ETSI TS 103 096-1 V2.1.1 (2024-08)

TECHNICAL SPECIFICATION

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

Reference

RTS/ITS-005118

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

Important notice

The present document can be downloaded from the ETSI Search & Browse Standards application.

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 prevailing version of an ETSI deliverable is the one made publicly available in PDF format on ETSI deliver.

Users should be aware that the present document may be revised or have its status changed, this information is available in the Milestones listing.

If you find errors in the present document, please send your comments to the relevant service listed under Committee Support Staff.

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure (CVD) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

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 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 (V2.1.1): "Intelligent Transport Systems (ITS); Security; Security header and certificate formats, Release 2".

[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 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TS 103 097 [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 [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] with the amendments of 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 based on 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).

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?".

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 Std 1609.2 [2], annex A.

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)
number value	supported number or amount of items

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.5.1/2 is the reference to the answer of item 2 in table A.5.1.

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.

The PICS pro forma in the present document contains two set of statements:

Clause A.6 - the PICS pro forma for the IEEE Std 1609.2 [2], containing the subset of the full PICS pro forma, relative to the content of ETSI TS 103 097 [1].

Clause A.7 - the PICS pro forma for the ETSI TS 103 097 [1], containing PICS entities for additional requirements from the ETSI TS 103 097 [1].

Both parts of the pro forma need to be filled in.

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

This PICS pro forma applies to the following standard: ETSI TS 103 097 [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 IEEE 1609.2 PICS pro forma

This presents a list of the security functionality that an implementation may claim to support.

The reference column of the following table indicates reference to IEEE Std 1609.2 [2] unless otherwise stated.

Item	Security configuration (top-level)	Reference	Status	Support
S1.	Support secure data service		O1	□ Yes □ No
S1.1.	Secure Data Exchange Entity (SDEE) identification	4.2.2.1	S1:M	□ Yes □ No
S1.1.1.	Support only one SDEE	4.2.2.1	S1.1:C1	□ Yes □ No
S1.1.2.	Distinguish between SDEEs	4.2.2.1	S1.1:C1	□ Yes □ No
S1.2.	Generate Secured Protocol Data Unit (SPDU)		S1:O2	□ Yes □ No
S1.2.1.	Create `Ieee1609Dot2Data` containing unsecured data	4.2.2.2.2	S1.2:O3	□ Yes □ No
S1.2.2.	Create `Ieee1609Dot2Data` containing valid `SignedData`	4.2.2.2.3, 5.2, 5.3.1, 5.3.3, 5.3.7, 6.3.4, 6.3.9, 9.3.9.1	S1.2:O3	□ Yes □ No
S1.2.2.1.	Using a valid HashAlgorithm	6.3.5	S1.2.2:M	□ Yes □ No
S1.2.2.1.1.	Support signing with hash algorithm SHA-256	6.3.5	S1.2.2:O3a	□ Yes □ No
S1.2.2.1.2.	Support signing with hash algorithm SHA-384	6.3.5	S1.2.2:O3a	□ Yes □ No
S1.2.2.1.3.	Support signing with other hash algorithm	6.3.5	S1.2.2:O	□ Yes □ No
S1.2.2.2.	Containing a Signed Data payload	6.3.6	S1.2.2:M	□ Yes □ No
S1.2.2.2.1.	… with payload containing data	6.3.7	S1.2.2.2:O4	□ Yes □ No
S1.2.2.2.2.	… with payload containing extDataHash	6.3.7	S1.2.2.2: O4	□ Yes □ No
S1.2.2.2.3.	… with generationTime in the security headers	6.3.9, 6.3.11	S1.2.2.2: O	□ Yes □ No
S1.2.2.2.4.	… with expiryTime in the security headers	6.3.9, 6.3.11	S1.2.2.2: O	□ Yes □ No
S1.2.2.2.5.	… with generationLocation in the security headers	6.3.9, 6.3.12	S1.2.2.2: O	□ Yes □ No
S1.2.2.2.6.	… with p2pcdLearningRequest in the security headers	6.3.9, 6.3.27	S1.2.2.2: O	□ Yes □ No
S1.2.2.2.7.	… with missingCrlIdentifier in the security headers	6.3.9, 6.3.16	S1.2.2.2: O	□ Yes □ No
S1.2.2.2.8.	… with encryptionKey in the security headers	6.3.9, 6.3.18	S1.2.2.2: O	□ Yes □ No
S1.2.2.2.8.1.	… … with a PublicEncryptionKey	6.3.9, 6.3.18, 6.3.19	S1.2.2.2.8:O5	□ Yes □ No
S1.2.2.2.8.2.	… … with a SymmetricEncryptionKey	6.3.9, 6.3.18, 6.3.20	S1.2.2.2.8:O5	□ Yes □ No
S1.2.2.2.9.	… with pduFunctionalType in the security headers	6.3.9, 6.3.25	S1.2.2.2: O	□ Yes □ No
S1.2.2.3.	Support a SignerIdentifier	6.3.26	S1.2.2:M	□ Yes □ No
S1.2.2.3.1.	… of type digest	6.3.28	S1.2.2.3:O6	□ Yes □ No
S1.2.2.3.2.	… of type certificate	6.4.2	S1.2.2.3:O6	□ Yes □ No
S1.2.2.3.2.1.	… … maximum number of certificates included in the SignerIdentifier	6.3.26	S1.2.2.3.2 1:M > 1:O	Enter number: ( )
S1.2.2.4.	Support a Signature	6.3.30	S1.2.2:M	□ Yes □ No
S1.2.2.4.1.	… an ecdsa256Signature	6.3.31	S1.2.2.4:O6a	□ Yes □ No
S1.2.2.4.1.1.	… … using NIST p256	6.3.31	S1.2.2.4.1:O7	□ Yes □ No
S1.2.2.4.1.2.	… … using Brainpool p256r1	6.3.31	S1.2.2.4.1:O7	□ Yes □ No
S1.2.2.4.1.3.	… … with a x-only *r* value	6.3.23	S1.2.2.4.1:O8	□ Yes □ No
S1.2.2.4.1.4.	… … with a compressed *r* value	6.3.23	S1.2.2.4.1:O8	□ Yes □ No
S1.2.2.4.1.5.	… … with an uncompressed *r* value	6.3.23	S1.2.2.4.1:O8	□ Yes □ No
S1.2.2.4.2.	… an ecdsa384Signature using Brainpool p384r1	6.3.32	S1.2.2.4:O6a	□ Yes □ No
S1.2.2.4.2.1.	… … with a x-only *r* value	6.3.23	S1.2.2.4.1:O8	□ Yes □ No
S1.2.2.4.2.2.	… … with a compressed *r* value	6.3.23	S1.2.2.4.1:O8	□ Yes □ No

