# ETSI TS 103 096-1 V1.1.1 (2013-07)


**Intelligent Transport Systems (ITS);**
**Testing;**
**Conformance test specification for TS 102 867 and TS 102 941;**
**Part 1: Protocol Implementation Conformance Statement (PICS)**

Reference
DTS/ITS-0050021

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***

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the 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
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

***Copyright Notification***

# Contents

# 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:

**TS 103 096-1: "Protocol Implementation Conformance Statement (PICS)";**

TS 103 096-2: "Test Suite Structure and Test Purposes (TSS&TP)";

TS 103 096-3: "Abstract Test Suite (ATS) and Protocol Implementation eXtra Information for Testing (PIXIT)";

TR 103 096-4: "Validation report".

# Introduction

To evaluate protocol conformance of a particular implementation, it is necessary to have a statement of which capabilities and options have been implemented for a telecommunication specification. Such a statement is called a Protocol Implementation Conformance Statement (PICS).

# 1 Scope

The present document provides the Protocol Implementation Conformance Statement (PICS) proforma for the test specifications for security algorithms as specified in TS 102 867 [1] and TS 102 941 [2] and in compliance with the relevant requirements and in accordance with the relevant guidance given in ISO/IEC 9646-7 [4] and ETS 300 406 [5].

The supplier of a protocol implementation which is claimed to conform to TS 102 867 [1] and TS 102 941 [2] is required to complete a copy of the PICS proforma provided in annex A of the present document and is required to provide the information necessary to identify both the supplier and the implementation.

# 2 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.

## 2.1 Normative references

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

[1] ETSI TS 102 867: "Intelligent Transport Systems (ITS); Security; Stage 3 mapping for IEEE 1609.2".

[2] ETSI TS 102 941: "Intelligent Transport Systems (ITS); Security; Trust and Privacy Management".

[3] ISO/IEC 9646-1: "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 1: General concepts".

[4] ISO/IEC 9646-7: "Information technology -- Open Systems Interconnection -- Conformance testing methodology and framework -- Part 7: Implementation Conformance Statements".

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

[6] IEEE P1609.2/D12 (January 2012): "IEEE Draft Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages".

NOTE: Available from http://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?reload=true&punumber=6140528.

## 2.2 Informative references

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 TS 102 867 [1], TS 102 941 [2] and the following apply:

**PICS proforma:** document, in the form of a questionnaire, designed by the protocol specifier or conformance test suite specifier, which, when completed for an OSI implementation or system, becomes the PICS

NOTE: See ISO/IEC 9646-1 [3].

**Protocol Implementation Conformance Statement (PICS):** statement made by the supplier of an Open Systems Interconnection (OSI) implementation or system, stating which capabilities have been implemented for a given OSI protocol

NOTE: See ISO/IEC 9646-1 [3].

**static conformance review:** review of the extent to which the static conformance requirements are met by the IUT, accomplished by comparing the PICS with the static conformance requirements expressed in the relevant standard(s)

NOTE: See ISO/IEC 9646-1 [3].

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in TS 102 867 [1], TS 102 941 [2] and the following apply:

| | |
|---|---|
| PICS | Protocol Implementation Conformance Statement |

# 4 Conformance

A PICS proforma which conforms to this PICS proforma 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 this PICS proforma specification shall:

a) describe an implementation which claims to conform to TS 102 867 [1] and TS 102 941 [2];

b) be a conforming ICS proforma which has been completed in accordance with the instructions for completion given in clause A.1;

c) include the information necessary to uniquely identify both the supplier and the implementation.

# Annex A (normative): PICS proforma



## A.1 Guidance for completing the ICS proforma

### A.1.1 Purposes and structure

The purpose of this PICS proforma 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 proforma is subdivided into clauses for the following categories of information:

- instructions for completing the PICS proforma;
- identification of the implementation;
- identification of the protocol;
- PICS proforma tables (for example: major capabilities, etc.).

### A.1.2 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.

As a consequence, PDU parameter tables in this annex are not the same as the tables describing the syntax of a PDU in the reference specification.

The PICS proforma contained in this annex is comprised of information in tabular form in accordance with the guidelines presented in ISO/IEC 9646-7 [4].

#### 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 [6], 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 an 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 an 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 [4], 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 proforma 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.5/4 is the reference to the answer of item 4 in table A.5.

## A.1.3 Instructions for completing the PICS proforma

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

## A.2 Identification of the Equipment

Identification of the Equipment should 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 should both be filled in if they are different.

A person who can answer queries regarding information supplied in the PICS should be named as the contact person.

### A.2.1 Date of the statement

.....

### A.2.2 Equipment Under Test identification

Name:

.....

.....

Hardware configuration:

.....

.....

.....

Software configuration:

.....

.....

.....

### A.2.3 Product supplier

Name:

.....

Address:

.....

.....

.....

Telephone number:

.....

Facsimile number:

.....

E-mail address:

.....

Additional information:

.....

.....

