# The ATM Forum
# Technical Committee

## Security Specification Version 1.1 Protocol Implementation Conformance Statement (PICS) Proforma Specification

**af-sec-0163.000**

**March, 2001**

## Copyright release for PICS:

The information in this publication is believed to be accurate as of its publication date. Such information is subject to change without notice and The ATM Forum is not responsible for any errors. The ATM Forum does not assume any responsibility to update or correct any information in this publication. Notwithstanding anything to the contrary, neither The ATM Forum nor the publisher make any representation or warranty, expressed or implied, concerning the completeness, accuracy, or applicability of any information contained in this publication. No liability of any kind shall be assumed by The ATM Forum or the publisher as a result of reliance upon any information contained in this publication.

The receipt or any use of this document or its contents does not in any way create by implication or otherwise:

- Any express or implied license or right to or under any ATM Forum member company's patent, copyright, trademark or trade secret rights which are or may be associated with the ideas, techniques, concepts or expressions contained herein; nor
- Any warranty or representation that any ATM Forum member companies will announce any product(s) and/or service(s) related thereto, or if such announcements are made, that such announced product(s) and/or service(s) embody any or all of the ideas, technologies, or concepts contained herein; nor
- Any form of relationship between any ATM Forum member companies and the recipient or user of this document.

Implementation or use of specific ATM standards or recommendations and ATM Forum specifications will be voluntary, and no company shall agree or be obliged to implement them by virtue of participation in The ATM Forum.

The ATM Forum is a non-profit international organization accelerating industry cooperation on ATM technology. The ATM Forum does not, expressly or otherwise, endorse or promote any specific products or services.

NOTE: The user's attention is called to the possibility that implementation of the ATM interoperability specification contained herein may require use of an invention covered by patent rights held by ATM Forum Member companies or others. By publication of this ATM interoperability specification, no position is taken by The ATM Forum with respect to validity of any patent claims or of any patent rights related thereto or the ability to obtain the license to use such rights. ATM Forum Member companies agree to grant licenses under the relevant patents they own on reasonable and nondiscriminatory terms and conditions to applicants desiring to obtain such a license. For additional information contact:

The ATM Forum
Worldwide Headquarters
1000 Executive Pkwy. #220
St. Louis, MO 63141
Tel: +1-314-205-0200
Fax: +1-314-576-7989

# Table of Contents

# 1. Introduction

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

## *1.1 Scope*

The present document provides the Protocol Implementation Conformance Statement (PICS) proforma for the Security Specification Version 1.1 defined in af-sec-0100.002 in compliance with the relevant requirements, and in accordance with the relevant guidance given in ISO/IEC 9646-7.

## *1.2 References*

[1] af-sec-0100.002: March 2001, ATM Forum, "ATM Security Specification Version 1.1".

[2] ISO/IEC 9646-1:1994, Information technology - Open systems interconnection - Conformance testing methodology and framework - Part 1: General Concepts. (See also ITU Recommendation X.290(1995)).

[3] ISO/IEC 9646-7: 1995, Information technology – Open Systemd interconnection – Conformance testing methodology and framework – Part 7: Implementation Conformance Statements (see also ITU-T Recommendation X.296 (1995)).

[4] ISO/IEC 9646-3: 1998, Information technology – Open Systems interconnection – Conformance testing methodology and framework – Part 3: The Tree a d Tabular Combined Notation (TTCN) (see also ITU-T Recommendation X.292 (1998)).

## *1.3 Definitions*

This document uses the following terms defined in ISO/IEC 9646-1[1]:

**Protocol Implementation Conformance Statement (PICS):** A statement made by the supplier of an implementation or system claimed to conform to a given specification, stating which capabilities have been implemented for a given protocol

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

## 1.4 Abbreviations:

| | |
|---|---|
| CP-AUTH | Control Plane Authentication |
| CPC | Control Plane Authentication & Integrity Capabilities |
| IUT | Implementation under test |
| MC | Major Capabilities |
| PICS | Protocol Implementation Conformance Statement |
| SME-1 | In-band security messaging |
| SME-2 | Signaling-based two-way messaging with fall-back to in-band security messaging |
| SME-3 | Signaling-based security two-way messaging for the pt-mpt ADD PARTY message |
| SUT | System under test |
| UAC | User Plane Authentication Capabilities |
| UACC | User Plane Access Control Capabilities |
| UCC | User Plane Confidentiality Capabilities |
| UIC | User Plane Data Origin Authentication & Integrity Capabilities |

## 1.5 Conformance

This PICS does not modify any of the requirements detailed in af-sec-0100.002. In case of apparent conflict between the statements in the base specification and the annotations of "M" (mandatory) and "O" (optional) in this PICS, the text of the base specification takes precedence.