Item	Security configuration (top-level)	Reference	Status	Support
S1.2.2.4.2.3.	… … with an uncompressed *r* value	6.3.23	S1.2.2.4.1:O8	□ Yes □ No
S1.2.2.5.	Determine that certificate used to sign data is valid (part of a consistent chain, valid at the current time and location, has not been revoked)	5.2	S1.2.2:M	□ Yes □ No
S1.2.2.5.1.	Determine that the generation location is consistent with the region in the certificate	5.2.4.2.3, 6.4.17	S1.2.2.5:M	□ Yes □ No
S1.2.2.5.1.1.	Support a circularRegion	6.4.17, 6.4.18	S1.2.2.5.1:O9	□ Yes □ No
S1.2.2.5.1.2.	Support a rectangularRegion	6.4.17, 6.4.20	S1.2.2.5.1:O9	□ Yes □ No
S1.2.2.5.1.2.1.	Maximum number of rectangularRegions supported	6.4.17, 6.4.20	S1.2.2.5.1.2 8:M > 8:O	Enter number: ( )
S1.2.2.5.1.3.	Support a polygonalRegion	6.4.17, 6.4.21	S1.2.2.5.1:O9	□ Yes □ No
S1.2.2.5.1.3.1.	Maximum number of points in a polygonalRegion	6.4.17, 6.4.21	S1.2.2.5.1.3 8:M > 8:O	Enter number: ( )
S1.2.2.5.1.4.	Support identifiedRegion	6.4.17, 6.4.22	S1.2.2.5.1:O9	□ Yes □ No
S1.2.2.5.1.4.1.	Maximum number of identifiedRegions supported	6.4.17, 6.4.22	S1.2.2.5.1.4: 8:M > 8:O	Enter number: ( )
S1.2.2.5.1.4.2.	Support IdentifiedRegion of type CountryOnly	6.4.22, 6.4.23	S1.2.2.5.1.4:O10	□ Yes □ No
S1.2.2.5.1.4.3.	Support IdentifiedRegion of type CountryAndRegions	6.4.22, 6.4.24	S1.2.2.5.1.4:O10	□ Yes □ No
S1.2.2.5.1.4.4.	Support IdentifiedRegion of type CountryAndSubregions	6.4.22, 6.4.25	S1.2.2.5.1.4:O10	□ Yes □ No
S1.2.2.5.1.4.5.	List of supported IdentifiedRegions (see note) NOTE: This list might or might not include an indication of the accuracy of the internal representation of each identified region.	5.2.4.4, 6.4.22	S1.2.2.5.1.4:M	Provide as Additional Information
S1.2.2.5.2.	Determine that the certificate has the proper appPermissions	6.4.8, 6.4.28	S1.2.2.5: M	□ Yes □ No
S1.2.2.5.2.1.	Maximum number of PsidSsp in the appPermissions sequence	6.4.8, 6.4.28	S1.2.2.5.2 8:M > 8:O	Enter number: ( )
S1.2.2.5.3.	Maximum supported length of the full chain (sending)	5.1.2.2	S1.2.2.5: 2:M >2:O	Enter number: ( )
S1.2.2.6.	Determine that key and certificate used to sign are a valid pair	5.3.7	S1.2.2:M	□ Yes □ No
S1.2.2.7.	Support signing with explicit certificates	6.4.6	S1.2.2.5:O11	□ Yes □ No
S1.2.2.8.	Support signing with implicit certificates	5.3.2, 6.4.5	S1.2.2.5:O11	□ Yes □ No
S1.2.2.9.	Generate Elliptic Curve Digital Signature Algorithm (ECDSA) keypairs using a high-quality random number generator	5.3.6	S1.2.2.4.1: M	□ Yes □ No
S1.2.3.	Create `Ieee1609Dot2Data` containing `EncryptedData`	4.2.2.3.2, 5.3.4, 6.3.33	S1.2:O2	□ Yes □ No
S1.2.3.1.	Generate Elliptic Curve Integrated Encryption Scheme (ECIES) ephemeral keypairs using a high-quality random number generator	5.3.4, 5.3.5, 5.3.6	S1.3.3: M	□ Yes □ No
S1.2.3.2.	Maximum number of recipients supported	6.3.33	S1.2.3 8:M > 8:O	Enter number: ( )
S1.2.3.2.1.	Containing PreSharedKeyRecipientInfo	6.3.34, 6.3.35	S1.2.3.2:O12	□ Yes □ No
S1.2.3.2.2.	Containing symmRecipientInfo	6.3.34, 6.3.36	S1.2.3.2:O12	□ Yes □ No
S1.2.3.2.3.	Containing certRecipientInfo	6.3.34, 6.3.37	S1.2.3.2:O12	□ Yes □ No
S1.2.3.2.4.	Containing signedDataRecipientInfo	6.3.34, 6.3.37	S1.2.3.2:O12	□ Yes □ No