.....

### A.2.4 Client

Name:

.....

Address:

.....

.....

.....

Telephone number:

.....

Facsimile number:

.....

E-mail address:

.....

Additional information:

.....

.....

.....

### A.2.5 PICS contact person

Name:

.....

Telephone number:

.....

Facsimile number:

.....

E-mail address:

.....

Additional information:

.....

.....

# A.3 Identification of the protocol

This PICS proforma applies to the following specifications:

TS 102 867 [1] and TS 102 941 [2].

# A.4 Global statement of conformance

The implementation described in this PICS meets all the mandatory requirements of the referenced standards?

**[ ] Yes**

**[ ] No**

NOTE: Answering "No" to this question indicates non-conformance to the protocol specification. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming. Explanations may be entered in the comments field at the bottom of each table or on attached pages.

# A.5 PICS proforma tables

**Table A.2: Main statement**

| Item | Is the IUT implemented to support: | Reference | Status | Support |
|---|---|---|---|---|
| 1 | Support 1609.2 | - | m | □Yes □No |

**Table A.3: Top level procedures**

| **Prerequisite:** A.2/1 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | Generate Secure Data | 4.3.1, 5.5, 7.2.13, 7.2.15 | m | □Yes □No |
| 2 | Receive secure data | 7.2.17, 7.2.19 | m | □Yes □No |
| 3 | Signed WSA | 7.3.2, 7.3.4 | m | □Yes □No |
| 4 | Certificate management | 7.2.23 | m | □Yes □No |

## A.5.1 Generate Secure Data

NOTE: It is assumed that if a device indicates support for a certain public key type, then it supports it for any targets (e.g. cert management, certificates, and application messages).

**Table A.4: Generate Secure Data procedures**

| **Prerequisite:** A.3/1 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | Create 1609Dot2Data containing valid SignedData | 4.3.1, 5.5, 7.2.13 | o.401 | □Yes □No |
| 2 | Create 1609Dot2Data containing EncryptedData | 7.2.15 | o.401 | □Yes □No |
| o.401: At least one of these procedures shall be supported. | | | | |

### A.5.1.1 SignedData procedures

**Table A.5: Generate Secure Data: 1609Dot2Data containing valid SignedData procedures**

| **Prerequisite:** A.4/1 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | valid SignedData with internal payload | 7.2.13 | o.501 | □Yes □No |
| 2 | valid SignedData with external payload | 7.2.13 | o.501 | □Yes □No |
| 3 | valid SignedData with partial payload | 7.2.13 | o.501 | □Yes □No |
| 4 | Ensure that certificate used to sign data is valid | 5.5 | o | □Yes □No |
| 5 | Ensure that key and certificate used to sign are a valid pair | 5.8.4 | m | □Yes □No |
| 6 | Use certificates of type anonymous | 7.2.13 | o.502 | □Yes □No |
| 7 | Use certificates of type identified | 7.2.13 | o.502 | □Yes □No |
| 8 | Use certificates of type identified not localized | 7.2.13 | o.502 | □Yes □No |
| 9 | Include generation time in security headers | 7.2.13 | o | □Yes □No |
| 10 | Include generation location in security headers | 7.2.13 | o | □Yes □No |
| 11 | Include expiry time in security headers | 7.2.13 | o | □Yes □No |
| 12 | Support use of SignerIdentifierType certificate_chain | 7.2.13 | m | □Yes □No |
| 13 | Support use of SignerIdentifierType certificate | 7.2.13 | o | □Yes □No |
| 14 | Support use of SignerIdentifierType certificate_digest | 7.2.13 | o | □Yes □No |
| 15 | Sign with ECDSA-224 | 7.2.13 | o.503 | □Yes □No |
| 16 | Sign with ECDSA-256 | 7.2.13 | o.503 | □Yes □No |
| 17 | Support signing with explicit certificates | 7.2.13 | o.504 | □Yes □No |
| 18 | Support signing with implicit certificates | 7.2.13 | o.504 | □Yes □No |
| 19 | Support signing with uncompressed points | 7.2.13 | o.505 | □Yes □No |
| 20 | Support signing with compressed points | 7.2.13 | o.505 | □Yes □No |
| 21 | Support signing with compressed fast verification information | 7.2.13 | o | □Yes □No |
| 22 | Support signing with uncompressed fast verification information | 7.2.13 | o | □Yes □No |
| o.501: At least one of these procedures shall be supported.<br>o.502: At least one of these procedures shall be supported.<br>o.503: At least one of these procedures shall be supported.<br>o.504: At least one of these procedures shall be supported.<br>o.505: At least one of these procedures shall be supported. | | | | |

