ETSI TS 103 096-3 V1.4.1 (2018-08)

TECHNICAL SPECIFICATION

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-00544

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

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
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 2018.
All rights reserved.

DECTTM, **PLUGTESTS**TM, **UMTS**TM and the ETSI logo are trademarks of ETSI registered for the benefit of its Members.
3GPPTM and **LTE**TM are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners.
oneM2M logo is protected for the benefit of its Members.
GSM® and the GSM logo are trademarks registered and owned by the GSM Association.

Contents

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 covering Conformance test specifications 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.

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 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 103 097 (V1.3.1): "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 (V1.4.1): "Intelligent Transport Systems (ITS); Testing; Conformance test specifications for ITS Security; Part 1: Protocol Implementation Conformance Statement (PICS)".

[5] ETSI TS 103 096-2 (V1.4.1): "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 V1.0.1j.

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 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions 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 Abbreviations

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

AA	Authorization Authority
AID	Application ID
ASN.1	Abstract Syntax Notation One
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
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 http://forge.etsi.org/. 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.

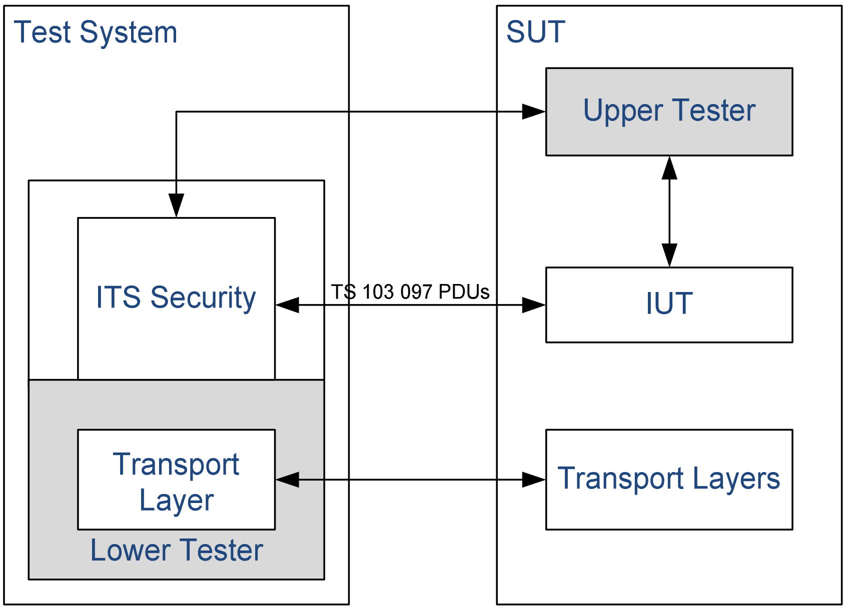

Figure 1: Abstract protocol tester - Security

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.

