This is a preview - click here to buy the full publication

INTERNATIONAL STANDARD

ISO/IEC 11586-1

First edition
1996-06-01

Information technology — Open Systems Interconnection — Generic upper layers security: Overview, models and notation

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Sécurité des couches supérieures génériques: Présentation, modèles et notation

Reference number
ISO/IEC 11586-1:1996(E)

This is a preview - click here to buy the full publication

Contents

		Page
1	Scope	1
2	Normative references	1
2.1	Identical Recommendations | International Standards	2
2.2	Paired Recommendations | International Standards equivalent in technical content	2
3	Definitions	2
4	Abbreviations	4
5	General overview	4
6	Security exchanges	5
6.1	Security exchange model	5
6.2	Notation for specifying security exchanges	6
7	Security transformations	7
7.1	Security transformation model	7
7.2	Notation for specifying security transformations	11
8	Abstract syntax notation for selective field protection	12
8.1	Basic notation	12
8.2	Notation with transformation qualifier	14
8.3	Mapping protection requirements to security transformations	15
8.4	Notation for specifying protection mappings	15
9	Conformance	16
Annex A – ASN.1 definitions		17
Annex B – Registration of security exchanges and security transformations		22
Annex C – Security exchange specifications		23
Annex D – Security transformation specifications		27
Annex E – Protection mapping specifications		38
Annex F – Object identifier usage		41
Annex G – Guidelines for the use of generic upper layers security facilities		42
Annex H – Relationship to other standards		47
Annex I – Examples of use of the generic upper layers security facilities		50
Annex J – Bibliography		54

© 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

This is a preview - click here to buy the full publication

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 11586-1 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.830.

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*

Annexes A to F form an integral part of this part of ISO/IEC 11586. Annexes G to J are for information only.

This is a preview - click here to buy the full publication

Introduction

This Recommendation | International Standard forms part of a series of Recommendations | multi-part 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 1 of this series.

For informative guidelines on the application of all facilities described in this series, see Annex G.

It is important to note that these generic security facilities do not in themselves provide security services; they are simply construction tools for security-related protocols. Furthermore, these facilities do not necessarily provide a stand-alone solution to all security communications requirements of applications. Application standards may still need to incorporate security features within their specifications, to work in conjunction with generic security services supported by the Generic Upper Layers Security facilities.

This is a preview - click here to buy the full publication

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – GENERIC UPPER LAYERS SECURITY: OVERVIEW, MODELS AND NOTATION

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 following:

a) general models of security exchange protocol functions and security transformations, based on the concepts described in the OSI Upper Layers Security Model (ITU-T Rec. X.803 | ISO/IEC 10745);

b) 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;

c) a set of informative guidelines as to the application of the generic upper layers security facilities covered by this series of Recommendations | International Standards.

1.3 This Recommendation | International Standard does not define the following:

a) a complete set of upper layer security facilities which may be required by other Recommendations | International Standards;

b) a complete set of security facilities for specific applications;

c) the mechanisms employed to support security services.

1.4 The security exchange model, and supporting notation, are intended both for use as the basis of defining the security exchange service element in subsequent parts of this series of Recommendations | International Standards, and for use by any other ASE which may import security exchanges into its own specification.

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.

This is a preview - click here to buy the full publication

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.207 (1993) | ISO/IEC 9545:1994, *Information technology – Open Systems Interconnection – Application Layer structure.*
- ITU-T Recommendation X.214 (1993) | ISO/IEC 8072:1994, *Information technology – Open Systems Interconnection – Transport service definition.*
- ITU-T Recommendation X.216 (1994) | ISO/IEC 8822:1994, *Information technology – Open Systems Interconnection – Presentation service definition.*
- ITU-T Recommendation X.217 (1995) | ISO/IEC 8649: ...[1)], *Information technology – Open Systems Interconnection – Service definition for the Association Control Service.*
- 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.509 (1993) | ISO/IEC 9594-8:1995, *Information technology – Open Systems Interconnection – The Directory: Authentication framework.*
- ITU-T Recommendation X.511 (1993) | ISO/IEC 9594-3:1995, *Information technology – Open Systems Interconnection – The Directory: Abstract service definition.*
- CCITT Recommendation X.660 (1992) | ISO/IEC 9834-1:1993, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities: General procedures.*
- 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).*
- ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model.*
- ITU-T Recommendation X.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework.*
- ITU-T Recommendation X.812[1)] | ISO/IEC 10181-3: ...[1)], *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework.*

2.2 Paired Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*

  ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*

---

1) Presently at the stage of draft.