**Table A.6: Certificate procedures**

| **Prerequisite:** A.5/4 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | Support signing with certificates containing start validity | 7.2.13, 7.5.1 | o | □Yes □No |
| 2 | Support signing with certificates containing lifetime as duration | 7.2.13, 7.5.1 | o | □Yes □No |
| 3 | Create Permissions_list field of a signing certificate. | 7.2.13, 7.5.1 | m | □Yes □No |
| 4 | Sign with certificate containing circular GeographicRegion | 7.2.13, 7.5.1 | o | □Yes □No |
| 5 | Sign with certificate containing rectangular GeographicRegion | 7.2.13, 7.5.1 | o | □Yes □No |
| 6 | Sign with certificate containing polygonal GeographicRegion | 7.2.13, 7.5.1 | o | □Yes □No |

**Table A.7: Certificate chain sub table**

| **Prerequisite:** A.5/12 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of certificates included in certificate chain Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 2 | 5.3.2, 7.8.2 | m | □Yes □No |
| 2 | > 2 | 5.3.2, 7.8.2 | o | □Yes □No |

**Table A.8: Permission List sub table**

| **Prerequisite: :** A.6/3 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of entries in permissions_list Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 8 | 7.2.19, 7.5.1 | m | □Yes □No |
| 2 | > 8 | 7.2.19, 7.5.1 | o | □Yes □No |

**Table A.9: Rectangular GeographicRegion sub table**

| **Prerequisite: :** A.6/5 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of RectangularRegions Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 6 | 6.3.13, 7.2.23 | m | □Yes □No |
| 2 | > 6 | 6.3.13, 7.2.23 | o | □Yes □No |

**Table A.10: Polygonal GeographicRegion sub table**

| **Prerequisite:** A.6/6 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of PolygonalRegion vertices Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 3 to 12 | 6.3.17, 7.2.13, 7.5.1 | m | □Yes □No |
| 2 | > 12 | 6.3.17, 7.2.13, 7.5.1 | o | □Yes □No |

## A.5.1.2 EncryptedData procedures

**Table A.11: Generate Secure Data:1609Dot2Data containing EncryptedData procedures**

| **Prerequisite:** A.4/2 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | Create EncryptedData containing SignedData | 7.2.15 | o | □Yes □No |
| 2 | Use RecipientInfos | 5.3.3, 7.2.15 | m | □Yes □No |
| 3 | Use ECIES-256 as public-key encryption algorithm | 7.2.15 | m | □Yes □No |
| 4 | Support encrypting to an encryption key included in an explicit cert | 7.2.15 | o.1101 | □Yes □No |
| 5 | Support encrypting to an encryption key included in an implicit cert | 7.2.15 | o.1101 | □Yes □No |
| 6 | Support encrypting to an uncompressed encryption key | 7.2.15 | o.1102 | □Yes □No |
| 7 | Support encrypting to a compressed encryption key | 7.2.15 | o.1102 | □Yes □No |
| 8 | Use AES-128 as symmetric encryption algorithm | 7.2.15 | m | □Yes □No |
| o.1101: At least one of these procedures shall be supported.<br>o.1102: At least one of these procedures shall be supported. | | | | |

**Table A.12: RecipientInfos sub table**

| **Prerequisite:** A.11/2 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of RecipientInfos in an EncryptedData Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 6 | 5.3.5, 7.2.17, 7.8.8 | m | □Yes □No |
| 2 | > 6 | 5.3.5, 7.2.17, 7.8.8 | o | □Yes □No |

# A.5.2 Receive Secure Data

**Table A.13: Receive Secure Data procedures**

| **Prerequisite:** A.3/2 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | Support use of Sec-SecureDataContent-Extraction.request or equivalent functionality to allow a secure communications entity to inspect the contents of data before verifying it | 7.2.17 | o | □Yes □No |
| 2 | Verify SignedData | 7.2.19 | c.1301 | □Yes □No |
| 3 | Decrypt EncryptedData | 4.3.1, 7.2.17, 7.8.8 | c.1301 | □Yes □No |
| c.1301: if A.2/1 supported then m else n/a. | | | | |

