ETSI TS 103 525-3 V2.1.1 (2024-09)

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);
Release 2

Reference
RTS/ITS-00599

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 - 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 ITS 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 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 102 941 (V2.2.1): "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2".

[2] ETSI TS 102 940 (V2.1.1): "Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management; Release 2".

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

[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 103 525-2 (V2.1.1): " Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS PKI management; Part 2: Test Suite Structure and Test Purposes (TSS & TP); Release 2".

[6] ETSI TS 102 871-2 (V1.5.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking; Part 2: Test Suite Structure and Test Purposes (TSS & TP)".

[7] ETSI TS 102 871-3 (V1.5.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for GeoNetworking; Part 3: Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)".

[8] 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".

[9] ETSI TS 103 096-3 (V2.1.1): "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); 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: "Intelligent Transport Systems (ITS); Testing; Framework for conformance and interoperability testing".

[i.2] ETSI TR 103 099 (V1.5.1): "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.

[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 102 940 [2], ETSI TS 102 941 [1], ETSI TS 103 097 [3], ETSI TS 103 525-1 [4], ETSI TS 103 525-2 [5], ETSI TS 102 871-3 [7], 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	Abstract Syntax Notation
AT	Authorization Ticket

ATM	Abstract Test Method
ATS	Abstract Test Suite
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
HSM	Hardware Security Machine
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
ISO	International Organization for Standardization
ITS	Intelligent Transport System
ITS-S	ITS-Station
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 Purpose
TP	Test Purposes
TR	Technical Report
TS	Test System
TSS	Test Suite Structure
TTCN	Testing and Test Control Notation
UT	Upper Tester
WGS	World Geodetic System
XML	eXtensible Markup Language
XSLT	Language for transforming XML documents

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_pki_ts103525-3.git. 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.

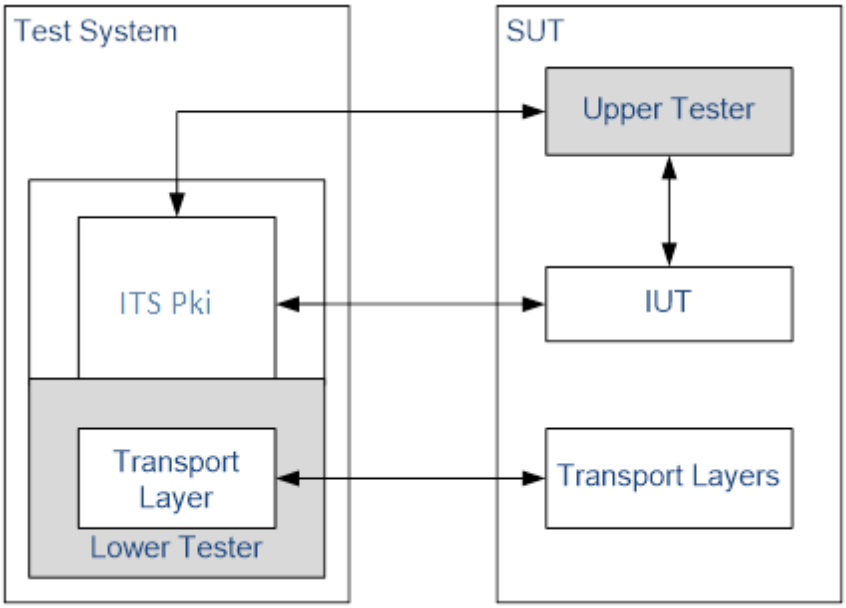

Figure 1: Abstract protocol tester - Pki

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 [2] and ETSI TS 102 941 [1].

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. See 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
.crt	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 [3]
- Permissions (AID SSP list)
- Geographical Validity Restriction as defined in ETSI TS 103 097 [3].

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_pki_ts103525-3.git.

Table 2: TTCN-3 Tool Test Adapter Location

TTCN-3 Tool	Location
TITAN	AtsPki.cfg

The relevant test adapter parameters for the Test System security and pki 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
TsSecuredMode	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 PKI test suite parameters defined in ETSI TS 103 525-2 [5] shall be applied. In addition the parameters defined in ETSI TS 102 871-3 [7] and in ETSI TS 103 096-2 [8] shall be applied as listed in tables 4 and 5.