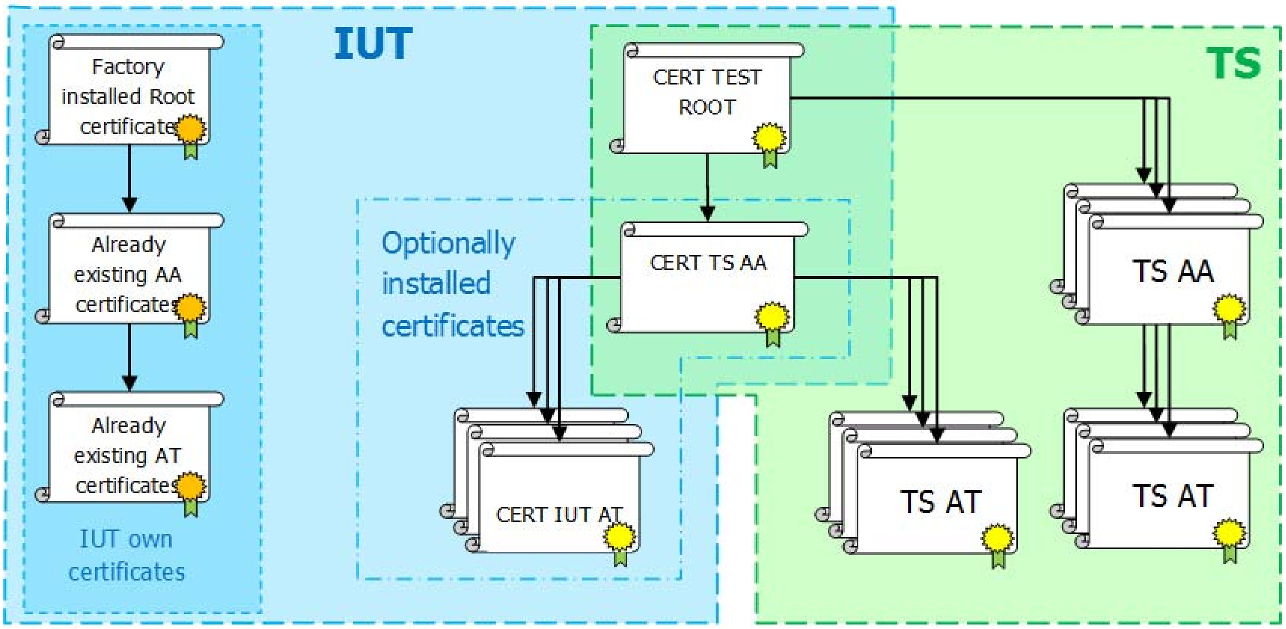
IUT
TS
Factory installed Root certificate
Already existing AA certificate
Already existing AT certificate
IUT own certificates
Optionally installed certificates
CERT TEST ROOT
CERT TS AA
CERT IUT AT
TS AA
TS AT
TS AT

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. 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, 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
- 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
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.

Table 4: PICS Parameters

Parameter	Reference	Role	Default value
PICS_GN_SECURITY	ETSI TS 102 871-2 [2], A.32/12	Shall be set to true to be able to execute security tests	false
PICS_SEC_CERTIFICATE_SELECTION	ETSI TS 103 096-2 [5], clause 5.1.5, T3/2	Certificate selection option	true
PICS_SEC_CIRCULAR_REGION PICS_SEC_RECTANGULAR_REGION PICS_SEC_POLYGONAL_REGION PICS_SEC_IDENTIFIED_REGION	ETSI TS 103 096-2 [5], clause 5.1.5, T3/3-6	The supporting of various region types	true
PICS_SEC_SHA256	ETSI TS 103 096-2 [5], clause 5.1.5, T3/8	Set to true if IUT supports SHA256 hash algorithm	true
PICS_SEC_SHA384	ETSI TS 103 096-2 [5], clause 5.1.5, T3/9	Set to true if IUT supports SHA384 hash algorithm	true
PICS_SEC_BRAINPOOL_P256R1	ETSI TS 103 096-2 [5], clause 5.1.5, T3/10	Set to true if IUT supports Brainpool P256R1 curve	true
PICS_SEC_BRAINPOOL_P384R1	ETSI TS 103 096-2 [5], clause 5.1.5, T3/11	Set to true if IUT supports Brainpool P384R1 curve	true

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>
    <version>3</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="compressed"/>
            </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="CAM"/>  <!-- CAM -->
            <aid value="DENM"/>  <!-- DENM -->
            <aid value="SPAT"/> <!-- TLM / SPAT -->
            <aid value="MAP"/> <!-- RLT / MAP-->
            <aid value="IVI"/> <!-- IVI -->
            <aid value="TLC"/> <!-- TLC -->
            <aid value="GN-MGMT"/> <!-- GN-MGMT -->
        </attribute>
    </subject>
    <validity>
        <restriction type="time" start="-365d" end="+730d"/>
        <restriction type="region">
```