### A.5.2.1 SignedData procedures

**Table A.14: Verify SignedData procedures**

| **Prerequisite:** A.13/2 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | Verify SignedData with internal payload | 7.2.19 | m | □Yes □No |
| 2 | Verify SignedData with external payload | 7.2.19 | m | □Yes □No |
| 3 | Verify SignedData with partial payload | 7.2.19 | m | □Yes □No |
| 4 | Process certificates of type anonymous | 7.2.19 | m | □Yes □No |
| 5 | Process certificates of type identified | 7.2.19 | m | □Yes □No |
| 6 | Process certificates of type identified not localized | 7.2.19 | m | □Yes □No |
| 7 | Reject data if subject type in end-entity certificate is not anonymous or identified not localized | 7.2.19 | m | □Yes □No |
| 8 | Support use of SignerIdentifierType certificate_chain | 7.2.19 | m | □Yes □No |
| 9 | Support use of SignerIdentifierType certificate | 7.2.19 | m | □Yes □No |
| 10 | Support use of SignerIdentifierType certificate_digest | 7.2.19 | m | □Yes □No |
| 11 | Verify SignedData with ECDSA-224 | 7.2.19 | m | □Yes □No |
| 12 | Verify SignedData with ECDSA-256 | 7.2.19 | m | □Yes □No |
| 13 | Support receiving explicit end-entity certificates | 7.2.19 | m | □Yes □No |
| 14 | Support receiving implicit end-entity certificates | 7.2.19 | m | □Yes □No |
| 15 | Support explicit CA certificates | 7.2.19 | m | □Yes □No |
| 16 | Support implicit CA certificates | 7.2.19 | m | □Yes □No |
| 17 | Support receiving uncompressed points | 7.2.19 | m | □Yes □No |
| 18 | Support receiving compressed points | 7.2.19 | m | □Yes □No |
| 19 | Verifying with compressed fast verification information | 7.2.19 | m | □Yes □No |
| 20 | Verifying with uncompressed fast verification information | 7.2.19 | m | □Yes □No |
| 121 | SignedData verification fails if trust anchor is not explicit certificate | 5.5.2.1 | m | □Yes □No |
| 22 | SignedData verification fails if explicit certificate in chain is issued by implicit certificate | 5.5.2.1 | m | □Yes □No |
| 23 | SignedData verification fails if data is inconsistent with the signing certificate | 5.5.3.2 | m | □Yes □No |
| 24 | SignedData verification fails if the certificate chain is inconsistent | 5.5.3.4 | m | □Yes □No |
| 25 | Receiver may specify relevance checks to be carried out | 5.5.5 | m | □Yes □No |
| 26 | Reject data based on generation location being incompatible with certificate | 7.2.19 | m | □Yes □No |
| 27 | Verify Permissions_list field of a received certificate | 7.2.19, 7.5.1 | m | □Yes □No |
| 29 | Correctly process incoming permissions of type from_issuer | 7.2.19, 7.5.1 | m | □Yes □No |
| 29 | Extract correct Service Specific Permissions from certificate | 7.2.17.4 | m | □Yes □No |

**Table A.15: Certificate chain sub table**

| **Prerequisite:** A.14/8 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of certificates included in certificate chain<br>Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 2 | 5.3.2, 7.8.2 | m | □Yes □No |
| 2 | > 2 | 5.3.2, 7.8.2 | m | □Yes □No |

**Table A.16: Relevance procedures**

| **Prerequisite: :** A.14/25 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | Allow receiver to Check Validity Based on Generation Time | 7.2.19 | m | □Yes □No |
| 2 | Allow receiver to Check Validity Based on Generation Location | 7.2.19 | m | □Yes □No |
| 3 | Allow receiver to Check Validity Based on Expiry Time | 7.2.19 | m | □Yes □No |
| 4 | Allow receiver to reject replay | 7.2.19 | o | □Yes □No |

**Table A.17: GeographicRegion sub table**

| **Prerequisite:** A. 14/26 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | Support circular GeographicRegion in certificate | 7.2.19 | m | □Yes □No |
| 2 | Support rectangular GeographicRegion in certificate | 7.2.19 | m | □Yes □No |
| 3 | Support polygonal GeographicRegion in certificate | 7.2.19 | m | □Yes □No |
| 4 | Support at least one certificate in the chain using a GeographicRegion of type from_issuer | 7.2.19 | m | □Yes □No |

**Table A.18: Permission List sub table**

| **Prerequisite: :** A.14/27 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of entries in permissions_list Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 8 | 7.2.19, 7.5.1 | m | □Yes □No |
| 2 | > 8 | 7.2.19, 7.5.1 | m | □Yes □No |

**Table A.19: Rectangular GeographicRegion sub table**

| **Prerequisite: :** A.17/2 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of RectangularRegions Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 6 | 6.3.13, 7.2.23 | m | □Yes □No |
| 2 | > 6 | 6.3.13, 7.2.23 | m | □Yes □No |

**Table A.20: Polygonal GeographicRegion sub table**

| **Prerequisite:** A.17/3 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of PolygonalRegion vertices Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 3 to 12 | 6.3.17, 7.2.13, 7.5.1 | m | |
| 2 | > 12 | 6.3.17, 7.2.13, 7.5.1 | m | |

## A.5.2.2 EncryptedData procedures

**Table A.21: Decrypt EncryptedData procedures**

| **Prerequisite:** A.13/3 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | Receive EncryptedData containing SignedData | 7.2.17 | m | □Yes □No |
| 2 | RecipientInfos | 5.3.5, 7.2.17, 7.8.8 | m | □Yes □No |

**Table A.22: RecipientInfos**

| **Prerequisite:** A.21/2 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of RecipientInfos in an EncryptedData Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 6 | 5.3.5, 7.2.17, 7.8.8 | m | □Yes □No |
| 2 | > 6 | 5.3.5, 7.2.17, 7.8.8 | m | □Yes □No |

## A.5.3 Signed WSA tables

**Table A.23: Signed WSA procedures**

| **Prerequisite:** A.3/4 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | Issue valid signed WSA | 7.3.2 | m | □Yes □No |
| 2 | Receive Signed WSA | 7.3.4 | m | □Yes □No |