For each protocol implementation for which conformance is claimed to the ATM Forum Security Specification Version 1.1, the supplier is required to complete a copy of the PICS proforma provided in this document and is required to provide the information necessary to identify both the supplier and the implementation.

# 2. Identification of the Implementation

Identification of the Implementation Under Test (IUT) and the system in which it resides (the System Under Test (SUT)) 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.

## 2.1 Date of the statement

..............................................................................................................................................

## 2.2 Implementation Under Test (IUT) identification

IUT name:

..............................................................................................................................................

..............................................................................................................................................

IUT version:

..............................................................................................................................................

## 2.3 System Under Test (SUT) identification

SUT name:

..............................................................................................................................................

..............................................................................................................................................

Hardware configuration:

..............................................................................................................................................

..............................................................................................................................................

..............................................................................................................................................

Operating system:

..............................................................................................................................................

## 2.4 Product supplier

Name:

..............................................................................................................................................

Address:

..............................................................................................................................................

..............................................................................................................................................

..............................................................................................................................................

Telephone number:

..............................................................................................................................................

Facsimile number:

..............................................................................................................................................

E-mail address:

..............................................................................................................................................

Additional information:

..............................................................................................................................................

..............................................................................................................................................

..............................................................................................................................................

## 2.5 Client (if different from product supplier)

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

## 2.6 PICS contact person

(A person to contact if there are any queries concerning the content of the PICS)
Name:
.......................................................................................................................................................
Telephone number:
.......................................................................................................................................................
Facsimile number:
.......................................................................................................................................................
E-mail address:
.......................................................................................................................................................
Additional information:
.......................................................................................................................................................
.......................................................................................................................................................
.......................................................................................................................................................

## 2.7 Identification of the Security Specification

This PICS proforma applies to the following standard:

**af-sec-0100.002 (March, 2001): "Security Specification Version 1.1".**

# 3. PICS Proforma

## *3.1 Global statement of conformance*

The implementation described in this PICS meets all of the mandatory requirements of the reference protocol.

[ ] YES
[ ] NO

Note: Answering "No" indicates non-conformance to the Security Specification Version 1.1. Non-supported mandatory capabilities are to be identified in the following tables, with an explanation by the implementor specify why the implementation is non-conforming.

## 3.2 Instructions for Completing the PICS Proforma

The supplier of the implementation shall complete the ICS proforma in each of the spaces provided. In particular, an explicit answer shall be entered, in each of the support column boxes provided, using the specified notation.

The supplier of the implementation shall fill in the support column. The following notations, defined in ISO/IEC 9646-7, are used for the support column:

Y or y supported by the implementation.
N or n not supported by the implementation.
N/A no answer required (allowed only if the status is n/a, directly or after evaluation of a conditional status).

The following notations defined in ISO/IEC 9646-7, are used for the status column:

C.n Conditional (may be selected to suit the implementation, provided that any requirements applicable to the options are observed).
M mandatory - the capability is required to be supported.
N/A not applicable - in the context, it is impossible to use the capability.
O optional - the capability may be supported or not.
O.i qualified optional - for mutually exclusive or selectable options from a set. "i" 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.
X prohibited - there is a requirement not to use the capability in the given context.

## 3.3 Major Capabilities (MC)

| Item | Does the Implementation… | Reference | Status | Conditions for Support | Support |
|---|---|---|---|---|---|
| MC1 | Supports at least one of SME Profile: (SME-1, SME-2, SME-3) | 1.6.2 | M | | SME-1: Yes__ No__<br>SME-2: Yes__ No__<br>SME-3: Yes__ No__ |
| MC2 | Support User Plane Authentication (AUTH)? | 3.1, 7.2.2.3 | O.1 | | Yes__ No__ |
| MC3 | Support User Plane Confidentiality (CONF)? | 3.1, 7.2.2.1 | O.1 | | Yes__ No__ |
| MC4 | Support User Plane Data Origin Authentication and Integrity (INTEG)? | 3.1, 7.2.2.2 | O.1 | | Yes__ No__ |
| MC5 | Support User Plane Access Control (ACC)? | 3.1, 7.2.2.6 | O.1 | | Yes__ No__ |
| MC6 | Support Control Plane Authentication and Integrity (CP-AUTH)? | 4.1 | O.1 | | Yes__ No__ |

O.1: Mandatory to support at least one of these capabilities.