Table 4: PICS Parameters

Parameter	Reference	Role	Default value
PICS_GN_SECURITY	ETSI TS 102 871-2 [6], clause 6.1.5	Shall be set to true to be able to execute security tests.	false
PICS_CERTIFICATE_SELECTION	ETSI TS 103 096-2 [8], clause 5.1.5, T3/2	Certificate selection option.	true
PICS_ITS_AID_OTHER_PROFILE	ETSI TS 103 096-2 [8], clause 5.1.5, T3/7	The value of the ITS_AID to be used for third profile testing. Set to zero to skip third profile testing.	0 (skip)

Table 5: PIXIT Parameters

Parameter	Reference	Role	Default value
PX_CERTIFICATE_POOL_PATH	Clause B.6	The path to the pool of certificates and keys	/data/certificates
PX_IUT_SEC_CONFIG_NAME	Clause B.7	The name of the subfolder in PX_CERTIFICATE_POOL_PATH with IUT certificates or digests	vendor
NOTE: PX_CERTIFICATE_POOL_PATH and PX_IUT_SEC_CONFIG_NAME shall be set to the same values as TsSecuredPath and TsSecuredConfiId.			

5.3.2.4 Certificate profiles

The ITS Security Test Suite contains certificate profiles describing content of certificates to be used by both TS and IUT. Then certificate profiles are used by the Certificate Generation Tool to generate all necessary certificates, see clause 5.3.2.5.

EXAMPLE:

```
<certificate name="CERT_TEST_ROOT" keep-existing="yes">
    <version>2</version>
    <signer type="self"></signer>
    <subject type="ROOT" name="">
        <!-- verification_key -->
        <attribute type="verification_key">
            <public_key algorithm="ecdsa_nistp256_with_sha256">
                <ecc_point type="uncompressed"/>
            </public_key>
        </attribute>
        <!-- assurance_level -->
        <attribute type="assurance_level">
            <assurance level="6" confidence="0"/>
        </attribute>
        <!-- its_aid_list -->
        <attribute type="its_aid_list">
            <aid value="36"/> <!-- CAM -->
            <aid value="37"/> <!-- DENM -->
        </attribute>
    </subject>
    <validity>
        <restriction type="time" start="2015-01-01" end="2016-01-01"/>
        <restriction type="region">
            <none/>
        </restriction>
    </validity>
    <signature algorithm="0"/>
</certificate>

<certificate name="CERT_TS_B_AT">
    <version>2</version>
    <signer type="digest" name="CERT_TS_B_AA"/>
    <subject type="AT" name="">
        <attribute type="verification_key">
            <public_key algorithm="0" point-type="uncompressed"/>
        </attribute>
        <attribute type="assurance_level">
            <assurance level="3"/>
        </attribute>
        <attribute type="its_aid_ssp_list">
            <ssp aid="36">&#0;</ssp> <!-- CAM -->
            <ssp aid="37">&#0;</ssp> <!-- DENM -->
        </attribute>
    </subject>
    <validity>
        <restriction type="time" start="2015-01-01" end="2016-01-01"/>
        <restriction type="region">
            <circle latitude="43.616908" longitude="7.052847" radius="5000"/>
        </restriction>
    </validity>
    <signature algorithm="0"/>
</certificate>
```

NOTE 1: Time and region restriction can be provided in relative way, defining the difference to the reference values.

NOTE 2: The name of resulting file is taken from the attribute 'name' of the certificate profile.

5.3.2.5 Certificate generation

Certificates can be generated based on certificate profiles using the certificate generation tool, provided as a part of the test suite. Certificate generation tool does not make any validation of the input profile, it just transforms the XML profile to the XER representation of the certificate, encode it to OER representation and signs it with the proper private key. Certificate generation tool uses openssl cryptographical library v.1.0.1j [i.8] or greater and asn1c ASN.1 compiler v.0.9.29 [i.9] or greater.

This tool contains two parts:

1) XSLT script to convert XML profiles to XER-encoded certificates.

