

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)*



Contents

	<i>Page</i>
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

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.

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.

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.*