```
            <none/>
        </restriction>
    </validity>
    <signature algorithm="0"/>
</certificate>
<certificate>
    <version>3</version>
    <signer type="digest" name="CERT_IUT_A_B_AA"/>
    <subject type="AT" name="">
        <!-- verification_key -->
        <attribute type="verification_key">
            <public_key algorithm="brainpool256">
                <ecc_point type="compressed"/>
            </public_key>
        </attribute>
        <!-- assurance_level -->
        <attribute type="assurance_level">
            <assurance level="3"/>
        </attribute>
        <!-- its_aid_ssp_list -->
        <attribute type="its_aid_ssp_list">
            <ssp aid="CAM">01 FF FF</ssp>  <!-- CAM -->
            <ssp aid="DENM">01 FF FF</ssp>  <!-- DENM -->
            <ssp aid="GN-MGMT">00</ssp>  <!-- GN-MGMT -->
        </attribute>
    </subject>
    <validity>
        <restriction type="time" start="+0d" end="+365d"/>
        <restriction type="region">
            <none/>
        </restriction>
    </validity>
    <signature algorithm="brainpool256"/>
</certificate>
```

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

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 CeCILL-C 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.

Certificates that shall be installed in order to run the mandatory tests:

- CERT_IUT_A_RCA

- CERT_IUT_A_AA

Certificates that shall be installed in order to run the optional tests:

- CERT_IUT_A _B_AA (AA certificate with brainpool256r1 verification key)
- CERT_IUT_A _B3_AA (AA certificate with brainpool384r1 verification key)
- CERT_IUT_A _N_AA (AA certificate with uncompressed verification key)
- CERT_TS_C_AA (AA certificate with rectangular region restrictions)
- CERT_TS_D_AA (AA certificate with polygonal region restrictions)
- CERT_TS_E_AA (AA certificate with identified region restrictions)

At least the CERT_IUT_A_RCA and CERT_IUT_A_AA certificates shall be installed onto the IUT to be able to validate messages sent by the TS. All certificates used in mandatory tests are derived from the CERT_IUT_A_RCA certificate.

Most of the test cases can be executed with any valid certificate installed on the IUT, which permit to send CAM/DENM (the way how this certificate has been obtained and installed is out of scope of the present document). This IUT certificate or at least its digest shall be installed onto the test system with the name CERT_IUT_A_AT.oer or CERT_IUT_A_AT.dgs.

However, there are some tests that require using special IUT AT certificates, mostly with different geographical region conditions, named:

- CERT_IUT_A_AT (no region restrictions)
- CERT_IUT_A_B_AT (brainpool256 verification key)
- CERT_IUT_A_B_N_AT (uncompressed brainpool256 verification key)
- CERT_IUT_A_B3_AT (brainpool384 verification key)
- CERT_IUT_A_B3_N_AT (uncompressed brainpool384 verification key)
- CERT_IUT_A_B33_AT (brainpool384 verification key, brainpool384 signature)
- CERT_IUT_A1_AT (expired certificate)
- CERT_IUT_A2_AT (not yet valid certificate)
- CERT_IUT_A3_AT (no CAM permissions)
- CERT_IUT_A4_AT (no DENM permissions)
- CERT_IUT_B_AT (circular region restrictions)
- CERT_IUT_C_AT (rectangular region restrictions)
- CERT_IUT_C1_AT (inconsistent rectangular region restriction)
- CERT_IUT_CA1_AT (reuse parent region restriction)
- CERT_IUT_CA2_AT (reuse parent region restriction)
- CERT_IUT_CA3_AT (reuse parent region restriction)
- CERT_IUT_CC_AA (reuse parent region restriction)
- CERT_IUT_D_AT (polygonal region restrictions)
- CERT_IUT_E_AT (identified region restrictions)

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 Security Test Suite is based on the test architecture described in ETSI TS 102 871-3 [3]. The test system communicates with the GeoNetworking SUT over the geoNetworkingPor 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-Security ATS:

- The geoNetworking Port, of type geoNetworkingPort
- The utPort of type LibItsGeoNetworking_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 table 6, have been defined in order to perform cryptographic operations and handle complex computations.

Table 6: External functions

Function	Parameters			Return	
	Dir.	Name	Type	Value	Type
