INTERNATIONAL STANDARD

ISO/IEC 11586-5

First edition
1997-04-01

Information technology — Open Systems Interconnection — Generic upper layers security: Security Exchange Service Element (SESE) Protocol Implementation Conformance Statement (PICS) proforma

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Sécurité générique pour les couches hautes: Proforme de déclaration de conformité pour la mise en œuvre du protocole (PICS) de l'élément de service d'échange de sécurité (SESE)



Reference number
ISO/IEC 11586-5:1997(E)

--`,,```,,,,````-`-`,,`,,`,`,,`---

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

Contents

		Page
1	Scope	1
2	Normative references	1
	2.1 Identical Recommendations | International Standards	1
	2.2 Paired Recommendations | International Standards equivalent in technical content	1
3	Definitions	2
4	Abbreviations	2
5	Conventions	2
6	Conformance	2
Annex A – Protocol Implementation Conformance Statement (PICS) proforma for the SESE protocol		
	A.1 Notations defined for the proforma	3
	A.1.1 Status column	3
	A.1.2 Support column	3
	A.2 PICS numbers	3
	A.3 Completion of the PICS	4
	A.4 Date of statement	4
	A.5 Implementation details	4
	A.6 ITU-T Rec. X.832 | ISO/IEC 11586-3 protocol details	5
	A.6.1 ITU-T Rec. X.832 | ISO/IEC 11586-3 technical corrigenda implemented	5
	A.7 Global statement of conformance	5
	A.8 Supported APDUs	5
	A.9 Supported APDU parameters	6
	A.9.1 SE-Transfer (SETR)	6
	A.9.2 SE-U-Abort (SEAB)	6
	A.9.3 SE-P-Abort (SEPA)	6
	A.9.4 Problem codes	7
	A.10 Abstract syntax	7
	A.11 Application Context	7
	A.12 Security exchanges	7
	A.12.1 Class of Security Exchange Supported	7
	A.12.2 Exchange Supported	8
	A.12.3 Directory Authentication Exchange (one way)	8
	A.12.4 Directory Authentication Exchange (two way)	8
	A.12.5 Simple Negotiation Exchange	8

© ISO/IEC 1997

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 11586-5 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 21, *Open systems interconnection, data management and open distributed processing*, in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.834.

ISO/IEC 11586 consists of the following parts, under the general title *Information technology — Open Systems Interconnection — Generic upper layers security*:

— *Part 1: Overview, models and notation*

— *Part 2: Security Exchange Service Element (SESE) service definition*

— *Part 3: Security Exchange Service Element (SESE) protocol specification*

— *Part 4: Protecting transfer syntax specification*

— *Part 5: Security Exchange Service Element (SESE) Protocol Implementation Conformance Statement (PICS) proforma*

— *Part 6: Protecting transfer syntax Protocol Implementation Conformance Statement (PICS) Proforma*

Annex A forms an integral part of this part of ISO/IEC 11586.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Introduction

This Recommendation | International Standard forms part of a series of Recommendations | International Standards that provide generic upper layer security services. The parts are as follows:

- Part 1: Overview, Model and Notation.
- Part 2: Security Exchange Service Element Service Definition.
- Part 3: Security Exchange Service Element Protocol Specification.
- Part 4: Protecting Transfer Syntax Specification.
- Part 5: Security Exchange Service Element Service PICS Proforma.
- Part 6: Protecting Transfer Syntax PICS Proforma.

This Recommendation | International Standard constitutes Part 5 of the series.

Part 3 defines a protocol for the communication of security exchange information between open systems as part of the operation of a security mechanism. To evaluate the conformance of a particular implementation, it is necessary to have a description of the capabilities and options which have been implemented. Such a description is called a Protocol Implementation Conformance Statement (PICS). This Recommendation | International Standard includes the PICS proforma for the security exchange service element protocol specified in Part 3 and the security exchanges defined in Part 1, Annex C.

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – GENERIC UPPER LAYERS SECURITY: SECURITY EXCHANGE SERVICE ELEMENT (SESE) PROTOCOL IMPLEMENTATION CONFORMANCE STATEMENT (PICS) PROFORMA

1 Scope

This Recommendation | International Standard defines a Protocol Implementation Conformance Statement (PICS) proforma for the detailed expression of the conformance requirements of ITU-T Rec. X.832 | ISO/IEC 11586-3 and Annex C of ITU-T Rec. X.830 | ISO/IEC 11586-1. This PICS proforma is in compliance with the relevant requirements, and in accordance with the relevant guidance for a PICS proforma, given in ITU-T Rec. X.291 and ISO/IEC 9646-2. Detail of the use of this proforma is provided in this Recommendation | International Standard. Implementations claiming conformance to ITU-T Rec. X.832 | ISO/IEC 11586-3 or Annex C of ITU-T Rec. X.830 | ISO/IEC 11586-1 shall complete the proforma as part of the conformance requirements. The level of detail required in the proforma exceeds that of the protocol specification by requiring details to uniquely identify the implementation and the supplier.

NOTE – PICS are related to base Recommendations and Standards and only base Recommendations and Standards. PICS structure might be expanded and refined for other documents using the base Standards (e.g. ISPICS).