### A.5.3.1 Issue valid signed WSA

**Table A.24: Issue valid signed WSA procedures**

| **Prerequisite:** A.23/1 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | key and certificate used to sign are a valid pair | 5.6.1 | m | □Yes □No |
| 2 | Support ServiceInfos in outgoing WSA | 5.4.1, 7.3.2 | m | □Yes □No |
| 3 | Support signing with explicit certificates | 7.3.2 | m | □Yes □No |
| 4 | Support signing with uncompressed points | 7.3.2 | m | □Yes □No |
| 5 | Support signing with no fast verification information | 7.3.2 | m | □Yes □No |

**Table A.25: ServiceInfos**

| **Prerequisite:** A. 24/2 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of ServiceInfos in WSA Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 32 | 5.4.1, 7.3.2 | m | □Yes □No |
| 2 | > 32 | 5.4.1, 7.3.2 | o | □Yes □No |

### A.5.3.2 Receive valid signed WSA

**Table A.26: Receive signed WSA procedures**

| **Prerequisite:** A.23/2 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | ServiceInfos in received WSA | 5.4.2, 7.3.4 | m | □Yes □No |
| 2 | WSA verification fails if trust anchor is not explicit certificate | 5.5.2.1 | m | □Yes □No |
| 3 | WSA verification fails if explicit certificate in chain is issued by implicit certificate | 5.5.2.1 | m | □Yes □No |
| 4 | WSA verification fails if the certificate chain is inconsistent | 5.5.3.4 | m | □Yes □No |
| 5 | Verify SignedWsa with ECDSA-256 | 7.3.4 | m | □Yes □No |
| 6 | Support receiving explicit CA certificates | 7.3.47.2.19 | m | □Yes □No |
| 7 | Support receiving implicit CA certificates | 7.3.47.2.19 | m | □Yes □No |
| 8 | Support receiving implicit end-entity certificates | 7.3.4 | m | □Yes □No |
| 9 | Support receiving compressed points | 7.3.4 | m | □Yes □No |
| 10 | Support fast verification with compressed fast verification information | 7.3.4 | o | □Yes □No |
| 11 | Extract generation time from SignedWsa | 7.3.4 | m | □Yes □No |
| 12 | Extract generation location from SignedWsa | 7.3.4 | m | □Yes □No |
| 13 | Extract expiry time from SignedWsa | 7.3.4 | m | □Yes □No |
| 14 | Support use of SignerIdentifierType certificate_chain | 7.3.4 | m | □Yes □No |
| 15 | Reject Signed WSA if subject type in end-entity certificate is not WSA | 7.3.4 | m | □Yes □No |
| 16 | Reject WSA based on generation location being incompatible with certificate | 7.3.4 | m | □Yes □No |
| 17 | Reject WSA if a priority for a secured service in the WSA is greater than the priority allowed for that service in the certificate | 7.3.47.2.19 | m | □Yes □No |
| 18 | Permissions_list field of a received certificate | 7.3.4, 7.5.17.2.19 | m | □Yes □No |
| 19 | Correctly process incoming permissions of type from_issuer | 7.3.4, 7.5.17.2.19 | m | □Yes □No |

| **Prerequisite:** A.23/2 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 20 | Extract correct Service Specific Permissions from end-entity certificate | 7.3.4, 7.5.17.2.19 | m | □Yes □No |
| 21 | Correctly process a WSA with some unsecured elements and some secured elements | 7.3.47.2.19 | m | □Yes □No |

**Table A.27: ServiceInfos**

| **Prerequisite:** A.26/1 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of ServiceInfos in WSA Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 32 | 5.4.1, 7.3.2 | m | □Yes □No |
| 2 | > 32 | 5.4.1, 7.3.2 | m | □Yes □No |

**Table A.28: Certificate chain sub table**

| **Prerequisite:** A.26/14 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of certificates included in certificate chain Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 2 | 5.3.2, 7.8.2 | m | □Yes □No |
| 2 | > 2 | 5.3.2, 7.8.2 | m | □Yes □No |

**Table A.29: Reject WSA procedures**

| **Prerequisite:** A.26/16 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | Circular GeographicRegion in certificate | 7.3.47.2.19 | m | □Yes □No |
| 2 | Rectangular GeographicRegion in certificate | 7.3.4 | m | □Yes □No |
| 3 | Polygonal GeographicRegion in certificate | 7.3.47.2.19 | m | □Yes □No |
| 4 | At least one certificate in the chain use a GeographicRegion of type from_issuer | 7.3.47.2.19 | m | □Yes □No |

**Table A.30: Permission List sub table**

| **Prerequisite: :** A.26/18 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of entries in permissions_list Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 8 | 7.2.19, 7.5.1 | m | □Yes □No |
| 2 | > 8 | 7.2.19, 7.5.1 | m | □Yes □No |