Item	Security configuration (top-level)	Reference	Status	Support
S1.2.3.2.5.	Containing rekRecipientInfo	6.3.34, 6.3.37	S1.2.3.2:O12	□ Yes □ No
S1.2.3.3.	Support public-key encryption	5.3.5	S1.2.3.2.3 OR S1.2.3.2.4 OR S1.2.3.2.5:M	□ Yes □ No
S1.2.3.3.1.	… using ECIES-256	5.3.5	S1.2.3.3:M	□ Yes □ No
S1.2.3.3.1.1.	… … using NIST p256	5.3.5	S1.2.3.3.1:O14	□ Yes □ No
S1.2.3.3.1.2.	… … using Brainpool p256r1	5.3.5	S1.2.3.3.1:O14	□ Yes □ No
S1.2.3.3.1.3.	Support encrypting to an uncompressed encryption key	6.3.18	S1.2.3.3.1:O15	□ Yes □ No
S1.2.3.3.1.4.	Support encrypting to a compressed encryption key	6.3.18	S1.2.3.3.1:O15	□ Yes □ No
S1.2.3.3.1.5.	Support encrypting to an encryption key included in an explicit cert	6.3.18	S1.2.3.3.1:O16	□ Yes □ No
S1.2.3.3.1.6.	Support encrypting to an encryption key included in an implicit cert	6.3.18	S1.2.3.3.1:O16	□ Yes □ No
S1.2.3.3.2.	… using a different algorithm introduced at a later date	6.3.40	S1.2.3.3:O	□ Yes □ No
S1.2.3.4.	Support symmetric encryption	6.3.41	S1.2.3:O13	□ Yes □ No
S1.2.3.4.1.	… using AES-128	5.3.8, 6.3.41	S1.2.3.4:M	□ Yes □ No
S1.2.3.4.2.	… using a different algorithm introduced at a later date	6.3.37	S1.2.3.4:O	□ Yes □ No
S1.2.3.5.	Return ephemeral key used in data encryption	5.3.4, 6.3.34	S1.2.3.4:O	□ Yes □ No
S1.3.	Receive secured protocol data unit (SPDU)		S1:O2	□ Yes □ No
S1.3.1.	Support preprocessing SPDUs	4.2.2.3.1	S1.3.2.3.1, S3.3 S3.4:M	□ Yes □ No
S1.3.2.	Verify `Ieee1609Dot2Data` containing `SignedData`	4.2.2.3.2, 5.2, 5.3.1, 5.3.3, 5.3.7, 6.3.4, 6.3.9	S1.3:O17	□ Yes □ No
S1.3.2.1.	Using a valid HashAlgorithm		S1.3.2:M	□ Yes □ No
S1.3.2.1.1.	Verify signed data using HashAlgorithm SHA-256	6.3.5	S1.3.2.1:O17a	□ Yes □ No
S1.3.2.1.2.	Verify signed data using HashAlgorithm SHA-384	6.3.5	S1.3.2.1:O17a	□ Yes □ No
S1.3.2.1.3.	Verify signed data using another HashAlgorithm	6.3.5	S1.3.2.1:O	□ Yes □ No
S1.3.2.2.	Containing a Signed Data payload	6.3.6	S1.3.2:M	□ Yes □ No
S1.3.2.2.1.	… with payload containing data	6.3.7	S1.3.2.2:O18	□ Yes □ No
S1.3.2.2.2.	… with payload containing extDataHash	6.3.7	S1.3.2.2:O18	□ Yes □ No
S1.3.2.2.3.	… with generationTime in the security headers	6.3.9, 6.3.11	S1.3.2.2:O	□ Yes □ No
S1.3.2.2.4.	… with expiryTime in the security headers	6.3.9, 6.3.11	S1.3.2.2:O	□ Yes □ No
S1.3.2.2.5.	… with generationLocation in the security headers	6.3.9, 6.3.12	S1.3.2.2:O	□ Yes □ No
S1.3.2.2.6.	… with missingCertIdentifier in the security headers	6.3.9, 6.3.27	S1.3.2.2:O	□ Yes □ No
S1.3.2.2.7.	… with missingCrlIdentifier in the security headers	6.3.9, 6.3.16	S1.3.2.2:O	□ Yes □ No
S1.3.2.2.8.	… with encryptionKey in the security headers	6.3.9, 6.3.18	S1.3.2.2:O	□ Yes □ No
S1.3.2.2.9.	… with pduFunctionalType in the security headers	6.3.9, 6.3.25	S1.3.2.2: O	□ Yes □ No
S1.3.2.2.9.1.	… … with a PublicEncryptionKey	6.3.9, 6.3.18, 6.3.19	S1.3.2.2.8:O19	□ Yes □ No
S1.3.2.2.9.2.	… … with a SymmetricEncryptionKey	6.3.9, 6.3.18, 6.3.20	S1.3.2.2.8:O19	□ Yes □ No
S1.3.2.3.	Support a SignerIdentifier	6.3.26	S1.3.2:M	□ Yes □ No
S1.3.2.3.1.	… of type digest	6.3.28	S1.3.2.3:O20	□ Yes □ No
S1.3.2.3.2.	… of type certificate	6.4.2	S1.3.2.3:O20	□ Yes □ No