2) Command line tool written in plain C to convert XER-encoded certificate to OER-encoding and sign it. This part can be compiled for any operating system that has openssl library installed. The tool is open source software and distributed under the ETSI free software license. The full certificate pool can be generated using makefile provided in /data/v3 folder in the test suite. In the case when HSM is used to store private keys, all correspondent public keys of IUT shall be exported from the HSM previously and put to the output folder (or any other folder, which can be specified with –K option for the generator). Name of the key file shall be the same as the profile name, file extension shall be .vkey for verification key and .ekey for encryption key, if any.

Certificates and private keys generated by the tool are ready to be used by TS and IUT.

5.3.2.6 Certificate installation

The ATS requires installing some certificates onto the IUT. The installation procedure is manual, customer dependent and out of scope of the present document. The list of certificates to be installed on the IUT is given in the certificate content definition, defined in ETSI TS 103 096-2 [8], clause 6.1.1 and ETSI TS 103 525-2 [5], clause 6.1.1.

These certificates can be generated and should be installed onto the IUT and may be selected by the TS using UT interface during the start-up phase of test case execution, see ETSI TR 103 099 [i.2], clause 5.5 and clause C.1.1.

5.4 Test architecture

The ITS Pki Test Suite is based on the test architecture described in ETSI TS 102 871-3 [7]. The test system communicates with the PKI SUT over the pkiPort and over the utPorts as described in clause 5.5.

5.5 Ports and ASPs

5.5.1 Introduction

Four ports are used by the ITS-Pki ATS:

- The PKI Port, of type HTTP.
- The geoNetworking Port, of type geoNetworkingPort.
- The utPkiPort of type LibItsPki_TestSystem.UpperTesterPort.
- The denmUtPort of type LibItsDenm_TestSystem.UpperTesterPort.
- The camUtPort of type LibItsCam_TestSystem.UpperTesterPort.

5.5.2 Primitives of the geoNetworkingPort

Two types of primitives are used in the securityPort:

- The geoNetworkingInd primitive used to receive messages of type GeoNetworkingPacket.
- The geoNetworkingReq primitive used to send messages of type GeoNetworkingPacket.

5.5.3 Primitives of the utPort

The Upper Tester port uses these types of primitives:

- The UtInitialize primitive used to initialize IUT.
- The UtCamTrigger primitive with the changeSpeed parameter is used to configure IUT to send CAM messages with high rate (greater than 1 Hz).
- The UtDenmTrigger primitive used trigger the event in the IUT to send a DEN message.
- The UtDenmTermination primitive used cancel the event of DEN message.

- The UtGnEventInd primitive is used to receive message from the SUT part to indicate that the message has been transmitted to the upper layer.

6 External functions

The external functions, described in ETSI TS 103 096-3 [9] shall be applied.

7 ATS conventions

7.1 Introduction

The ATS conventions are intended to give a better understanding of the ATS but they also describe the conventions made for the development of the ATS. These conventions shall be considered during any later maintenance or further development of the ATS.

The ATS conventions contain the testing conventions, described in clause 7.2 and the naming conventions, described in clause 7.3. The testing conventions describe the functional structure of the ATS. The naming conventions describe the structure of the naming of all ATS elements.

To define the ATS, the guidelines of the document ETSI ETS 300 406 [i.7] were considered.

7.2 Testing conventions

7.2.1 Testing states

7.2.1.1 Initial states

All test cases start with the function f_prInitialState. This function brings the IUT in an "initialized" state by invoking the upper tester primitive UtInitialize.

7.2.1.2 Final state

All test cases end with the function f_poDefault. This function brings the IUT back to operational state. As no specific actions are required for the idle state in the ETSI TS 103 097 [3], the function f_poDefault does not invoke any action.

As necessary, further actions may be included in the f_poDefault function.

7.3 Naming conventions

7.3.1 Introduction

This test suite follows the naming convention guidelines provided in the ETSI EG 202 798 [i.1].

7.3.2 General guidelines

The naming convention is based on the following underlying principles:

- in most cases, identifiers should be prefixed with a short alphabetic string (specified in table 6) indicating the type of TTCN-3 element it represents;
- suffixes should not be used except in those specific cases identified in table 8;
- prefixes and suffixes should be separated from the body of the identifier with an underscore ("_");

EXAMPLE 1: `c_sixteen, t_wait`.

