1: "Protocol Implementation Conformance Statement (PICS)";

TS 103 096-2: "Test Suite Structure and Test Purposes (TSS&TP)";

TS 103 096-3: "Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)";

TR 103 096-4: "Validation report".

1 Scope

The present document provides parts of the Abstract Test Suite (ATS) for Security as defined in IEEE 1609.2 [1], TS 102 941 [2] and in TS 102 867 [3] in compliance with the relevant requirements and in accordance with the relevant guidance given in ISO/IEC 9646-7 [8]. The TTCN modules and PIXIT declarations are not defined in the present document and will be added in a later revision.

The ISO standard for the methodology of conformance testing (ISO/IEC 9646-1 [5] and ISO/IEC 9646-2 [6]) as well as the ETSI rules for conformance testing (ETS 300 406 [9]) are used as a basis for the test methodology.

2 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.

2.1 Normative references

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

[1] IEEE P1609.2/D12 (January 2012): "IEEE Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages".

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

[3] ETSI TS 102 867: "Intelligent Transport Systems (ITS); Security; Stage 3 mapping for IEEE 1609.2".

[4] ETSI TS 103 096-1: Conformance test specification for Security Test requirements and Protocol Implementation Conformance Statement (PICS) proforma.

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

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

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

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

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

[10] FIPS PUB 186-3: "Digital Signature Standard (DSS)".

[11] SEC 1: "Elliptic Curve Cryptography".

2.2 Informative references

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 IEEE 1609.2 [1] TS 102 941 [2], TS 102 867 [3], ISO/IEC 9646-6 [7] and ISO/IEC 9646-7 [8] apply.

3.2 Abbreviations

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

AA	Authorization Authority
ASP	Abstract Service Primitive
ATM	Abstract Test Method
ATS	Abstract Test Suite
CA	Certification Authority
EA	Enrolment Authority
EB	Exceptional behaviour
ITS	Intelligent Transport System
ITS-S	ITS Station
IUT	Implementation Under Test
LDM	Local Dynamic Map
MTC	Main Test Component
PCTR	Protocol Conformance Test Report
PSID	Provider Service Identifier
SAP	Service Access Point
SCS	System Conformance Statement
SCTR	Static Conformance Test Report
SUT	System Under Test
TP	Test Purposes
TSS	Test Suite Structure
TTCN	Testing and Test Control Notation

4 Abstract Test Method

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

4.1 Abstract protocol tester

The abstract protocol tester used by the ITS-Security test suite is described in figure 1. The test system will simulate valid and invalid protocol behaviour, and will analyze the reaction of the IUT.

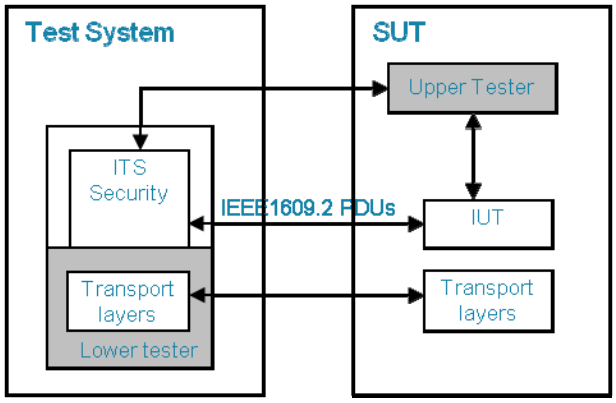

Figure 1: Abstract protocol tester - Security

4.2 Test Configuration

This test suite uses four test configurations in order to cover the different test scenarios. In these configurations, the tester simulates one or several ITS station implementing the ITS Security framework.