Item	Security configuration (top-level)	Reference	Status	Support
S1.3.2.3.2.1.	… … maximum number of certificates included in the SignerIdentifier	6.3.26	S1.3.2.3.2 1:M > 1:O	Enter number: ( )
S1.3.2.4.	Support a Signature	6.3.30	S1.3.2:M	□ Yes □ No
S1.3.2.4.1.	… a ecdsa256Signature	6.3.31	S1.3.2.4:)O20a	□ Yes □ No
S1.3.2.4.1.1.	… … using NIST p256	6.3.31	S1.3.2.4.1:O21	□ Yes □ No
S1.3.2.4.1.2.	… … using Brainpool p256r1	6.3.31	S1.3.2.4.1:O21	□ Yes □ No
S1.3.2.4.1.3.	… … with a x-only *r* value	6.3.23	S1.3.2.4.1:O22	□ Yes □ No
S1.3.2.4.1.4.	… … with a compressed *r* value	6.3.23	S1.3.2.4.1:O22	□ Yes □ No
S1.3.2.4.1.5.	… … with a compressed *r* value and fast verification	6.3.23	S1.3.2.4.1:O22	□ Yes □ No
S1.3.2.4.1.6.	… … with a uncompressed *r* value	6.3.23	S1.3.2.4.1:O22	□ Yes □ No
S1.3.2.4.1.7.	… … with a uncompressed *r* value and fast verification	6.3.23	S1.3.2.4.1:O22	□ Yes □ No
S1.3.2.4.2.	… an ecdsa384Signature using Brainpool p384r1	6.3.32	S1.3.2.4:O20a	□ Yes □ No
S1.3.2.4.2.1.	… … with a x-only *r* value	6.3.23	S1.3.2.4.1:O22	□ Yes □ No
S1.3.2.4.2.2.	… … with a compressed *r* value	6.3.23	S1.3.2.4.1:O22	□ Yes □ No
S1.3.2.4.2.3.	… … with a compressed *r* value and fast verification	6.3.23	S1.3.2.4.1:O22	□ Yes □ No
S1.3.2.4.2.4.	… … with a uncompressed *r* value	6.3.23	S1.3.2.4.1:O22	□ Yes □ No
S1.3.2.4.2.5.	… … with a uncompressed *r* value and fast verification	6.3.23	S1.3.2.4.1:O22	□ Yes □ No
S1.3.2.5.	`SignedData` verification fails if the certificate is not valid (part of a consistent chain, valid at the current time and location, has not been revoked)	5.2, 6.4.2	S1.3.2:M	□ Yes □ No
S1.3.2.5.1.	Reject data based on generation location being inconsistent with certificate	6.4.8, 6.4.17	S1.3.2.5:O	□ Yes □ No
S1.3.2.5.1.1.	… using a circularRegion	6.4.17, 6.4.18	S1.3.2.5.1:O23	□ Yes □ No
S1.3.2.5.1.2.	Support a rectangularRegion	6.4.17, 6.4.20	S1.3.2.5.1:O23	□ Yes □ No
S1.3.2.5.1.3.	Maximum number of rectangularRegions supported	6.4.17, 6.4.20	S1.3.2.5.1.2 8:M > 8:O	Enter number: ( )
S1.3.2.5.1.4.	Support a polygonalRegion	6.4.17, 6.4.21	S1.3.2.5.1:O23	□ Yes □ No
S1.3.2.5.1.5.	Maximum number of points in a polygonalRegion	6.4.17, 6.4.21	S1.3.2.5.1.4 8:M > 8:O	Enter number: ( )
S1.3.2.5.1.6.	Support identifiedRegion	6.4.17, 6.4.22	S1.3.2.5.1 8:M > 8:O	Enter number: ( )
S1.3.2.5.1.6.1.	Maximum number of identifiedRegions supported	6.4.17, 6.4.22	S1.3.2.5.1.6: 8:M > 8:O	Enter number: ( )
S1.3.2.5.1.6.2.	Support IdentifiedRegion of type CountryOnly	6.4.22, 6.4.23	S1.3.2.5.1.6:O24	□ Yes □ No
S1.3.2.5.1.6.3.	Support IdentifiedRegion of type CountryAndRegions	6.4.22, 6.4.24	S1.3.2.5.1.6:O24	□ Yes □ No
S1.3.2.5.1.6.4.	Support IdentifiedRegion of type CountryAndSubregions	6.4.22, 6.4.25	S1.3.2.5.1.6:O24	□ Yes □ No
S1.3.2.5.1.6.5.	List of supported IdentifiedRegions and the accuracy of each	5.2.4.4, 6.4.22	S1.2.2.5.1.4:M	Provide as Additional Information
S1.3.2.5.2.	Reject data if the certificate does not have the proper appPermissions	6.4.8, 6.4.28	S1.3.2.5:M	□ Yes □ No
S1.3.2.5.3.	Maximum number of PsidSsp in the appPermissions sequence	6.4.8, 6.4.28	S1.3.2.5 8:O > 8:O	Enter number: ( )
S1.3.2.5.4.	Determine that the assuranceLevel is an acceptable level	6.4.8, 6.4.27	S1.3.2.5:O	□ Yes □ No
S1.3.2.5.5.	Maximum supported length of the full chain (receiving)	5.1.2.2	S1.2.2.5: 2:M >2:O	Enter number: ( )
S1.3.2.6.	Support verifying SPDUs signed with explicit authorization certificates	6.4.5	S1.3.2:O25	□ Yes □ No

