Intelligent Transport Systems (ITS);
Testing;
Conformance test specifications for ITS Security;
Part 1: Protocol Implementation Conformance Statement (PICS)
Contents

Intellectual Property Rights ................................................................................................................................ 4
Foreword............................................................................................................................................................. 4
Modal verbs terminology .................................................................................................................................... 4
1 Scope .............................................................................................................................................................. 5
2 References ................................................................................................................................................ 5
2.1 Normative references ............................................................................................................................... 5
2.2 Informative references.............................................................................................................................. 5
3 Definitions and abbreviations ............................................................................................... .................... 5
3.1 Definitions .................................................................................................................................................. 5
3.2 Abbreviations ............................................................................................................................................. 6
4 Conformance ................................................................................................................................................... 6

Annex A (normative): Security PICS pro forma ......................................................................................... 7
A.1 Partial cancellation of copyright............................................................................................................... 7
A.2 Guidance for completing the PICS pro forma.......................................................................................... 7
A.2.1 Purposes and structure ......................................................................................................................... 7
A.2.2 Abbreviations and conventions ......................................................................................................... 7
A.2.3 Instructions for completing the PICS pro forma ................................................................................. 8
A.3 Identification of the Equipment................................................................................................................ 8
A.3.1 Introduction .......................................................................................................................................... 8
A.3.2 Date of the statement ......................................................................................................................... 9
A.3.3 Equipment Under Test identification ............................................................................................... 9
A.3.4 Product supplier ................................................................................................................................ 9
A.3.5 Client .................................................................................................................................................. 10
A.3.6 PICS contact person ........................................................................................................................ 10
A.4 Identification of the protocol .................................................................................................................. 10
A.5 Global statement of conformance........................................................................................................... 11
A.6 PICS pro forma tables ............................................................................................................................ 11
A.6.1 Introduction .......................................................................................................................................... 11
A.6.2 Main statement ................................................................................................................................... 11
A.6.3 Certificate Management ..................................................................................................................... 11
A.6.4 Generate and Receive Secure Data ................................................................................................. 11
A.6.5 Protocol constants............................................................................................................................. 11

Annex B (informative): Bibliography ........................................................................................................... 12

History .............................................................................................................................................................. 13
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 1 of a multi-part deliverable covering Conformance test specification for ITS Security, as identified below:

- Part 1: "Protocol Implementation Conformance Statement (PICS)";
- Part 2: "Test Suite Structure and Test Purposes (TSS & TP)";
- Part 3: "Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)".

Modal verbs terminology

In the present document "shall", "shall not", "should", "should not", "may", "need not", "will", "will not", "can" and "cannot" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"must" and "must not" are NOT allowed in ETSI deliverables except when used in direct citation.
1 Scope

The present document provides the Protocol Implementation Conformance Statement (PICS) pro forma for the test specifications for security algorithms as specified in ETSI TS 103 097 [1] and in accordance with the relevant guidance given in ISO/IEC 9646-7 [3] and ETS 300 406 [4].

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

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

[1] ETSI TS 103 097 (V1.2.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats”.


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

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

Not applicable.

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] and in ISO/IEC 9646-1 [2] apply.
3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 103 097 [1] and the following apply:

- **PDU**: Protocol Data Unit
- **PICS**: Protocol Implementation Conformance Statement
- **UT**: Upper Tester

4 Conformance

A PICS pro forma which conforms to this PICS pro forma specification shall be technically equivalent to annex A, and shall preserve the numbering and ordering of the items in annex A.

A PICS which conforms to the present document shall:

a) describe an implementation which claims to conform to ETSI TS 103 097 [1];

b) be a conforming PICS pro forma which has been completed in accordance with the instructions for completion given in clause A.2;

c) include the information necessary to uniquely identify both the supplier and the implementation.
Annex A (normative):
Security PICS pro forma

A.1 Partial cancellation of copyright

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 PICS pro forma in this annex so that it can be used for its intended purposes and may further publish the completed PICS pro forma.

A.2 Guidance for completing the PICS pro forma

A.2.1 Purposes and structure

The purpose of the present document is to provide a mechanism whereby a supplier of an implementation of the requirements defined in relevant specifications may provide information about the implementation in a standardized manner.

The PICS pro forma is subdivided into clauses for the following categories of information:
- instructions for completing the PICS pro forma;
- identification of the implementation;
- identification of the protocol;
- PICS pro forma tables (for example: major capabilities, etc.).

A.2.2 Abbreviations and conventions

This annex does not reflect dynamic conformance requirements but static ones. In particular, a condition for support of a PDU parameter does not reflect requirements about the syntax of the PDU (i.e. the presence of a parameter) but the capability of the implementation to support the parameter.