**Table A.31: Rectangular GeographicRegion sub table**

| **Prerequisite: :** A.29/2 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of RectangularRegions Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 6 | 6.3.13, 7.2.23 | m | □Yes □No |
| 2 | > 6 | 6.3.13, 7.2.23 | m | □Yes □No |

**Table A.32: Polygonal GeographicRegion sub table**

| **Prerequisite:** A.29/3 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of PolygonalRegion vertices Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 3 to 12 | 6.3.17, 7.2.13, 7.5.1 | m | □Yes □No |
| 2 | > 12 | 6.3.17, 7.2.13, 7.5.1 | m | □Yes □No |

## A.5.4 Certificate management

**Table A.33: Certificate management procedures**

| **Prerequisite:** A.3/5 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | Generate certificate request/response | 7.2.23 | o | □Yes □No |
| 2 | Decrypt certificate request/response | 7.2.25 | m | □Yes □No |
| 3 | Parse certificate request/response | 7.8.10 | m | □Yes □No |
| 4 | Receive CRL | 5.6.4.1 | o | □Yes □No |
| 5 | Verify CRL | 5.6.4.2 | o | □Yes □No |

### A.5.4.1 Generate certificate request/certificate response

**Table A.34: Generate certificate request/response procedures**

| **Prerequisite:** A.33/1 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | key and public key or certificate used to sign are a valid pair | 5.6.1 | m | □Yes □No |
| 2 | Certificate request is self-signed | 5.6.1.1, 7.2.23 | o.3401 | □Yes □No |
| 3 | Certificate request signed by CSR certificate | 5.6.1.1, 7.2.23 | o.3401 | □Yes □No |
| 4 | Certificate request of type anonymous | 7.2.23 | o.3402 | □Yes □No |
| 5 | Certificate request of type identified | 7.2.23 | o.3402 | □Yes □No |
| 6 | Certificate request of type identified not localized | 7.2.23 | o.3402 | □Yes □No |
| 7 | Certificate request of type WSA signer | 7.2.23 | o.3402 | □Yes □No |
| 8 | Certificate request of type Secure Data Exchange CSR | 7.2.23 | o.3402 | □Yes □No |
| 9 | Certificate request of type WSA CSR | 7.2.23 | o.3402 | □Yes □No |
| 10 | Request explicit certificate | 7.2.23 | o.3403 | □Yes □No |
| 11 | Request implicit certificate | 7.2.23 | o.3403 | □Yes □No |
| 12 | Permissions Array | 7.2.23 | m | □Yes □No |
| 13 | Support circular GeographicRegion | 7.2.23 | o.3404 | □Yes □No |
| 14 | Support rectangular GeographicRegion | 7.2.23 | o.3404 | □Yes □No |
| 15 | Support polygonal GeographicRegion | 7.2.19 | o.3404 | □Yes □No |
| 16 | Include start validity | 7.2.23 | o | □Yes □No |
| 17 | Include lifetime as duration | 7.2.23 | o | □Yes □No |
| 18 | Include expiration | 7.2.23 | m | □Yes □No |
| 19 | Verification public key is ECDSA-224 | 7.2.23 | o.3405 | □Yes □No |
| 20 | Verification public key is ECDSA-256 | 7.2.23 | o.3405 | □Yes □No |
| 21 | Include encryption key | 7.2.23 | o | □Yes □No |
| 22 | Response encryption key is ECIES-256 | 7.2.23 | m | □Yes □No |
| 23 | Encrypt request to explicit CA certificate | 7.2.19 | o.3406 | □Yes □No |
| 24 | Encrypt request to implicit CA certificate | 7.2.19 | o.3406 | □Yes □No |
| o.3401: At least one of these procedures shall be supported.<br>o.3402: At least one of these procedures shall be supported.<br>o.3403: At least one of these procedures shall be supported.<br>o.3404: At least one of these procedures shall be supported.<br>o.3405: At least one of these procedures shall be supported.<br>o.3406: At least one of these procedures shall be supported. | | | | |

**Table A.35: Self signed certificate procedures**

| **Prerequisite:** A.34/2 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | public key in self-signed certificate request matches private key that signed it | 5.8.4 | m | □Yes □No |

**Table A.36: CSR certificate procedures**

| **Prerequisite:** A.34/3 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | certificate request is consistent with CSR certificate that signed it | 5.6.1.2, 7.2.23 | m | □Yes □No |
| 2 | Sign with implicit CSR certificate | 7.2.23 | o.3601 | □Yes □No |
| 3 | Sign with explicit CSR certificate | 7.2.23 | o.3601 | □Yes □No |
| o.3601: At least one of these procedures shall be supported. | | | | |

**Table A.37: *Permissions Array***

| **Prerequisite:** A.34/12 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of entries in *Permissions Array* Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 32 | 7.2.23 | m | □Yes □No |
| 2 | > 32 | 7.2.23 | o | □Yes □No |