Item	Security configuration (top-level)	Reference	Status	Support
S1.3.2.7.	Support verifying SPDUs signed with implicit authorization certificates	5.3.2, 6.4.5	S1.3.2:O25	□ Yes □ No
S1.3.2.8.	Support explicit certificate authority (CA) certificates	6.4.2, 6.4.6	S1.3.2:M	□ Yes □ No
S1.3.2.9.	Support receiving implicit CA certificates	6.4.2, 6.4.5	S1.3.2:O	□ Yes □ No
S1.3.2.10.	`SignedData` verification fails in the following circumstances:	6.3.4	S1.3.2:M	□ Yes □ No
S1.3.2.10.1.	… SPDU-Parsing: Invalid Input	6.3.4	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.2.	… SPDU-Parsing: Unsupported critical information field	6	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.3.	… SPDU-Parsing: Certificate not found	4.3, 6.3.13, 6.3.14, 6.3.15	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.4.	… SPDU-Parsing:Generation time not available	4.3, 6.3.13, 6.3.14, 6.3.15	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.5.	… SPDU-Parsing:Generation location not available	4.3, 6.3.13, 6.3.14, 6.3.15	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.6.	… SPDU-Certificate-Chain: Not enough information to construct chain	5.1.2	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.7.	… SPDU-Certificate-Chain: Chain ended at untrusted root	5.1.2	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.8.	… SPDU-Certificate-Chain: Chain was too long for implementation	5.1.2	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.9.	… SPDU-Certificate-Chain: Certificate revoked	5.1.2	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.10.	… SPDU-Certificate-Chain: Expired CRL	5.1.2	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.11.	… SPDU-Certificate-Chain: Inconsistent expiry times	5.1.2	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.12.	… SPDU-Certificate-Chain: Inconsistent start times	5.1.2	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.13.	… SPDU-Certificate-Chain: Inconsistent chain permissions	5.1.2	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.14.	… SPDU-Crypto: Verification failure	5.3.1	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.15.	… SPDU-Consistency: Future certificate at generation time	5.2.4	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.16.	… SPDU-Consistency: Expired certificate at generation time	5.2.4	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.17.	… SPDU-Consistency: Expiry date too early	5.2.4	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.18.	… SPDU-Consistency: Expiry date too late	5.2.4	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.19.	… SPDU-Consistency: Generation location outside validity region	5.2.4	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.20.	… SPDU-Consistency: Unauthorized PSID	5.2.4	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.21.	… SPDU-Internal-Consistency: Expiry time before generation time	6.4.8, 6.4.14, 5.2.4	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.22.	… SPDU-Internal-Consistency: extDataHash does not match	5.2.4	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.23.	… SPDU-Local-Consistency: PSIDs do not match	5.2.4	S1.3.2.10:O	□ Yes □ No
S1.3.2.10.24.	… SPDU-Local-Consistency: Chain was too long for SDEE	5.2.4	S1.3.2.10:M	□ Yes □ No
S1.3.2.10.25.	… SPDU-Relevance: SPDU Too Old	5.2.5	S1.3.2.10:O	□ Yes □ No
S1.3.2.10.26.	… SPDU-Relevance: Future SPDU	5.2.5	S1.3.2.10:O	□ Yes □ No
S1.3.2.10.27.	… SPDU-Relevance: Expired SPDU	5.2.5	S1.3.2.10:O	□ Yes □ No
S1.3.2.10.28.	**… SPDU-Relevance: SPDU Too Distant**	5.2.5	S1.3.2.10:O	□ Yes □ No
S1.3.2.10.29.	… SPDU-Relevance: Replayed SPDU	5.2.5	S1.3.2.10:O	□ Yes □ No
S1.3.3.	Decrypt `Ieee1609Dot2Data` containing `EncryptedData`	4.2.2.3.3, 5.3.5, 6.3.33	S1.3:O17	□ Yes □ No
S1.3.3.1.	Generate ECIES keypairs using a high-quality random number generator	5.3.4, 5.3.5, 5.3.6	S1.3.3: M	□ Yes □ No