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and the parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards indicated below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.210 (1993) | ISO/IEC 10731:1994 *Information technology – Open Systems Interconnection – Basic Reference Model: Conventions for the definition of OSI services.*
- ITU-T Recommendation X.830 (1995) | ISO/IEC 11586-1:1996, *Information technology – Open Systems Interconnection – Generic upper layers security: Overview, models and notation.*
- ITU-T Recommendation X.832 (1995) | ISO/IEC 11586-3:1996, *Information technology – Open Systems Interconnection – Generic upper layers security: Security Exchange Service Element (SESE) protocol specification.*

2.2 Paired Recommendations | International Standards equivalent in technical content

- ITU-T Recommendation X.290 (1995), *OSI conformance testing methodology and framework for protocol Recommendations for ITU-T applications – General concepts.*

  ISO/IEC 9646-1:1994, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 1: General concepts.*
- ITU-T Recommendation X.291 (1995), *OSI conformance testing methodology and framework for protocol Recommendations for ITU-T applications – Abstract test suite specification.*

  ISO/IEC 9646-2:1994, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 2: Abstract Test Suite specification.*

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

3 Definitions

3.1 This Recommendation | International Standard makes use of the following terms defined in ITU-T Rec. X.290 and ISO/IEC 9646-1:

a) Protocol Implementation Conformance Statement (PICS);

b) PICS proforma;

c) Protocol Implementation eXtra Information for Testing (PIXIT).

4 Abbreviations

4.1 The following abbreviations used in this Recommendation | International Standard are defined in ITU-T Rec. X.290 and ISO/IEC 9646-1:

a) PICS;

b) PIXIT.

5 Conventions

This Recommendation | International Standard uses the descriptive conventions in the OSI Service Conventions, ITU-T Rec. X.210 | ISO/IEC 10731. The PICS proforma annex has been designed to be a self contained section of this Recommendation | International Standard, for use in testing and procurement.

6 Conformance

A conforming PICS proforma shall be technically equivalent to the ITU-T | ISO/IEC published PICS proforma and shall preserve the numbering and ordering of the items in the ITU-T | ISO/IEC PICS proforma.

A PICS which conforms to this Recommendation | International Standard shall:

a) describe an implementation which conforms to ITU-T Rec. X.832 | ISO/IEC 11586-3;

b) be a conforming PICS proforma, which has been completed in accordance with the instruction for completion given in A.1 and A.3; and

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A[1)]

Protocol Implementation Conformance Statement (PICS) proforma for the SESE protocol

(This annex forms an integral part of this Recommendation | International Standard)

A.1 Notations defined for the proforma

In order to reduce the size of tables in the PICS proforma, notations have been introduced that have allowed the use of a multi-column layout, where the columns are headed 'Status', and 'Support'. The definition of each of these follows.

A.1.1 Status column

This column indicates the level of support required for conformance to ITU-T Rec. X.832 | ISO/IEC 11586-3. The values are as follows:

M Mandatory support is required.

O Optional support is permitted for conformance to ITU-T Rec. X.832 | ISO/IEC 11586-3. If implemented, it must conform to the specifications and restrictions contained in ITU-T Rec. X.832 | ISO/IEC 11586-3. These restrictions may affect the optionality of other items.

n/a The item is not applicable.

c*n* The item is conditional (where *n* is the number which identifies the condition which is applicable). The definitions for the conditional statements used in this annex are written under the tables in which they first appear.

O.*n* The item is optional, but the optionality is qualified (where *n* is the number which identifies the qualification which is applicable). The definitions for the qualified optional statements used in this annex are written under the tables in which they first appear.

A.1.2 Support column

The 'Support' column shall be completed by the supplier or implementor to indicate the level of implementation of each feature. The proforma has been designed such that the only entries required in the 'Support' column are:

Y Yes, the feature has been implemented

N No, the feature has not been implemented

– Not applicable.

A.2 PICS numbers

Each line within the PICS proforma which requires implementation detail to be entered is numbered at the left hand edge of the line. This numbering is included as a means of uniquely identifying all possible implementation details within the PICS proforma. The need for such unique referencing has been identified by the testing bodies.

The means of referencing individual responses should be to specify the following sequence:

a) a reference to the smallest subclause enclosing the relevant item;

b) a solidus character, '/';

c) the reference number of the row in which the response appears;

d) if, and only if, more than one response occurs in the row identified by the reference number, then each possible entry is implicitly labelled a, b, c, etc., from left to right, and this letter is appended to the sequence.

---

1) **Copyright release for PICS proforma:**
Users of this Recommendation | International Standard may freely reproduce the PICS proforma in this annex so that it can be used for its intended purpose, and may further publish the completed PICS.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.3 Completion of the PICS

The implementor shall complete all entries in the column marked 'Support'. In certain clauses of the PICS proforma further guidance for completion may be necessary. Such guidance shall supplement the guidance given in this clause and shall have a scope restricted to the clause in which it appears. In addition, other specifically identified information shall be provided by the implementor where requested. No changes shall be made to the proforma except the completion as required. Recognizing that the level of detail required may, in some instances, exceed the space available for responses a number of responses specifically allow for the addition of appendices to the PICS.