- only module names, data type names and module parameters should begin with an upper-case letter. All other names (i.e. the part of the identifier following the prefix) should begin with a lower-case letter;
- the start of second and subsequent words in an identifier should be indicated by capitalizing the first character. Underscores should not be used for this purpose.

EXAMPLE 2: `f_initialState`.

Table 6 specifies the naming guidelines for each element of the TTCN-3 language indicating the recommended prefix, suffixes (if any) and capitalization.

Table 6: ETSI TTCN-3 generic naming conventions

Language element	Naming convention	Prefix	Example identifier
Module	Use upper-case initial letter	none	IPv6Templates
Group within a module	Use lower-case initial letter	none	messageGroup
Data type	Use upper-case initial letter	none	SetupContents
Message template	Use lower-case initial letter	m_	m_setupInit
Message template with wildcard or matching expression	Use lower-case initial letters	mw_	mw_anyUserReply
Modifying message template	Use lower-case initial letter	md_	md_setupInit
Modifying message template with wildcard or matching expression	Use lower-case initial letters	mdw_	mdw_anyUserReply
Signature template	Use lower-case initial letter	s_	s_callSignature
Port instance	Use lower-case initial letter	none	signallingPort
Test component instance	Use lower-case initial letter	none	userTerminal
Constant	Use lower-case initial letter	c_	c_maxRetransmission
Constant (defined within component type)	Use lower-case initial letter	cc_	cc_minDuration
External constant	Use lower-case initial letter	cx_	cx_macId
Function	Use lower-case initial letter	f_	f_authentication()
External function	Use lower-case initial letter	fx_	fx_calculateLength()
Altstep (incl. Default)	Use lower-case initial letter	a_	a_receiveSetup()
Test case	Use ETSI numbering	TC_	TC_COR_0009_47_ND
Variable (local)	Use lower-case initial letter	v_	v_macId
Variable (defined within a component type)	Use lower-case initial letters	vc_	vc_systemName
Timer (local)	Use lower-case initial letter	t_	t_wait
Timer (defined within a component)	Use lower-case initial letters	tc_	tc_authMin
Module parameters for PICS	Use all upper case letters	PICS_	PICS_DOOROPEN
Module parameters for other parameters	Use all upper case letters	PX_	PX_TESTER_STATION_ID
Formal Parameters	Use lower-case initial letter	p_	p_macId
Enumerated Values	Use lower-case initial letter	e_	e_syncOk

7.3.3 ITS specific TTCN-3 naming conventions

Next to such general naming conventions, table 7 shows specific naming conventions that apply to the ITS TTCN-3 test suite.

Table 7: ITS specific TTCN-3 naming conventions

Language element	Naming convention	Prefix	Example identifier
ITS Module	Use upper-case initial letter	Its"IUTname"_	ItsPki_
Module containing types and values	Use upper-case initial letter	Its"IUTname"_TypesAndValues	ItsPki_TypesAndValues
Module containing Templates	Use upper-case initial letter	Its"IUTname"_Templates	ItsPki_Templates
Module containing test cases	Use upper-case initial letter	Its"IUTname"_TestCases	ItsPki_TestCases
Module containing functions	Use upper-case initial letter	Its"IUTname"_Functions	ItsPki_Functions
Module containing external functions	Use upper-case initial letter	Its"IUTname"_ExternalFunctions	ItsPki_ExternalFunctions
Module containing components, ports and message definitions	Use upper-case initial letter	Its"IUTname"_Interface	ItsPki_Interface
Module containing main component definitions	Use upper-case initial letter	Its"IUTname"_TestSystem	ItsPki_TestSystem
Module containing the control part	Use upper-case initial letter	Its"IUTname"_TestControl	ItsPki_TestControl

7.3.4 Usage of Log statements

All TTCN-3 log statements use the following format using the same order:

- Three asterisks.
- The TTCN-3 test case or function identifier in which the log statement is defined.
- One of the categories of log: INFO, WARNING, ERROR, PASS, FAIL, INCONC, TIMEOUT.
- Free text.
- Three asterisks.