fx_hashWithSha256	in	p_toBeHashedData	octetstring	Hash	Oct32
fx_hashWithSha384	in	p_toBeHashedData	octetstring	Hash	Oct48
fx_signWithEcdsaNistp256WithSha256	in	p_toBeSignedSecuredMessage	octetstring	Signature	octetstring
	in	p_privateKey	octetstring		
fx_verifyWithEcdsaNistp256WithSha256	in	p_toBeVerifiedData	octetstring	Status code	boolean
	in	p_signature	octetstring		
	in	p_publicCompressedKey	octetstring		
	in	p_publicCompressedMode	octetstring		
fx_signWithEcdsaBrainpoolp256WithSha256	in	p_toBeSignedSecuredMessage	octetstring	Signature	octetstring
	in	p_privateKey	octetstring		
fx_verifyWithEcdsaBrainpoolp256WithSha256	in	p_toBeVerifiedData	octetstring	Status code	boolean
	in	p_signature	octetstring		
	in	p_publicCompressedKey	octetstring		
	in	p_publicCompressedMode	octetstring		
fx_signWithEcdsaNistp384WithSha384	in	p_toBeSignedSecuredMessage	octetstring	Signature	octetstring
	in	p_privateKey	octetstring		
fx_verifyWithEcdsaNistp384WithSha384	in	p_toBeVerifiedData	octetstring	Status code	boolean
	in	p_signature	octetstring		
	in	p_publicCompressedKey	octetstring		
	in	p_publicCompressedMode	octetstring		
fx_generateKeyPair	out	p_privateKey	octetstring	Status code	boolean
	out	p_publicKeyX	octetstring		
	out	p_publicKeyY	octetstring		
fx_loadCertificates	in	p_rootDirectory	charstring	Status code	boolean
	in	p_configId	charstring		
fx_unloadCertificates				Status code	boolean
fx_readCertificate	in	p_certificateId	charstring	Status code	boolean
	out	p_certificate	octetstring		
fx_readCertificateDigest	in	p_certificateId	charstring	Status code	boolean
	out	p_certificate	octetstring		
fx_readSigningKey	in	p_keysId	charstring g	Status code	boolean
	out	p_key	Oct32		
fx_readEncryptingKey	in	p_keysId	charstring g	Status code	boolean
	out	p_key	Oct32		
fx_isValidPolygonalRegion	in	p_region	PolygonalRegion	Status code	boolean
fx_isPolygonalRegionInside	in	p_parent	PolygonalRegion	Status code	boolean
	in	p_region	PolygonalRegion		
fx_isLocationInsideCircularRegion	in	p_region	CircularRegion	Status code	boolean
	in	p_location	ThreeDLocation		
fx_isLocationInsideRectangularRegion	in	p_region	RectangularRegions	Status code	boolean
	in	p_location	ThreeDLocation		
fx_isLocationInsidePolygonalRegion	in	p_region	PolygonalRegion	Status code	boolean
	in	p_location	ThreeDLocation		
fx_isLocationInsideIdentifiedRegion	in	p_region	IdentifiedRegion	Status code	boolean
	in	p_location	ThreeDLocation		
fx_dms2dd (degree-minutes-seconds to degree-degree)	in	p_degrees	Int	Status code	boolean
	in	p_minutes	Int		
	in	p_seconds	Float		
	out	p_latlon	Oct1		

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 [1], 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 7) 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 7 specifies the naming guidelines for each element of the TTCN-3 language indicating the recommended prefix, suffixes (if any) and capitalization.

Table 7: 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 8 shows specific naming conventions that apply to the ITS TTCN-3 test suite.

Table 8: ITS specific TTCN-3 naming conventions

Language element	Naming convention	Prefix	Example identifier
ITS Module	Use upper-case initial letter	Its"IUTname"_	ItsSecurity_
Module containing types and values	Use upper-case initial letter	Its"IUTname"_TypesAndValues	ItsSecurity_TypesAndValues
Module containing Templates	Use upper-case initial letter	Its"IUTname"_Templates	ItsSecurity_Templates
Module containing test cases	Use upper-case initial letter	Its"IUTname"_TestCases	ItsSecurity_TestCases
Module containing functions	Use upper-case initial letter	Its"IUTname"_Functions	ItsSecurity_Functions
Module containing external functions	Use upper-case initial letter	Its"IUTname"_ExternalFunctions	ItsSecurity_ExternalFunctions
Module containing components, ports and message definitions	Use upper-case initial letter	Its"IUTname"_Interface	ItsSecurity_Interface
Module containing main component definitions	Use upper-case initial letter	Its"IUTname"_TestSystem	ItsSecurity_TestSystem
Module containing the control part	Use upper-case initial letter	Its"IUTname"_TestControl	ItsSecurity_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("*** TP_SEC_ITSS_ENR_NB_06: INFO: Preamble: Received and answered Enrolment
Request ***")
```