4.2.1 Test configuration CF01

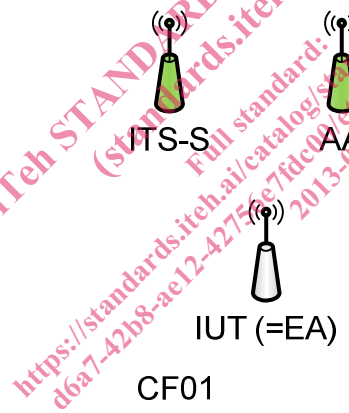

Figure 2: Test Configuration 1

4.2.2 Test configuration CF02

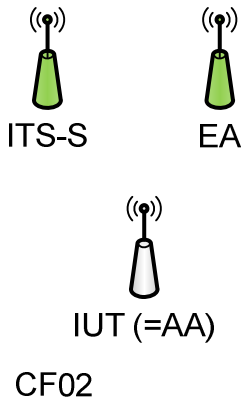

Figure 3: Test Configuration 2

4.2.3 Test configuration CF03

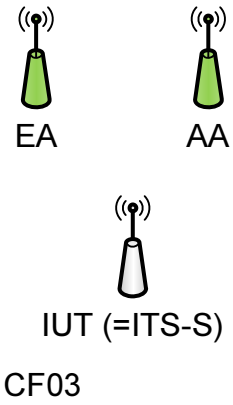

Figure 4: Test Configuration 3

4.2.4 Test configuration CF04

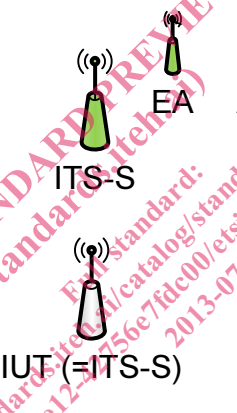

Figure 5: Test Configuration 4

4.3 Test architecture

The present document implements the general TTCN-3 test architecture described in EG 202 798 [i.1], clauses 6.3.2 and 8.3.1.

Figure 6 shows the TTCN-3 test architecture used for the ITS-Security ATS. In single-component testcases (configuration CF04), the MTC is of type ItsSec and communicates with the IUT over securityPort. In multi-component testcases (configuration CF01, CF02 and CF03), the MTC is of type ItsMtc and is used to synchronize the different PTCs. The PTCs are implemented using ItsSec components and communicate with the IUT over securityPort. Port securityPort is used to exchange IEEE 1609.2 [1] protocol messages between the Security test components and the IUT.

The Upper tester entity in the SUT enables triggering Security related functionalities by simulating primitives from application or LDM entities. It is required to trigger the ITS-Security layer in the SUT to send facility messages, which are resulting from upper layer primitives. Furthermore, receiving secured messages may result in the ITS-Security layer sending primitives to the appropriate facility layer.