**Table A.38: Rectangular GeographicRegion sub table**

| **Prerequisite: :** A.34/14 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of RectangularRegions Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 6 | 6.3.13, 7.2.23 | m | □Yes □No |
| 2 | > 6 | 6.3.13, 7.2.23 | o | □Yes □No |

**Table A.39: Polygonal GeographicRegion sub table**

| **Prerequisite:** A.34/15 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of PolygonalRegion vertices Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 3 to 12 | 6.3.17, 7.2.13, 7.5.1 | m | □Yes □No |
| 2 | >12 | 6.3.17, 7.2.13, 7.5.1 | o | □Yes □No |

**Table A.40: ECIES-256 procedures**

| **Prerequisite:** A.34/21 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | Encryption public key is ECIES-256 | 7.2.23 | m | □Yes □No |

## A.5.4.2 Parse certificate request/certificateresponse

**Table A.41: Parse certificate request/response procedures**

| **Prerequisite:** A.33/3 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | Accept response with certificate permissions not identical to permissions in corresponding request | 5.6.2.2 | m | □Yes □No |
| 2 | Reject response if any CRL is not valid | 5.6.4.2 | m | □Yes □No |
| 3 | Store CRLs that were included in response | 7.8.10 | m | □Yes □No |
| 4 | Response verification fails if trust anchor is not explicit certificate | 5.5.2.1, 7.8.10 | m | □Yes □No |
| 5 | Reponses verification fails if explicit certificate in chain is issued by implicit certificate | 5.5.2.1, 7.8.10 | m | □Yes □No |
| 6 | Response verification fails if the certificate chain is inconsistent | 5.5.3.4, 7.8.10 | m | □Yes □No |
| 7 | Response verification fails if explicit certificates in chain do not verify with the issuing CA's public key | 5.5.3.4, 7.8.10 | m | □Yes □No |
| 8 | Reject response if certificate does not match private key | 7.2.9 | m | □Yes □No |
| 9 | Accept certificate that includes start validity | 5.6.2.2, 6.3.2 | m | □Yes □No |
| 10 | Accept certificate that includes lifetime as duration | 5.6.2.2, 6.3.2 | m | □Yes □No |
| 11 | Accept certificate with ECDSA-224 verification public key | 5.6.2.2, 6.3.2 | m | □Yes □No |
| 12 | Accept certificate with ECDSA-256 verification public key | 5.6.2.2, 6.3.2 | m | □Yes □No |
| 13 | Accept certificate including encryption key | 5.6.2.2, 6.3.2 | m | □Yes □No |
| 14 | Support receiving uncompressed points | 5.6.2.2, 6.3.2 | m | □Yes □No |
| 15 | Support receiving compressed points | 5.6.2.2, 6.3.2 | m | □Yes □No |
| 16 | Support fast verification with compressed fast verification information | 5.6.2.2, 6.3.2 | m | □Yes □No |
| 17 | Support fast verification with uncompressed fast verification information | 5.6.2.2, 6.3.2 | m | □Yes □No |
| 18 | Permissions_list field. | 7.5.1 | m | □Yes □No |
| 19 | Accept certificates with permissions of type from_issuer | 7.5.1 | m | □Yes □No |

**Table A.42: ECIES-256 procedures**

| **Prerequisite:** A.41/13 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | Encryption public key is ECIES-256 | 7.2.23 | m | □Yes □No |

**Table A.43: Certificate chain**

| **Prerequisite:** A.41/17 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of certificates included in certificate chain Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 2 | 5.3.2, 7.8.2 | m | □Yes □No |
| 2 | > 2 | 5.3.2, 7.8.2 | m | □Yes □No |

**Table A.44: Regions in Certificate chain**

| **Prerequisite:** A.41/17 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | Circular GeographicRegion in certificate | 7.3.47.2.19 | m | □Yes □No |
| 2 | Rectangular GeographicRegion in certificate | 7.3.4 | m | □Yes □No |
| 3 | Polygonal GeographicRegion in certificate | 7.3.47.2.19 | m | □Yes □No |

**Table A.45: Permission List sub table**

| **Prerequisite: :** A.41/18 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of entries in permissions_list Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 8 | 7.2.19, 7.5.1 | m | □Yes □No |
| 2 | > 8 | 7.2.19, 7.5.1 | m | □Yes □No |

**Table A.46: Rectangular GeographicRegion sub table**

| **Prerequisite: :** A.43/2 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of RectangularRegions Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 6 | 6.3.13, 7.2.23 | m | □Yes □No |
| 2 | > 6 | 6.3.13, 7.2.23 | m | □Yes □No |

**Table A.47: Polygonal GeographicRegion sub table**

| **Prerequisite:** A.43/3 | | | | |
|---|---|---|---|---|
| **Item** | **Maximum number of PolygonalRegion vertices Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | = 3 to 12 | 6.3.17, 7.2.13, 7.5.1 | m | □Yes □No |
| 2 | > 12 | 6.3.17, 7.2.13, 7.5.1 | m | □Yes □No |