A.4 Date of statement

Date of statement? (yy-mm-dd)

A.5 Implementation details

The supplier of the protocol implementation shall specify the information necessary to uniquely identify the implementation and the system in which it may reside. This may include details of:

a) supplier, implementation name, operating system, suitable hardware;

b) system supplier and/or client of the test laboratory that is to test the implementation;

c) information on whom to contact if there are queries concerning the content of the PICS; and

d) the relationship between this PICS and the System Conformance Statement for the System (see note).

NOTE – The System Conformance Statement is identified in ITU-T Rec. X.290 and ISO/IEC 9646-1. It contains a declaration of the layers of the Reference Model covered by the implementation to be tested.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.6 ITU-T Rec. X.832 | ISO/IEC 11586-3 protocol details

A.6.1 ITU-T Rec. X.832 | ISO/IEC 11586-3 technical corrigenda implemented

A.7 Global statement of conformance

Are all mandatory features implemented? (Yes or no)

NOTE – If a positive response is not given to this box, then the implementation does not conform to ITU-T Rec. X.832 | ISO/IEC 11586-3.

A.8 Supported APDUs

	APDU	Sending		Receiving		Reference	Comment
		Status	Support	Status	Support		
A.8/1	SE-TRANSFER (SETR)	M		M		Part 3 6.2	
A.8/2	SE-U-ABORT (SEAB)	M		M		Part 3 6.3	
A.8/3	SE-P-ABORT (SEPA)	M		M		Part3 6.4	

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.9 Supported APDU parameters

A.9.1 SE-Transfer (SETR)

	Parameter	Sending		Receiving	
		Status	Support	Status	Support
A.9.1/1	SE Identifier	M		M	
A.9.1/2	Item Identifier	M		M	
A.9.1/3	SE Item	M		M	
A.9.1/4	Invocation Id (specify range supported)	O range		M range	
A.9.1/5	Start Flag	M		M	
A.9.1/6	End Flag	M		M	

A.9.2 SE-U-Abort (SEAB)

	Parameter	Sending		Receiving	
		Status	Support	Status	Support
A.9.2/1	Invocation Id	c0		M	
A.9.2/2	Item Identifier	M		M	
A.9.2/3	Errors	M		M	
	c0: if A.9.1/4 supported then M else n/a				

A.9.3 SE-P-Abort (SEPA)

	Parameter	Sending		Receiving	
		Status	Support	Status	Support
A.9.3/1	Invocation Id	c0		M	
A.9.3/2	Item Identifier	M		M	
A.9.3/3	Problem Code	M		M	

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.9.4 Problem codes

	Problem code	Reference	Sending		Receiving	
			Status	Support	Status	Support
A.9.4/1	General problem codes	Part 3 6.4.1	M		M	
A.9.4/2	Transfer problem codes	Part 3 6.4.2	M		M	
A.9.4/3	Abort problem codes	Part 3 6.4.3	M		M	

A.10 Abstract syntax

What is the abstract syntax supported ? (Give object identifier)

A.11 Application Context

		Reference	Status	Support
A.11/1	Basic SESE Application Context	Part 1 Annex B	O	
A.11/2	If not give object identifier for application context supported			

A.12 Security exchanges

A.12.1 Class of Security Exchange Supported

		Reference	Status	Support
A.12.1/1	Alternating class of security exchanges	Part 1 6.1	O	
A.12.1/2	Arbitrary class of security exchange	Part 1 6.1	O	

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A.12.2 Exchange Supported

		Reference	Status	Support
A.12.2/1	Directory Authentication Exchange (one way)	Part 1 Annex C1	c1	
A.12.2/2	Directory Authentication Exchange (two way)	Part 1 Annex C2	c1	
A.12.2/3	Simple Negotiation Exchange	Part 1 Annex C3	c1	
A.12.2/4	What other security exchanges are supported (give object identifiers)			
	c1: if [A.12.1/1] then O else n/a			

A.12.3 Directory Authentication Exchange (one way)

	Security Exchange Item	Sending		Receiving	
		Status	Support	Status	Support
A.12.3/1	Directory Credentials	c2		c2	
	c2: if [A.12.2/1] then M else n/a				

A.12.4 Directory Authentication Exchange (two way)

	Security Exchange Item	Sending		Receiving	
		Status	Support	Status	Support
A.12.4/1	Initiator Credentials	c3		c3	
A.12.4/2	Responder Credentials	c3		c3	
A.12.4/3	Authentication Failure	c3		c3	
	c3: if [A.12.2/2] then M else n/a				

A.12.5 Simple Negotiation Exchange

	Security Exchange Item	Sending		Receiving	
		Status	Support	Status	Support
A.12.5/1	Offered Ids	c4		c4	
A.12.5/2	Accepted Ids	c4		c4	
	c4: if [A.12.2/3] then M else n/a				

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

© ISO/IEC

ICS 35.100.01

Descriptors: data processing, information interchange, network interconnection, open systems interconnection, communication procedure, security techniques, protocols, implementation.

Price based on 8 pages

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale