
**Information technology — Open Systems
Interconnection — Generic upper layers
security: Protecting transfer syntax
specification**

*Technologies de l'information — Interconnexion de systèmes ouverts
(OSI) — Sécurité des couches supérieures génériques: Spécifications pour
la syntaxe de transfert de protection*

Contents

| | <i>Page</i> |
|---|-------------|
| 1 Scope | 1 |
| 2 Normative references | 1 |
| 2.1 Identical Recommendations International Standards | 1 |
| 3 Definitions | 2 |
| 4 Abbreviations | 2 |
| 5 General overview | 2 |
| 5.1 Model of a protecting transfer syntax | 3 |
| 5.2 Initial encoding rules | 3 |
| 5.3 Security transformation | 4 |
| 5.4 Syntax structure | 4 |
| 6 Data structures for a protecting transfer syntax | 4 |
| 7 Incorporation into underlying protocol | 5 |
| 8 Synchronization procedures | 6 |
| 9 Object identifier assignment | 6 |
| 10 Conformance | 6 |

© ISO/IEC 1996

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 11586-4 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.833.

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 Protocol Implementation Conformance Statement (PICS) proforma*
- *Part 6: Protecting transfer syntax Protocol Implementation Conformance Statement (PICS) proforma*

Introduction

This Recommendation | International Standard forms part of a series of Recommendations | International Standards, which provide(s) a set of facilities to aid the construction of Upper Layers protocols which support the provision of security services. The parts are as follows:

- Part 1: Overview, Models 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 PICS Proforma;
- Part 6: Protecting Transfer Syntax PICS Proforma.

This Recommendation | International Standard constitutes Part 3 of this series.

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – GENERIC UPPER LAYERS SECURITY: PROTECTING TRANSFER SYNTAX SPECIFICATION

1 Scope

1.1 This series of Recommendations | International Standards defines a set of generic facilities to assist in the provision of security services in OSI applications. These include:

- a) a set of notational tools to support the specification of selective field protection requirements in an abstract syntax specification, and to support the specification of security exchanges and security transformations;
- b) a service definition, protocol specification and PICS proforma for an application-service-element (ASE) to support the provision of security services within the Application Layer of OSI;
- c) a specification and PICS proforma for a security transfer syntax, associated with Presentation Layer support for security services in the Application Layer.

1.2 This Recommendation | International Standard defines the protecting transfer syntax, associated with Presentation Layer support for security services in the Application Layer.

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 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 listed 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.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*.
- ITU-T Recommendation X.216 (1994) | ISO/IEC 8822:1994, *Information technology – Open Systems Interconnection – Presentation service definition*.
- ITU-T Recommendation X.226 (1994) | ISO/IEC 8823-1:1994, *Information technology – Open Systems Interconnection – Connection-oriented presentation protocol: Protocol specification*.
- ITU-T Recommendation X.680 (1994) | ISO/IEC 8824-1:1995, *Information technology – Abstract Syntax Notation One (ASN.1): Specification of basic notation*.
- ITU-T Recommendation X.681 (1994) | ISO/IEC 8824-2:1995, *Information technology – Abstract Syntax Notation One (ASN.1): Information object specification*.
- ITU-T Recommendation X.682 (1994) | ISO/IEC 8824-3:1995, *Information technology – Abstract Syntax Notation One (ASN.1): Constraint specification*.
- ITU-T Recommendation X.683 (1994) | ISO/IEC 8824-4:1995, *Information technology – Abstract Syntax Notation One (ASN.1): Parameterization of ASN.1 specifications*.
- ITU-T Recommendation X.690 (1994) | ISO/IEC 8825-1:1995, *Information technology – ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*.

ISO/IEC 11586-4 : 1996 (E)

- ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.
- ITU-T Recommendation X.830 (1995) | ISO/IEC 11586-1:1996, *Information technology – Open Systems Interconnection – Generic upper layers security: Overview, models and notation*.