### A.5.4.3 Verify CRL

**Table A.48: Verify CRL procedures**

| **Prerequisite:** A.33/7 | | | | |
|---|---|---|---|---|
| **Item** | **Is the IUT implemented to support:** | **Reference** | **Status** | **Support** |
| 1 | Reject CRL if chain cannot be constructed | 5.6.4.2 | m | □Yes □No |
| 2 | Reject CRL if chain is not consistent | 5.6.4.2 | m | □Yes □No |
| 3 | Reject CRL if certificate is not consistent with CRL | 5.6.4.2 | m | □Yes □No |
| 4 | Reject CRL if certificate or CRL signature cannot be verified | 5.6.4.2 | m | □Yes □No |

# Annex B (normative): PICS profile proforma for CAM



## B.1 Security profile identification

| | |
|---|---|
| Name | CAM |
| PSID | 16512 |

## B.2 Global statement of conformance

The implementation described in this PICS profile meets all the mandatory requirements of the referenced standards?

**[ ] Yes**

**[ ] No**

NOTE: Answering "No" to this question indicates non-conformance to the protocol specification. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming. Explanations may be entered in the comments field at the bottom of each table or on attached pages.

## B.3 PICS profile proforma tables

### B.3.1 Secure messaging (sending)

**Table B.1: Modified Table A.4: Generate Secure Data procedures**

| Item | Is the IUT implemented to support: | Reference | Status | Support |
|---|---|---|---|---|
| 1 | Create 1609Dot2Data containing valid SignedData | 4.3.1, 5.5, 7.2.13 | m | □Yes □No |

**Table B.2: Modified Table A.5: 1609Dot2Data containing valid SignedData procedures:**

| Item | Is the IUT implemented to support: | Reference | Status | Support |
|---|---|---|---|---|
| 1 | valid SignedData with internal payload | 7.2.13 | m | □Yes □No |
| 9 | Include generation time in security headers | 7.2.13 | x | □Yes □No |
| 10 | Include generation location in security headers | 7.2.13 | x | □Yes □No |
| 11 | Include expiry time in security headers | 7.2.13 | x | □Yes □No |
| 14 | Support use of SignerIdentifierType certificate_digest | 7.2.13 | m | □Yes □No |
| 16 | Sign with ECDSA-256 | 7.2.13 | m | □Yes □No |
| 17 | Support signing with explicit certificates | 7.2.13 | m | □Yes □No |

## B.3.2 Secure messaging (receiving)

**Table B.3: Modified Table A.13: Receive Secure Data procedures**

| Item | Is the IUT implemented to support: | Reference | Status | Support |
|---|---|---|---|---|
| 2 | Verify SignedData | 7.2.19 | m | □Yes □No |

# Annex C (normative): PICS profile proforma for DENM



## C.1 Security profile identification

| | |
|---|---|
| Name | DENM |
| PSID | 16513 |

## C.2 Global statement of conformance

The implementation described in this PICS profile meets all the mandatory requirements of the referenced standards?

**[ ] Yes**

**[ ] No**

NOTE: Answering "No" to this question indicates non-conformance to the protocol specification. Non-supported mandatory capabilities are to be identified in the PICS, with an explanation of why the implementation is non-conforming. Explanations may be entered in the comments field at the bottom of each table or on attached pages.

## C.3 PICS profile proforma tables

### C.3.1 Secure messaging (sending)

**Table C.1: Modified Table A.4: Generate Secure Data procedures**

| Item | Is the IUT implemented to support: | Reference | Status | Support |
|---|---|---|---|---|
| 1 | Create 1609Dot2Data containing valid SignedData | 4.3.1, 5.5, 7.2.13 | m | □Yes □No |

**Table C.2: Modified Table A.5: 1609Dot2Data containing valid SignedData procedures**

| Item | Is the IUT implemented to support: | Reference | Status | Support |
|---|---|---|---|---|
| 1 | valid SignedData with internal payload | 7.2.13 | m | □Yes □No |
| 9 | Include generation time in security headers | 7.2.13 | x | □Yes □No |
| 10 | Include generation location in security headers | 7.2.13 | x | □Yes □No |
| 11 | Include expiry time in security headers | 7.2.13 | x | □Yes □No |
| 14 | Support use of SignerIdentifierType certificate_digest | 7.2.13 | m | □Yes □No |
| 16 | Sign with ECDSA-256 | 7.2.13 | m | □Yes □No |
| 17 | Support signing with explicit certificates | 7.2.13 | m | □Yes □No |

## C.3.2 Secure messaging (receiving)

**Table C.3: Modified Table A.13: Receive Secure Data procedures**

| Item | Is the IUT implemented to support: | Reference | Status | Support |
|---|---|---|---|---|
| 2 | Verify SignedData | 7.2.19 | m | □Yes □No |

# History

| Document history | | |
|---|---|---|
| V1.1.1 | July 2013 | Publication |
| | | |
| | | |
| | | |
| | | |