In the sending direction, the support of a parameter means that the implementation is able to send this parameter (but it does not mean that the implementation always sends it).

In the receiving direction, it means that the implementation supports the whole semantic of the parameter that is described in the main part of the present document.

The PICS pro forma contained in this annex is comprised of information in tabular form in accordance with the guidelines presented in ISO/IEC 9646-7 [3].

Item column
The item column contains a number which identifies the item in the table.

Item description column
The item description column describes in free text each respective item (e.g. parameters, timers, etc.). It implicitly means "is <item description> supported by the implementation?".

Reference column
The reference column gives reference to ETSI TS 103 097 [1] except where explicitly stated otherwise.

Status column
The various status used in this annex are in accordance with the rules in table A.1.
Table A.1: Key to status codes

<table>
<thead>
<tr>
<th>Status code</th>
<th>Status name</th>
<th>Meaning</th>
</tr>
</thead>
<tbody>
<tr>
<td>M</td>
<td>mandatory</td>
<td>The capability shall be supported. It is a static view of the fact that the conformance requirements related to the capability in the reference specification are mandatory requirements. This does not mean that a given behaviour shall always be observed (this would be a dynamic view), but that it shall be observed when the implementation is placed in conditions where the conformance requirements from the reference specification compel it to do so. For instance, if the support for a parameter in a sent PDU is mandatory, it does not mean that it shall always be present, but that it shall be present according to the description of the behaviour in the reference specification (dynamic conformance requirement).</td>
</tr>
<tr>
<td>O</td>
<td>optional</td>
<td>The capability may or may not be supported. It is an implementation choice.</td>
</tr>
<tr>
<td>n/a</td>
<td>not applicable</td>
<td>It is impossible to use the capability. No answer in the support column is required.</td>
</tr>
<tr>
<td>X</td>
<td>prohibited (excluded)</td>
<td>There is a requirement not to use this capability in the given context.</td>
</tr>
<tr>
<td>c.&lt;int&gt;</td>
<td>conditional</td>
<td>The requirement on the capability (&quot;m&quot;, &quot;o&quot;, &quot;x&quot; or &quot;n/a&quot;) depends on the support of other optional or conditional items. &quot;int&quot; is an integer identifying an unique conditional status expression which is defined immediately following the table.</td>
</tr>
<tr>
<td>o.&lt;int&gt;</td>
<td>qualified optional</td>
<td>For mutually exclusive or selectable options from a set. &quot;int&quot; is an integer which identifies an unique group of related optional items and the logic of their selection which is defined immediately following the table.</td>
</tr>
<tr>
<td>I</td>
<td>irrelevant (out-of-scope)</td>
<td>Capability outside the scope of the reference specification. No answer is requested from the supplier.</td>
</tr>
</tbody>
</table>

Mnemonic column

The Mnemonic column contains mnemonic identifiers for each item.

Support column

The support column shall be filled in by the supplier of the implementation. The following common notations, defined in ISO/IEC 9646-7 [3], are used for the support column:

Y or y supported by the implementation

N or n not supported by the implementation

N/A, n/a or - no answer required (allowed only if the status is N/A, directly or after evaluation of a conditional status)

References to items

For each possible item answer (answer in the support column) within the PICS pro forma there exists a unique reference, used, for example, in the conditional expressions. It is defined as the table identifier, followed by a solidus character "/", followed by the item number in the table.

EXAMPLE: A.5/2 is the reference to the answer of item 2 in table A.5.

A.2.3 Instructions for completing the PICS pro forma

The supplier of the implementation may complete the PICS pro forma in each of the spaces provided. More detailed instructions are given at the beginning of the different clauses of the PICS pro forma.

A.3 Identification of the Equipment

A.3.1 Introduction

Identification of the Equipment shall be filled in so as to provide as much detail as possible regarding version numbers and configuration options.

The product supplier information and client information shall both be filled in if they are different.
A person who can answer queries regarding information supplied in the PICS shall be named as the contact person.

A.3.2 Date of the statement ........................................................................................................................................

A.3.3 Equipment Under Test identification

Name:
.........................................................................................................................................................................................
.........................................................................................................................................................................................

Hardware configuration:
.........................................................................................................................................................................................
.........................................................................................................................................................................................
.........................................................................................................................................................................................

Software configuration:
.........................................................................................................................................................................................
.........................................................................................................................................................................................
.........................................................................................................................................................................................

A.3.4 Product supplier

Name:
.........................................................................................................................................................................................

