



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

Reference

RTS/ITS-00542

Keywords

ITS, PICS, security

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.

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 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	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.....	6
3.1 Definitions	6
3.2 Abbreviations	6
4 Conformance	6
Annex A (normative): Security PICS pro forma.....	7
A.1 The right to copy	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.....	9
A.3.1 Introduction	9
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.....	11
A.5 Global statement of conformance.....	11
A.6 PICS pro forma tables	11
History	13

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 1 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 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 [i.2] and ETSI ETS 300 406 [i.3].

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] IEEE Std 1609.2™-2016: "IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages", as amended by IEEE Std 1609.2a™-2017: "IEEE Standard for Wireless Access In Vehicular Environments - Security Services for Applications and Management Messages - Amendment 1".

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] ISO/IEC 9646-1: "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 1: General concepts".
- [i.2] ISO/IEC 9646-7: "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 7: Implementation Conformance Statements".
- [i.3] ETSI ETS 300 406: "Methods for testing and Specification (MTS); Protocol and profile conformance testing specifications; Standardization methodology".

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 [i.1] apply.

3.2 Abbreviations

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

CRL	Certificate Revocation List
GN-MGMT	GeoNetworking Management message
P2PCD	Peer-to-Peer Certificate Distribution
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement

4 Conformance

- a) A PICS pro forma which conforms to this PICS pro forma specification shall be technically equivalent to annex A of the IEEE Std 1609.2 [2] and to annex A of the present document and shall preserve the numbering and ordering of the items in annex A.
- b) The following clauses of the IEEE Std 1609.2 [2] are irrelevant for conformance with ETSI TS 103 097 [1] and may be skipped:
 - A.2.3.2 Certificate revocation list (CRL) verification entity;
 - A.2.3.3 Peer-to-peer certificate distribution (P2PCD) functionality (S3.1, S3.2, S3.3, S3.4).

A PICS which conforms to the present document shall:

- a) describe an implementation which claims to conform to ETSI TS 103 097 [1] and IEEE Std 1609.2 [2];
- 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 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 Security 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 [i.2].

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

Status code	Status name	Meaning
M	mandatory	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).
O	optional	The capability may or may not be supported. It is an implementation choice.
n/a	not applicable	It is impossible to use the capability. No answer in the support column is required.
X	prohibited (excluded)	There is a requirement not to use this capability in the given context.
c.<int>	conditional	The requirement on the capability ("m", "o", "x" or "n/a") depends on the support of other optional or conditional items. "int" is an integer identifying a unique conditional status expression which is defined immediately following the table.
o.<int>	qualified optional	For mutually exclusive or selectable options from a set "int" is an integer which identifies a unique group of related optional items and the logic of their selection which is defined immediately following the table.
I	irrelevant (out-of-scope)	Capability outside the scope of the reference specification. No answer is requested from the supplier.

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 [i.2], 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

This PICS proforma applies to the following standard: ETSI TS 103 097 (V1.3.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats".

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

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

Table A.2: Content of SPDU

Item	Is the IUT implemented to support:	Reference	Override	Status	Support
1	generationTime in SignedData	5.2	[2] S1.2.2.2.3	m	
2	p2pcdLearningRequest in SignedData	5.2	[2] S1.2.2.2.6	x	
3	missingCrIIdentifier in SignedData	5.2	[2] S1.2.2.2.7	x	
4	Maximum number of certificates in the signature	5.2	[2] S1.2.2.3.2.1	1	
5	Signing with explicit certificates	6, [2], 6.4.6	[2] S1.2.2.7	m	
6	Signing with implicit certificates	6	[2] S1.2.2.8	x	

Table A.3: Security profile for CAMs

Item	Is the IUT implemented to support:	Reference	Override	Status	Support
1	Secured CA messages	7.1.1		o	
2	Inline P2PCD operations	7.1.1 [2], 8.2.4.1.2, 8.2.4.2.3	[2], S3.6	m	
3	Support a signer identifier of type digest	7.1.1	[2], S1.2.2.3.1	m	
4	Support a signer identifier of type certificate		[2], S1.2.2.3.2	m	

Table A.4: Security profile for DENMs

Item	Is the IUT implemented to support:	Reference	Override	Status	Support
1	Secured DEN messages	7.1.2		o	
4	Support a signer identifier of type certificate	7.1.2	[2], S1.2.2.3.2	m	

Table A.5: Security profile for other messages

Item	Is the IUT implemented to support:	Reference	Status	Support
1	Secured other messages	7.1.3	o	

Table A.6: Security profile for other messages

Item	Is the IUT implemented to support:	Reference	Status	Support
1	Secured other messages	7.1.3	o	

Table A.7: Protocol constants

Item	Constant	Value allowed	Reference	Status	Value
1	Beacon ITS AID	0 - skip beacon tests NN - value of ITS AID Default: 141 (GN-MGMT)	7.3	m	

Table A.8: Certificate management

Item	Is the IUT implemented to support:	Reference	Status	Support
1	Loading of custom certificates	6	o	

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