Item	Security configuration (top-level)	Reference	Status	Support
S1.3.3.2.	Maximum number of RecipientInfos supported in an incoming `EncryptedData`	6.3.33	S1.3.3: 8:M > 8:O	Enter number: ( )
S1.3.3.2.1.	Containing pskRecipientInfo	6.3.34, 6.3.37	S1.3.3.2:O26	□ Yes □ No
S1.3.3.2.2.	Containing symmRecipientInfo	6.3.34	S1.3.3.2:O26	□ Yes □ No
S1.3.3.2.3.	Containing certRecipientInfo	6.3.34	S1.3.3.2:O26	□ Yes □ No
S1.3.3.2.4.	Containing signedDataRecipientInfo	6.3.34	S1.3.3.2:O26	□ Yes □ No
S1.3.3.2.5.	Containing rekRecipientInfo	6.3.34	S1.3.3.2:O26	□ Yes □ No
S1.3.3.3.	Support decrypting using a public-key algorithm	5.3.5	S1.3.3.2.3 OR S1.3.3.2.4 OR S1.3.3.2.5:M	□ Yes □ No
S1.3.3.3.1.	… using ECIES-256	5.3.5	S1.3.3.3:M	□ Yes □ No
S1.3.3.3.1.1.	… … using NIST p256	5.3.5	S1.3.3.3:O28	□ Yes □ No
S1.3.3.3.1.2.	… … using Brainpool p256r1	5.3.5	S1.3.3.3:O28	□ Yes □ No
S1.3.3.3.2.	… using a different algorithm introduced at a later date	6.3.40	S1.3.3.3:O	□ Yes □ No
S1.3.3.4.	Support decrypting using a symmetric algorithm	6.3.41	S1.3.3:M	□ Yes □ No
S1.3.3.4.1.	... using AES-128	6.3.41	S1.3.3.4:M	□ Yes □ No
S1.3.3.4.2.	… using a different algorithm introduced at a later date	6.3.37	S1.3.3.4:O	□ Yes □ No
S1.3.3.4.3.R	Return ephemeral key when decrypting	5.3.4	S1.3.3:O	□ Yes □ No