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

- Log statements are used in the body of the functions, so that invocation of functions is 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, "*** TP_SEC_ITSS_ENR_NB_06: PASS: Enrolment Response correctly
accepted ***")
```

7.3.5 Test Case (TC) identifier

Table 9 shows the test case naming convention, which follows the same naming convention as the test purposes.

Table 9: TC naming convention

Identifier:	TC_<ts>_<tgt>_<gr>_<sgr>_<tn>_[x]		
	<ts> = test suite	SEC	Security Test suite
	<tgt> = target	ITSS	ITS Station
	<gr> = group	SND	Send Data
		RCV	Receive Data
	<sgr> =sub-group	MSG	General messages
		CAM	CAM Profile
		DENM	DENM Profile
		GENMSG	Other messages
		CERT	Certificates
	<tn> = testcase sequence number		
	[x] = type of testing	BV	Normal Behaviour
		BO	Exceptional Behaviour

EXAMPLE: TP identifier: TP_SEC_ITSS_SND_CAM_01
TC identifier: TP_SEC_ITSS_RCV_GENMSG_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 10.

Table 10: 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     Draft ETSI TS 103 097 V1.1.14 Clause 5.1    SecuredMessage
 * @reference   EN 302 636-4-1 [1], clauses 9.3.2, 8.6.2 and Annex G
 */
```

Annex A (informative): 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 [1], ETSI TS 103 096-1 [4] and ETSI TS 103 096-2 [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 contained in the archive ts_10309603v010401p0.zip which accompanies the present document.

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 [1]
Protocol to be tested:	Security header and certificate formats
ATS Specification:	ETSI TS 103 096-3
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 103 097 [1]
Version:	
PICS References:	ETSI TS 103 096-1 [4]

B.8.2 IUT information

Security GN PIXITs shall be as in table B.7.

Table B.7: Security GN 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

The relevant GeoNetworking PIXITs (see ETSI TS 102 871-3 [3]) shall be as listed in table B.8.

Table B.8: 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_btpA
PX_BTP_IN_UT_IND	**Comment**	Is BTP header present in IUT's UT indication. Only applicable if PX_GN_UPPER_LAYER == e_btpA or e_btpB
	Type	Boolean
	Def. value	True
PX_DESTINATION_PORT	**Comment**	BTP Destination port of the IUT Set it to predefined CAM or DENM ports regarding which parts is on the test now
	Type	Integer
	Def. value	0

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.6 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	July 2013	Publication
V1.2.1	September 2015	Publication
V1.3.1	March 2017	Publication
V1.4.1	August 2018	Publication