Address:
.........................................................................................................................................................................................
.........................................................................................................................................................................................
.........................................................................................................................................................................................

Telephone number:
.........................................................................................................................................................................................

Facsimile number:
.........................................................................................................................................................................................

E-mail address:
.........................................................................................................................................................................................

Additional information:
.........................................................................................................................................................................................
.........................................................................................................................................................................................
A.3.5 Client

Name: ..........................................................................................................................................................................................
Address: .......................................................................................................................................................................................
.......................................................................................................................................................................................
.......................................................................................................................................................................................
Telephone number: ........................................................................................................................................................................
Facsimile number: ........................................................................................................................................................................
E-mail address: ...........................................................................................................................................................................
Additional information: ...................................................................................................................................................................
.......................................................................................................................................................................................
.......................................................................................................................................................................................

A.3.6 PICS contact person

Name: ..........................................................................................................................................................................................
Telephone number: ........................................................................................................................................................................
Facsimile number: ........................................................................................................................................................................
E-mail address: ...........................................................................................................................................................................
Additional information: ...................................................................................................................................................................
.......................................................................................................................................................................................
.......................................................................................................................................................................................

A.4 Identification of the protocol

The present document applies to the following specifications:

ETSI TS 103 097 [1].
A.5 Global statement of conformance

Are all mandatory capabilities implemented? (Yes/No) .......................

NOTE: Answering "No" to this question indicates non-conformance to the ITS Security standard specification ETSI TS 103 097 [1]. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming, on pages attached to the PICS pro forma.

A.6 PICS pro forma tables

A.6.1 Introduction

Unless stated otherwise, the column references of all tables below indicate the clause numbers of ETSI TS 103 097 [1].

A.6.2 Main statement

Table A.2: Main statement

<table>
<thead>
<tr>
<th>Item</th>
<th>Is the IUT implemented to support:</th>
<th>Reference</th>
<th>Status</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Support ETSI TS 103 097 [1]</td>
<td>N/A</td>
<td>m</td>
<td></td>
</tr>
</tbody>
</table>

A.6.3 Certificate Management

Table A.3: Certificate management

<table>
<thead>
<tr>
<th>Prerequisite: A.2/1</th>
<th>Item</th>
<th>Is the IUT implemented to support:</th>
<th>Reference</th>
<th>Status</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>loading of custom certificates?</td>
<td>N/A</td>
<td>o</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>selecting of certificates by the UT interface?</td>
<td>N/A</td>
<td>o</td>
<td></td>
</tr>
</tbody>
</table>

A.6.4 Generate and Receive Secure Data

Table A.4: Certificate geographic regions

<table>
<thead>
<tr>
<th>Prerequisite: A.2/1</th>
<th>Item</th>
<th>Is the IUT implemented to support:</th>
<th>Reference</th>
<th>Status</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>certificate without GeographicRegion</td>
<td>4.2.20</td>
<td>o</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>certificate containing circular GeographicRegion</td>
<td>4.2.20</td>
<td>o</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>certificate containing rectangular GeographicRegion</td>
<td>4.2.20</td>
<td>o</td>
<td></td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>certificate containing polygonal GeographicRegion</td>
<td>4.2.20</td>
<td>o</td>
<td></td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>certificate containing identified GeographicRegion</td>
<td>4.2.20</td>
<td>o</td>
<td></td>
</tr>
</tbody>
</table>

Table A.5: Identified geographic region dictionaries

<table>
<thead>
<tr>
<th>Prerequisite: A.4/5</th>
<th>Item</th>
<th>Is the IUT implemented to support:</th>
<th>Reference</th>
<th>Status</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1</td>
<td>ISO-3166-1 region dictionary</td>
<td>4.2.26</td>
<td>o</td>
<td>□Yes □No</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>UN-STATS region dictionary</td>
<td>4.2.26</td>
<td>o</td>
<td>□Yes □No</td>
</tr>
</tbody>
</table>

A.6.5 Protocol constants

Table A.6: Protocol constants

<table>
<thead>
<tr>
<th>Item</th>
<th>Constant</th>
<th>Reference</th>
<th>Status</th>
<th>Value allowed</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>beacon ITS AID</td>
<td>7.3</td>
<td>o</td>
<td>0 - skip beacon tests</td>
<td>NN - value of ITS AID</td>
</tr>
</tbody>
</table>
Annex B (informative):
Bibliography


## History

<table>
<thead>
<tr>
<th>Document history</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1.1.1 July 2013</td>
</tr>
<tr>
<td>V1.2.1 September 2015</td>
</tr>
</tbody>
</table>