ETSI TS 103 525-1 V2.1.1 (2024-09)

Intelligent Transport Systems (ITS);
Testing;
Conformance test specifications for ITS PKI management;
Part 1: Protocol Implementation Conformance Statement (PICS); Release 2

Reference
RTS/ITS-00597

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 - 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 1 of a multi-part deliverable covering Conformance test specifications for ITS PKI management, 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 102 941 [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 102 941 (V2.2.1): "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management; Release 2".

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

[3] 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".

[4] ETSI TS 103 601 (V2.1.1): "Intelligent Transport Systems (ITS); Security; Security management messages communication requirements and distribution protocols; 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] 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 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 102 941 [1] and ISO/IEC 9646-1 [i.1] apply.

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI TS 103 097 [2] and the following apply:

CRL	Certificate Revocation List
PDU	Protocol Data Unit
PICS	Protocol Implementation Conformance Statement

4 Conformance

A PICS pro forma which conforms to this PICS pro forma specification shall be technically equivalent to annex A of the present document 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 102 941 [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 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 [2] unless otherwise stated.

Status column

The status column describes the status of the item. The various status used in this annex are in accordance with the rules described in IEEE 1609.2 [3], annex A. Predicate in conditional and optional items is of form of Reference to items, as described below.

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 dot character ".", followed by the item number in the table.

EXAMPLE: A.5.2.1 is the reference to the answer of item 2.1 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 details as possible regarding version numbers and configuration options.

Both the product supplier information and client information shall 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 specification: ETSI TS 102 941 [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 102 941 [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 102 941 [1].

The various status used in this annex are in accordance with the rules described in IEEE 1609.2 [3], annex A.

Table A.1: Security containers and algorithms

Item	Is the IUT implemented to support:	Reference	Status	Support
1	Secure PDU (SPDU) support	6.2	M	
2	Support SPDU signing	6.2, S1.2.2 [3]	M	
2.1	… with hash algorithm SHA-256	S1.2.2.1.1 [3]	M	
2.2	… with hash algorithm SHA-384	S1.2.2.1.2 [3]	O	
2.3	… with ECDSA-256 NIST p256	S1.2.2.4.1.1 [3]	M	
2.4	… with ECDSA-256 Brainpool p256	S1.2.2.4.1.2 [3]	O	
2.5	… with ECDSA-384 Brainpool p384	S1.3.2.4.2 [3]	O	
3	Support SPDU signature verification	6.2, S1.3.2 [3]	M	
3.1	… with hash algorithm SHA-256	S1.3.2.1.1 [3]	M	
3.2	… with hash algorithm SHA-384	S1.3.2.1.2 [3]	M	
3.3	… with ECDSA-256 NIST p256	S1.3.2.4.1.1 [3]	M	
3.4	… with ECDSA-256 Brainpool p256	S1.3.2.4.1.2 [3]	M	
3.5	… with ECDSA-384 Brainpool p384	S1.3.2.4 [3]	M	
4	Support public-key encryption	6.2, S1.2.3 [3]	M	
4.1	… using ECIES-256 with NIST p256	S1.2.3.4.1.1 [3]	M	
4.2	… using ECIES-256 with Brainpool p256	S1.2.3.4.1.2 [3]	O	
5	Support public-key decryption	S1.3.3 [3]	M	
5.1	… using ECIES-256 with NIST p256	S1.3.3.3.1.1 [3]	M	
5.2	… using ECIES-256 with Brainpool p256	S1.3.3.3.1.2 [3]	M	
6	IUT supports Butterfly Expension Keys	6.2.3.5	O	
7	IUT supports X.509 certificates	6.2.3.5	O	

Table A.2: ITS-S testing

Item	Is the IUT implemented to support:	Reference	Status	Support
1	IUT is ITS-S		C1	
2	IUT supports enrolment procedure	6.2.3.2	A.2.1:O	
2.1	IUT supports re-enrolment procedure	6.2.3.2	A.2.2:O	
2.2	IUT supports the enrolment repetition mechanism	5.1 [4]	A.2.2:O	
3	IUT supports authorization procedure	6.2.3.3	A.2.1:M	
3.1	IUT does not require privacy in authorization requests	6.2.3.3	A.2.3:O	
3.2	IUT does not use prove of possession for authorization requests	6.2.3.3	A.2.3:O	
3.3	IUT supports the authorization repetition mechanism	5.2 [4]	A.2.3:O	