A.7 ETSI TS 103 097 PICS pro forma

This clause contains statements for requirements defined in ETSI TS 103 097 [1]. Some of these PICS can override the PICS described in Annex A of IEEE Std 1609.2 [2].

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

Table A.7.1: Security profile for CAMs

Item	Is the IUT implemented to support:	Reference	Override	Status	Support
1	Secured CA messages	7.1.1		O	□ Yes □ No
2	Inline P2PCD operations for AT certificates	7.1.1 [2], 8.2.5.1.2, 8.2.5.2.3	[2], S3.6	A.7.1/1:M	□ Yes □ No
3	Inline P2PCD operations for AA certificates	7.1.1 [2], 8.2.5.1.2, 8.2.5.2.3	[2], S3.6	A.7.1/1:M	□ Yes □ No
4	Support a signer identifier of type digest	7.1.1	[2], S1.2.2.3.1	A.7.1/1:M	□ Yes □ No
5	Support a signer identifier of type certificate	7.1.1	[2], S1.2.2.3.2	A.7.1/1:M	□ Yes □ No

Table A.7.2: Security profile for DENMs

Item	Is the IUT implemented to support:	Reference	Override	Status	Support
1	Secured DEN messages	7.1.2		A.7.1/1:O	□ Yes □ No
4	Support a signer identifier of type certificate	7.1.2	[2], S1.2.2.3.2	A.7.1/1:M	□ Yes □ No

Table A.7.3: Security profile for other messages

Item	Is the IUT implemented to support:	Reference	Status	Support
1	Secured other messages	7.1.3	A.7.1/1:O	□ Yes □ No

Table A.7.4: 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	A.7.1/1:M	Enter value ( )

Table A.7.5: Certificate management

Item	Is the IUT implemented to support:	Reference	Status	Support
1	Loading of custom certificates	6	O	□ Yes □ No
2	Support of implicit certificates	5.3.2 [2]	O	□ Yes □ No

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
V1.5.1	January 2022	Publication
V1.5.2	July 2022	Publication
V2.1.1	August 2024	Publication