## 3.4 User Plane Authentication (AUTH) Capabilities (UAC)

| Item | Does the Implementation… | Reference | Status | Conditions for Support | Support |
|---|---|---|---|---|---|
| UAC1 | Supports SME Profile 1 (SME-1)? | 1.6.2, 5.1 | C.1 | | Yes__ No__ |
| UAC2 | Supports SME Profile 2 (SME-2)? | 1.6.2, 5.1 | C.1 | | Yes__ No__ |
| UAC3 | Supports SME Profile 3 (SME-3)? | 1.6.2, 5.1 | C.1 | | Yes__ No__ |
| UAC4 | Support Security Algorithm Profile AUTH-1? | 1.6.1, 3.1, 7.2.3.7 | O.2 | | Yes__ No__ |
| UAC5 | Support Security Algorithm Profile AUTH-2? | 1.6.1, 3.1, 7.2.3.7 | O.2 | | Yes__ No__ |
| UAC6 | Support Security Algorithm Profile AUTH-3? | 1.6.1, 3.1, 7.2.3.7 | O.2 | | Yes__ No__ |
| UAC7 | Support Security Algorithm Profile AUTH-4? | 1.6.1, 3.1, 7.2.3.7 | O.2 | | Yes__ No__ |
| UAC8 | Support Security Algorithm Profile AUTH-5? | 1.6.1, 3.1, 7.2.3.7 | O.2 | | Yes__ No__ |
| UAC9 | Support Security Algorithm Profile AUTH-6? | 1.6.1, 3.1, 7.2.3.7 | O.2 | | Yes__ No__ |
| UAC10 | Support one or more User-Defined Security Algorithms? | 1.6.1, 3.1, 7.2.3.7 | O.2 | | Yes__ No__ |

C.1: IF supports UAC THEN mandatory to support at least one of these SME Profiles ELSE O.
O.2: Mandatory to support at least one of these capabilities.

## 3.5 User Plane Confidentiality (CONF) Capabilities (UCC)

| Item | Does the Implementation… | Reference | Status | Conditions for Support | Support |
|---|---|---|---|---|---|
| UCC1 | Supports SME Profile 1 (SME-1)? | 1.6.2, 5.1 | C.2 | | Yes__ No__ |
| UCC2 | Supports SME Profile 2 (SME-2)? | 1.6.2, 5.1 | C.2 | | Yes__ No__ |
| UCC3 | Supports SME Profile 3 (SME-3)? | 1.6.2, 5.1 | C.2 | | Yes__ No__ |
| UCC4 | Support Confidentiality Algorithm Profile CONF-1? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC5 | Support Confidentiality Algorithm Profile CONF-2? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC6 | Support Confidentiality Algorithm Profile CONF-3? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC7 | Support Confidentiality Algorithm Profile CONF-4? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC8 | Support Confidentiality Algorithm Profile CONF-5? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC9 | Support Confidentiality Algorithm Profile CONF-6? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC10 | Support Confidentiality Algorithm Profile CONF-7? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC11 | Support Confidentiality Algorithm Profile CONF-8? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC12 | Support Confidentiality Algorithm Profile CONF-9? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC13 | Support Confidentiality Algorithm Profile CONF-10? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC14 | Support Confidentiality Algorithm Profile CONF-11? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC15 | Support Confidentiality Algorithm Profile CONF-12? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC16 | Support Confidentiality Algorithm Profile CONF-13? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC17 | Support Confidentiality Algorithm Profile CONF-14? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC18 | Support Confidentiality Algorithm Profile CONF-15? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC19 | Support Confidentiality Algorithm Profile CONF-16? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC20 | Support Confidentiality Algorithm Profile CONF-17? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC21 | Support Confidentiality Algorithm Profile CONF-18? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC22 | Support Confidentiality Algorithm Profile CONF-19? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC23 | Support Confidentiality Algorithm Profile CONF-20? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |
| UCC24 | Support one or more User-Defined Security Algorithms? | 1.6.1, 3.2, 7.2.3.9 | O.3 | | Yes__ No__ |

C.2: IF supports UCC THEN mandatory to support at least one of these SME Profiles ELSE O.
O.3: Mandatory to support at least one of these capabilities.

