INTERNATIONAL STANDARD

ISO/IEC 11586-2

First edition
1996-06-01

Information technology — Open Systems Interconnection — Generic upper layers security: Security Exchange Service Element (SESE) service definition

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Sécurité des couches supérieures génériques: Définition du service pour l'élément de service d'échange de sécurité (SESE)



Reference number
ISO/IEC 11586-2:1996(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
3	Definitions	1
4	Abbreviations	2
5	Conventions	2
6	Service overview	2
	6.1 Specific service facilities	2
	6.2 Procedural model for SE-TRANSFER service facility	2
7	Service definition	3
	7.1 Parameters of service primitives	3
	7.2 Service primitives	4
8	Sequencing information	4

© 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

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 11586-2 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.831.

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*

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 | 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 2 of this series.

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) SERVICE DEFINITION

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 application layer protocols. 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;

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 service provided by the Security Exchange Service Element (SESE). The SESE is an ASE which allows the communication of security information to support the provision of security services within 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.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model.*

3 Definitions

The following terms are used as defined in ITU-T Rec. X.803 | ISO/IEC 10745:

- security exchange;

  security exchange item.

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

4 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

ASE Application Service Element

OSI Open Systems Interconnection

PICS Protocol Implementation Conformance Statement

SEI Security Exchange Item

5 Conventions

Clause 7 employs a tabular presentation of the SESE service primitive parameters. Each parameter is summarized using the following notation:

M Presence of the parameter is mandatory

O Presence of the parameter is an SESE protocol machine option

U Presence of the parameter is an SESE service user option

C Presence of the parameter is conditional

(=) The value of this parameter is identical to the value of the corresponding parameter of the preceding SESE service primitive.

6 Service overview

The security exchange service element provides for the communication of information associated with any security exchange, as described in Part 1. This service is typically used for the transfer of authentication, access control, non-repudiation or security management information.

6.1 Specific service facilities

The following service facilities are defined:

a) SE-TRANSFER;

b) SE-U-ABORT;

c) SE-P-ABORT.

The SE-TRANSFER service facility is used to initiate a security exchange of a certain type, transfer the first security-exchange-item (SEI), as well as transfer the other SEIs of a security exchange. It is the only service facility required in completing a security exchange.

The SE-U-ABORT service facility is used by the SESE service user to indicate that an error has occurred. This service is used to abnormally terminate a security exchange in progress. Optionally, this service may also abnormally terminate the ASO-association.

The SE-P-ABORT service facility is used by the SESE service provider to indicate that an error has occurred. This service is used to abnormally terminate a security exchange in progress. Optionally, this service may also abnormally terminate the ASO-association.

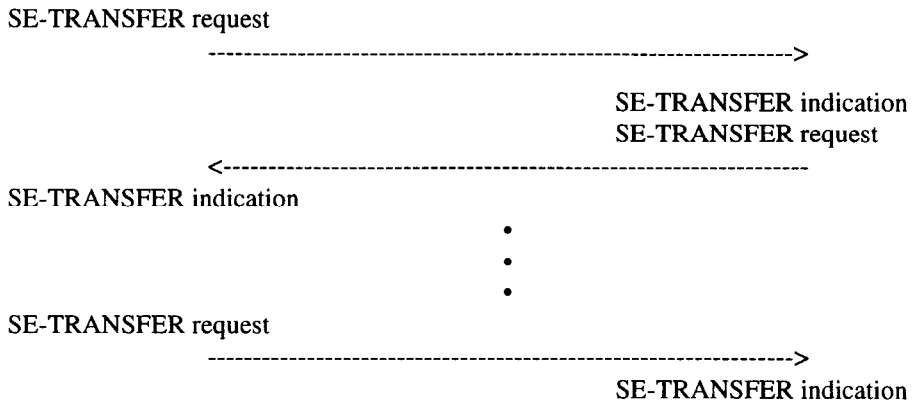
6.2 Procedural model for SE-TRANSFER service facility

Part 1 of this Recommendation | International Standard defines the following procedural model for security exchanges:

An initial Security Exchange Item (SEI) is transferred from A to B. This is optionally followed by one or more transfers of SEIs between A and B, according to the specific security exchange identified in the SE-TRANSFER. The sequence may be terminated upon receipt of any SEI, by generation of an error indication by either service user or service provider.