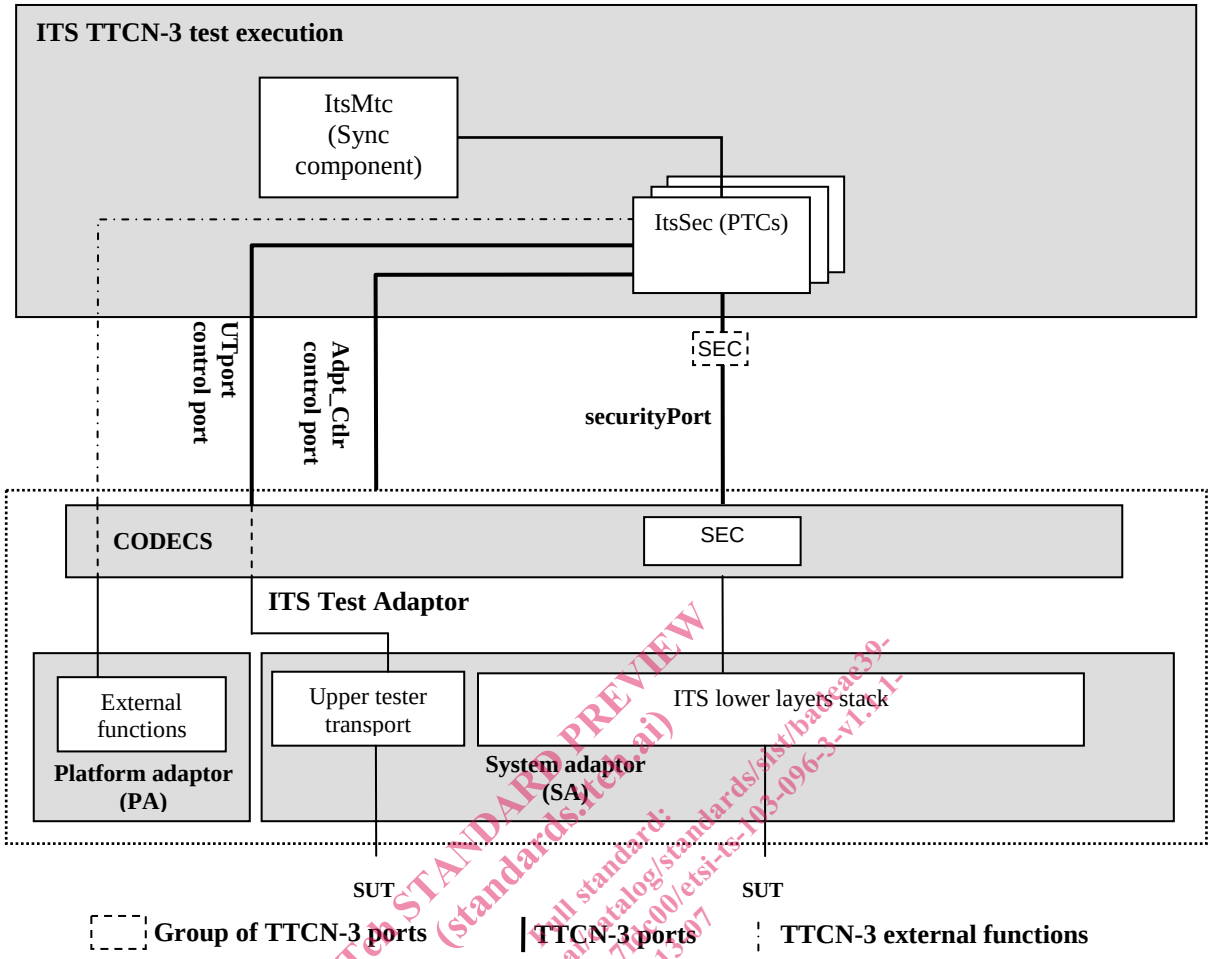

Figure 6: test system architecture

4.4 Ports and ASPs

Two ports are used by the ITS-Security ATS:

- The securityPort, of type SecurityPort
- The utPort of type UpperTesterPort

4.4.1 Primitives of the securityPort

Two types of primitives are used in the securityPort:

- The ieee1609Dot2Ind primitive used to receive messages of type Ieee1609Dot2Message.
- The ieee1609Dot2Req primitive used to send messages of type Ieee1609Dot2Message.

4.4.2 Primitives of the utPort

This port uses three types of primitives:

- The UtInitialize primitive used to initialise IUT
- The UtConfigure primitive used to configure specific options in IUT
- The UtTrigger primitive used trigger actions in IUT
- The UtStatus primitive used to retrieve status information from IUT

Table 1 lists all configuration options that the Test system should be able to modify in IUT for correct test execution.

Table 1: IUT configuration options

Configuration options
use certificate_chain
use explicit_certificates
use a self-signed enrolment request
use start_validity flag and not a lifetime_is_duration
use use_start_validity and lifetime_is_duration
use sec_data_exch_identified_localized
use signature of form x_coordinate_only (use of FIPS 186-3 specification [10])
use compressed public keys in signature (SEC 1 specification [11])
use uncompressed public keys in signature
include generation time when signing a message
include expiry_ time when signing a message
include generation _location when signing a message
use ecdsa_nistp256_with_sha256 as PKAlgorithm when signing a message
put certificate in each of the signed messages

Table 2 summarizes the actions that the Test System may require the IUT to perform via UtTrigger primitive.

Table 2: Actions triggered in IUT

Actions
send an EnrolmentRequest message
send an EnrolmentRequest message with more than 8 PSID records
send an AuthorizationRequest message
send a signed message
send a signed message with partial data
send a signed message with external data
send multiple signed message

Status codes returned by IUT via UtStatus primitive upon receipt of a IEEE 1609.2 [1] message are listed in table 3.

Table 3: IUT status codes

Status codes
ACCEPTED
DISCARDED
REJ_INVALID_REGION
REJ_INVALID_VALIDITY_PERIOD
REJ_INVALID_PERMISSIONS
REJ_UNSUPPORTED_SIGNER_TYPE
REJ_INVALID_EXPIRATION
REJ_DUPLICATED_PERMISSIONS
REJ_FORBIDDEN_SUBJECT_TYPE
REJ_FORBIDDEN_CF
REJ_FORBIDDEN_PERMISSIONS
REJ_FORBIDDEN_ACK
REJ_INVALID_REQUESTED_HASH
REJ_EXPIRED_DATA
REJ_IRRELEVANT_REGION
REJ_REVOKED_CERTIFICATE
REJ_UNAUTHORIZED_REGION
REJ_UNAUTHORIZED_AID
REJ_INVALID_CERTIFICATE_CHAIN
REJ_INVALID_SIGNATURE
REJ_UNSUPPORTED_MSG_TYPE