## 3.6 User Plane Data Origin Authentication and Integrity (INTEG) Capabilities (UIC)

| Item | Does the Implementation… | Reference | Status | Conditions for Support | Support |
|---|---|---|---|---|---|
| UIC1 | Supports SME Profile 1 (SME-1)? | 1.6.2, 5.1 | C.3 | | Yes__ No__ |
| UIC2 | Supports SME Profile 2 (SME-2)? | 1.6.2, 5.1 | C.3 | | Yes__ No__ |
| UIC3 | Supports SME Profile 3 (SME-3)? | 1.6.2, 5.1 | C.3 | | Yes__ No__ |
| UIC4 | Support Integrity Algorithm Profile INTEG-1? | 1.6.1, 3.3, 7.2.3.8 | O.4 | | Yes__ No__ |
| UIC5 | Support Integrity Algorithm Profile INTEG-2? | 1.6.1, 3.3, 7.2.3.8 | O.4 | | Yes__ No__ |
| UIC6 | Support Integrity Algorithm Profile INTEG-3? | 1.6.1, 3.3, 7.2.3.8 | O.4 | | Yes__ No__ |
| UIC7 | Support Integrity Algorithm Profile INTEG-4? | 1.6.1, 3.3, 7.2.3.8 | O.4 | | Yes__ No__ |
| UIC8 | Support Integrity Algorithm Profile INTEG-5? | 1.6.1, 3.3, 7.2.3.8 | O.4 | | Yes__ No__ |
| UIC9 | Support Integrity Algorithm Profile INTEG-6? | 1.6.1, 3.3, 7.2.3.8 | O.4 | | Yes__ No__ |
| UIC10 | Support Integrity Algorithm Profile INTEG-7? | 1.6.1, 3.3, 7.2.3.8 | O.4 | | Yes__ No__ |
| UIC11 | Support Integrity Algorithm Profile INTEG-8? | 1.6.1, 3.3, 7.2.3.8 | O.4 | | Yes__ No__ |
| UIC12 | Support Integrity Algorithm Profile INTEG-9? | 1.6.1, 3.3, 7.2.3.8 | O.4 | | Yes__ No__ |
| UIC13 | Support Integrity Algorithm Profile INTEG-10? | 1.6.1, 3.3, 7.2.3.8 | O.4 | | Yes__ No__ |
| UIC14 | Support Integrity Algorithm Profile INTEG-11? | 1.6.1, 3.3, 7.2.3.8 | O.4 | | Yes__ No__ |
| UIC15 | Support one or more User-Defined Security Algorithm? | 1.6.1, 3.3, 7.2.3.8 | O.4 | | Yes__ No__ |
| UIC16 | Support negotiation of Integrity either with or without replay protection at set-up time? | 1.6.1, 3.3, 7.2.3.8 | O.4 | | Yes__ No__ |

C3: IF supports UIC THEN mandatory to support at least one of these SME Profiles ELSE O.
O.4: Mandatory to support at least one of these capabilities.

## 3.7 User Plane Access Control (ACC) Capabilities (UACC)

| Item | Does the Implementation… | Reference | Status | Conditions for Support | Support |
|---|---|---|---|---|---|
| UACC1 | Supports ACC Profile ACC-1? | 1.6.1, 3.4, 7.2.2.6 | M | | Yes__ No__ |

### *3.8 Control Plane Authentication and Integrity (CP-AUTH) Capabilities (CPC)*

| Item | Does the Implementation… | Reference | Status | Conditions for Support | Support |
|---|---|---|---|---|---|
| CPC1 | Supports SME Profile 1 (SME-1)? | 1.6.1, 4 | C.4 | | Yes__ No__ |
| CPC2 | Supports SME Profile 2 (SME-2)? | 1.6.1, 4 | C.4 | | Yes__ No__ |
| CPC3 | Supports SME Profile 3 (SME-3)? | 1.6.1, 4 | C.4 | | Yes__ No__ |
| CPC4 | Support Integrity Algorithm Profile INTEG-1? | 1.6.1, 4 | O.5 | | Yes__ No__ |
| CPC5 | Support Integrity Algorithm Profile INTEG-2? | 1.6.1, 4 | O.5 | | Yes__ No__ |

C.4: IF Supports CPC THEN mandatory to support at least one of these SME Profiles ELSE O.
O.5: Mandatory to support at least one of these capabilities.