EXAMPLE 1:

```
log("*** TC_SEC_PKI_EA_SND_01_BV: INFO: Preamble: Received and answered Enrolment Request ***")
```

Furthermore, the following rules are applied for the ITS-Pki ATS:

- Log statements are used in the body of the functions, so that invocation of functions are visible in the test logs
- All TTCN-3 *setverdict* statements are combined with a log statement following the same above rules (see example 2)

EXAMPLE 2:

```
setverdict(pass, "*** TC_SEC_PKI_EA_SND_01 BV: PASS: Enrolment Response correctly accepted ***")
```

7.3.5 Test Case (TC) identifier

Table 8 shows the test case naming convention, which follows the same naming convention as the test purposes.

Table 8: TC naming convention

Identifier	TP_<root>_<tgt>_<gr>_<sub-gr> <sn>_<x>	Sub-Group	Category
	<root> = root	SECPKI	
	<tgt> = target	ITSS	ITS-Station
		AA	Authorization Authority
		EA	Enrolment Authority
		RCA	Root Certification Authority
		DC	Distribution Center
		CPOC	C-ITS Point of Contact
	<gr> = group	ENR	Enrolment
		AUTH	Authorization
		AUTHVAL	Authorization Validation
		CRL	CRL handling
		CTL	CTL handling
		CACERTGEN	CA certificate generation
		CTLGEN	CTL generation
		ECTLGEN	ECTL generation
		CRLGEN	CRL generation
		LISTDIST	CTL/CRL/ECTL distribution
		TLMCERTGEN	TLM certificate generation
	<sub-gr> = sub-group	SND (optional)	Send
		RCV	Receive
	<sn> = test purpose sequential number		01 to 99
	<x> = category	BV	Valid Behaviour tests
		BO	Invalid Behaviour Tests

EXAMPLE: TP identifier: SECPKI_AA_AUTH _01_BV
TC identifier: TC_SECPKI_AA_AUTH_RCV_01_BV

7.4 On line documentation

The T3D tool enables providing on-line documentation browser in HTML, by tagging TTCN-3 comments. These tags are defined in table 9.

Table 9: TTCN-3 comment tags

Tag	Description
@author	Specifies the names of the authors or an authoring organization which either has created or is maintaining a particular piece of TTCN-3 code.
@desc	Describes the purpose of a particular piece of TTCN-3 code. The description should be concise yet informative and describe the function and use of the construct.
@remark	Adds extra information, such as the highlighting of a particular feature or aspect not covered in the description.
@see	Refers to other TTCN-3 definitions in the same or another module.
@return	Provides additional information on the value returned by a given function.
@param	Documents the parameters of parameterized TTCN-3 definitions.
@version	States the version of a particular piece of TTCN-3 code.

The HTML files result from the compilation of the TTCN-3 modules with the T3D tool. These HTML files are ready for browsing, and contain links enabling to navigate through the ATS.

EXAMPLE:

```
/**
 * @desc Check that ITS-S sends a SecuredMessage containing protocol version set to 2
 * @see     ETSI TS 103 097 [3] V1.4.1 Clause 5.1    SecuredMessage
 * @reference   ETSI EN 302 636-4-1 [1], clauses 9.3.2, 8.6.2 and Annex G
 */
```

Annex A (normative): ATS in TTCN-3

A.1 TTCN-3 files and other related modules

This test suite has been produced using the Testing and Test Control Notation (TTCN) according to ETSI ES 201 873-1 [i.9].

ETSI TS 103 097 [3], ETSI TS 103 525-1 [4] and ETSI TS 103 525-2 [5] have been applied to develop this test suite.

This test suite has been compiled error-free using two different commercial TTCN-3 compilers.

The TTCN-3 library modules, which form parts of the present document, are accessible from the ETSI source repository: https://forge.etsi.org/rep/ITS/ttcn/ats_pki_ts103525-3.git.

The publishing tag *v2.1.1* shall be used.

Annex B (normative): Partial PIXIT pro forma for Security

B.1 The right to copy

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the Partial PIXIT pro forma in this annex so that it can be used for its intended purposes and may further publish the completed Partial PIXIT.