Table A.3: PKI testing

Item	Is the IUT implemented to support:	Reference	Status	Support
1	IUT is a PKI	6	C1	
2	IUT supports EA behaviour	6	A.3.1:O	
3	IUT supports AA behaviour	6	A.3.1:O	
4	IUT supports RCA behaviour	6	A.3.1:O	
5	IUT supports DC behaviour	6	A.3.1:O	
6	IUT supports TLM behaviour	6	A.3.1:O	
7	IUT supports CPOC behaviour	6	A.3.1:O	

Table A.4: EA testing

Item	Is the IUT implemented to support:	Reference	Status	Support
1	IUT supports ITS-S enrolment	6.2.3.3	A.3.2:M	
2	IUT supports ITS-S re-enrolment	6.2.3.3	A.4.1:O	
3	IUT supports authorization validation handling	6.2.3.4	A.3.2:O	
4	IUT supports ITS-S enrolment request repetition mechanism	5.1 [4]	A.4.1:M	
5	IUT supports ITS-S enrolment using X.509 certificates	6.1.3	A1.6:O	

Table A.5: AA testing

Item	Is the IUT implemented to support:	Reference	Status	Support
1	IUT supports ITS-S authorization	6.2.3.3	A.3.3:M	
2	IUT supports authorization requests without prove of possession	6.2.3.3	A.5.1:O	
3	IUT supports authorization request without privacy	6.2.3.3	A.5.1:O	
4	IUT supports authorization validation request	6.2.3.4	A.3.3:O	
5	IUT supports authorization requests repetition mechanism	5.2 [4]	A.5.1:M	
6	IUT supports authorization using Butterfly Keys	6.2.3.5	A.3.3 and A.1.6:O	

Table A.6: RCA/DC testing

Item	Is the IUT implemented to support:	Reference	Status	Support
1	IUT supports CRL generation	6.3.3	A.3.4:M	
2	IUT supports CTL generation	6.3.2	A.3.4:O	
2.1	IUT supports Delta CTL generation	6.3.2	A.6.2:O	
3	IUT supports CRL distribution	6.3.3	A.3.5:M	
4	IUT supports CTL distribution	6.3.2	A.3.5:O	
4.1	IUT supports Delta CTL distribution	6.3.2	A.3.5:O	

Table A.7: TLM/CPOC testing

Item	Is the IUT implemented to support:	Reference	Status	Support
1	IUT supports ECTL generation	6.3.1	A.3.6:M	
1.1	IUT supports Delta ECTL generation	6.3.1	A.7.1:M	
2	IUT supports ECTL distribution	6.3.1	A.3.7:M	
2.1	IUT supports Delta ECTL distribution	6.3.1	A.3.7:M	

Table A.8: CRL/CTL Handling

Item	Is the IUT implemented to support:	Reference	Status	Support
1	IUT is able to handle ECTL information	6.3.6	O	
1.1	IUT is able to handle Delta ECTL information	6.3.6	A.8.1:O	
2	IUT is able to download ECTL	6.3.1	A.8.1:O	
3	IUT is able to handle Root CTL information	6.3.6	O	
3.1	IUT is able to handle Delta Root CTL information	6.3.6	A.8.3:O	
4	IUT is able to download Root CTL	6.3.1	A.8.3:O	
5	IUT is able to handle CRL information	6.3.6	M	
6	IUT is able to download CRL	6.3.1	A.8.5:O	
7	IUT is able to redistribute Delta ECTL	4.2, 5.3, 5.4 [4]	A.2.1 & A.8.1.1: O	
8	IUT is able to redistribute Delta Root CTL information	4.2, 5.3, 5.4 [4]	A.2.1 & A.8.3.1: O	
9	IUT is able to redistribute CRL information	4.3, 5.3, 5.4 [4]	A.2.1 & A.8.5: O	

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