The time-sequence diagram shown below is an example illustrating the special case of a sequence of SEI transfers in alternate directions for an n-way security exchange. (This is an example of the "Alternating" class of exchange defined in 6.1 of ITU-T Rec. X.830 | ISO/IEC 11586-1.)

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



7 Service definition

The SESE service primitives are of the following types:

SE-TRANSFER	Non-confirmed
SE-U-ABORT	Non-confirmed
SE-P-ABORT	Provider-initiated

7.1 Parameters of service primitives

Following are descriptions of the service primitives parameters.

7.1.1 Security exchange identifier

This parameter identifies the particular type of security exchange being initiated. The identifier is established when the security exchange is defined, using the SECURITY-EXCHANGE information object class defined in Part 1.

7.1.2 Invocation identifier

This parameter identifies a particular security exchange invocation. It is used for subsequently referring to that invocation for correlation purposes, in a SE-TRANSFER, SE-U-ABORT, or SE-P-ABORT primitives.

Invocation identifiers are especially useful in handling multiple security exchange invocations within the context of, for example, an application association.

Invocation identifiers are provided by the users of services which initiate security exchanges, and it is the responsibility of such users to ensure that these identifiers are unambiguous within the scope of all active security exchange invocations.

7.1.3 Security exchange item

The item to be conveyed, as implied by the security exchange identifier.

7.1.4 Item identifier

In a SE-TRANSFER primitive, this parameter indicates which item of the security exchange this primitive is conveying. In a SE-U-ABORT or SE-P-ABORT primitive, this parameter indicates the item of a security exchange on which an error condition has been detected.

The specification of a security exchange may place specific constraints on the use of the "item identifier". It is the responsibility of the SESE user to ensure that these constraints are met.

7.1.5 Start flag

In a SE-TRANSFER primitive, this parameter is used to indicate the transfer of the first security-exchange-item of a security exchange.

7.1.6 End flag

In a SE-TRANSFER primitive, this parameter is used to indicate that this security exchange item corresponds to the last security exchange required to satisfy the security mechanism. It is needed to accommodate those mechanisms requiring n exchanges, where n is not known *a priori*.

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

7.1.7 Error list

This parameter is one or more lists of error codes with optional error parameters. The error code indicates the cause of a SE-U-ABORT being generated. Error codes are established when a security exchange is defined, using the SE-ERROR information object class defined in Part 1. The optional error parameters provide additional information describing the cause of an abort.

7.1.8 Problem code

This parameter indicates the cause of an SE-P-ABORT being generated. The set of possible values is specified in clause 6 of Part 3.

7.1.9 Fatality indicator

In a SE-U-ABORT request primitive, this parameter is used to indicate to the SESE service provider whether or not the ASO-association (e.g. application association) must be terminated.

In a SE-U-ABORT indication and SE-P-ABORT indication primitives, this parameter is used to indicate to the SESE service user whether or not the ASO-association (e.g. application association) must be terminated.

7.2 Service primitives

The parameters of the SESE service primitives are provided below. (Refer to 6.1 for a definition of the SESE services, and to 7.1 for a description of the specific parameters.)

7.2.1 SE-TRANSFER service

The parameters of the SE-TRANSFER service are as follows:

Parameter Name	*Req*	*Ind*
Security exchange identifier	M	M(=)
Invocation identifier	U	C(=)
Security exchange item	M	M(=)
Item identifier	U	C(=)
Start flag	U	C(=)
End flag	U	C(=)

7.2.2 SE-U-ABORT service

The parameters of the SE-U-ABORT service are as follows:

Parameter Name	*Req*	*Ind*
Invocation identifier	U	C(=)
Item identifier	U	C(=)
Error list	U	C(=)
Fatality Indicator	U	C(=)

7.2.3 SE-P-ABORT service

The parameters of the SE-P-ABORT service are as follows:

Parameter Name	*Ind*
Invocation identifier	O
Item identifier	O
Problem code	M
Fatality Indicator	O

8 Sequencing information

The only sequencing constraint stipulated in this Service definition is that the invocation of SE-TRANSFER primitives with the same invocation identifier must be consistent with 7.1.2.

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

Descriptors: data processing, information interchange, network interconnection, open systems interconnection, application layer, communication procedure, security techniques, services.

Price based on 4 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