B.2 Introduction

The PIXIT pro forma is based on ISO/IEC 9646-6 [i.5].

B.3 Identification summary

The Identification summary shall be as specified in table B.1.

Table B.1: Identification summary

PIXIT Number:	
Test Laboratory Name:	
Date of Issue:	
Issued to:	

B.4 ATS summary

The ATS summary shall be as specified in table B.2.

Table B.2: ATS summary

Protocol Specification:	ETSI TS 103 097 [3]
Protocol to be tested:	Security header and certificate formats
ATS Specification:	ETSI TS 103 096-3 [9]
Abstract Test Method:	Clause 4

B.5 Test laboratory

The Test laboratory info shall be specified as in table B.3.

Table B.3: Test laboratory info

Test Laboratory Identification:	
Test Laboratory Manager:	
Means of Testing:	
SAP Address:	

B.6 Client identification

The Client identification shall be specified as in table B.4.

Table B.4: Client identification

Client Identification:	
Client Test manager:	
Test Facilities required:	

B.7 SUT

SUT shall be specified as in table B.5.

Table B.5: SUT

Name:	
Version:	
SCS Number:	
Machine configuration:	
Operating System Identification:	
IUT Identification:	
PICS Reference for IUT:	
Limitations of the SUT:	
Environmental Conditions:	

B.8 Protocol layer information

B.8.1 Protocol identification

Protocol identification shall be as specified in table B.6.

Table B.6: Protocol identification

Name:	ETSI TS 102 941
Version:	
PICS References:	ETSI TS 103 525-1

B.8.2 IUT information

PKI PIXITs shall be as listed in table B.7.

Table B.7: Relevant PKI PIXITs

Identifier	Description	
PX_FIRST_ENROLMENT	**Comment**	Set to true if it is the first enrolment
	Type	boolean
	Def. value	true
PX_INCLUDE_ENCRYPTION_KEYS	**Comment**	Set to true if the encryption keys be included in authorization request
	Type	boolean
	Def. value	true
PX_AUTHORIZATION_REQUEST_WITH_POP	**Comment**	Set to true if the authorization request uses SignedWithPop mechanism
	Type	boolean
	Def. value	true
PX_RE_ENROLMENT_DELAY	**Comment**	Delay to wait between two enrolment requests
	Type	float
	Def. value	2.0
PX_RE_AUTHORIZATION_DELAY	**Comment**	Delay to wait between two re-authorizarion requests
	Type	float
	Def. value	2.0
PX_TRIGGER_EC_BEFORE_AT	**Comment**	Set to true if the Test System shall generate an enrolment request before the authorization request
	Type	boolean
	Def. value	true
PX_CERT_EXPIRATION_DELAY	**Comment**	Delay to wait after enrolment certificate exiration
	Type	float
	Def. value	2.0
PX_EC_REPETITION_TIMEOUT	**Comment**	Maximum delay between two enrolment request repetition
	Type	float
	Def. value	120.0
PX_EC_REPETITION_TIMEOUT_TH2	**Comment**	Maximum delay before the IUT stops enrolment request repetition
	Type	float
	Def. value	150.0
PX_AT_REPETITION_TIMEOUT_TH2	**Comment**	Maximum delay before the IUT stops authorization request repetition
	Type	float
	Def. value	15.0

The relevant Security GN PIXITs shall be as in table B.8.

Table B.8: Security PIXITs

Identifier	Description	
PX_CERTIFICATE_POOL_PATH	**Comment**	Path to the certificates and private keys pool
	Type	Octetstring
	Def. value	/data/certificates
PX_IUT_SEC_CONFIG_NAME	**Comment**	Name of the IUT identifier (subfolder in PX_CERTIFICATE_POOL_PATH)
	Type	Octetstring
	Def. value	cfg01
PX_IUT_DEFAULT_CERTIFICATE	**Comment**	The name (or digest) of the certificate to be used by the IUT by default
	Type	Octetstring
	Def. value	CERT_IUT_A_AT
PX_OTHER_ITS_AID	**Comment**	The ITS AID for Beacon messages. Use zero to skip tests of Secured Beacons
	Type	Integer
	Def. value	141
PX_WRONG_PROTOCOL_VERSION	**Comment**	Invalid protocol version
	Type	UInt8
	Def. value	1
PX_WGSLONGITUDE	**Comment**	Invalid WGS longitude
	Type	SecLongitude
	Def. value	0
PX_WGSLATITUDE	**Comment**	Invalid WGS latitude
	Type	SecLatitude
	Def. value	0

The relevant GeoNetworking PIXITs (see ETSI TS 102 871-3 [7]) shall be as listed in table B.9.

Table B.9: Relevant GeoNetworking PIXITs

Identifier	Description	
PICS_GN_LOCAL_GN_ADDR	**Comment**	GeoNetworking address of the GeoAdhoc router
	Type	GN_Address
	Def. value	typeOfAddress := e_manual, stationType := e_passengerCar, stationCountryCode := c_uInt10Zero, mid := c_6ZeroBytes
PX_GN_UPPER_LAYER	**Comment**	The IUT's upper layer
	Type	Enumerated
	Def. value	e_btpB

Annex C (normative): PCTR pro forma for Security

C.1 The right to copy

Notwithstanding the provisions of the copyright clause related to the text of the present document, ETSI grants that users of the present document may freely reproduce the PCTR pro forma in this annex so that it can be used for its intended purposes and may further publish the completed PCTR.

C.2 Introduction

The PCTR pro forma is based on ISO/IEC 9646-6 [i.5].

C.3 Identification summary

C.3.1 Protocol conformance test report

A protocol conformance test report shall be as in table C.1.

Table C.1: Protocol conformance test report

PCTR Number:	
PCTR Date:	
Corresponding SCTR Number:	
Corresponding SCTR Date:	
Test Laboratory Identification:	
Test Laboratory Manager:	
Signature:	

C.3.2 IUT identification

An IUT shall be identified as specified in table C.2.

Table C.2: IUT identification

Name:	
Version:	
Protocol specification:	
PICS:	
Previous PCTR if any:	

C.3.3 Testing environment

The testing environment shall be as specified in table C.3.

Table C.3: Testing environment

PIXIT Number:	
ATS Specification:	
Abstract Test Method:	
Means of Testing identification:	
Date of testing:	
Conformance Log reference(s):	
Retention Date for Log reference(s):	

C.3.4 Limits and reservation

Additional information relevant to the technical contents or further use of the test report, or the rights and obligations of the test laboratory and the client, may be given here. Such information may include restriction on the publication of the report.

.....

.....

.....

.....

.....

C.3.5 Comments

Additional comments may be given by either the client or the test laboratory on any of the contents of the PCTR, for example, to note disagreement between the two parties.

.....

.....

.....

.....

.....

C.4 IUT Conformance status

This IUT has or has not been shown by conformance assessment to be non-conforming to the specified protocol specification.

Strike the appropriate words in this sentence. If the PICS for this IUT is consistent with the static conformance requirements (as specified in clause C.3 in the present document) and there are no "FAIL" verdicts to be recorded (in clause C.6 in the present document) strike the words "has or", otherwise strike the words "or has not".

C.5 Static conformance summary

The PICS for this IUT is or is not consistent with the static conformance requirements in the specified protocol.

Strike the appropriate words in this sentence.

C.6 Dynamic conformance summary

The test campaign did or did not reveal errors in the IUT.

Strike the appropriate words in this sentence. If there are no "FAIL" verdicts to be recorded (in clause C.8 of the present document) strike the words "did or" otherwise strike the words "or did not".

Summary of the results of groups of test:

.....

.....

.....

.....

.....

C.7 Static conformance review report

If clause C.3 indicates non-conformance, this clause itemizes the mismatches between the PICS and the static conformance requirements of the specified protocol specification.

.....

.....

.....

.....

.....

C.8 Test campaign report

For the complete list of all test cases refer to the test control module of the file described in annex A of the present document.

C.9 Observations

Additional information relevant to the technical content of the PCTR is given here.

.....

.....

.....

.....

History

Document history		
V1.1.1	March 2019	Publication
V1.2.1	January 2022	Publication
V1.2.2	July 2022	Publication
V2.1.1	September 2024	Publication