INTERNATIONAL STANDARD

ISO/IEC 11586-3

First edition
1996-06-01

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

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO/IEC 11586-3:1996
https://standards.iteh.ai/catalog/standards/sist/66d4159e-c0d7-4e26-8d8f-73fdfd0a510b/iso-iec-11586-3-1996

INTERNATIONAL ISO/IEC

Reference number
ISO/IEC 11586-3:1996(E)

Contents

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 11586-3:1996
https://standards.iteh.ai/catalog/standards/sist/66d4159e-c0d7-4e26-8d8f-73fdfd0a510b/iso-iec-11586-3-1996

© 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 11586-3 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.832.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

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

ISO/IEC 11586-3:1996
https://standards.iteh.ai/catalog/standards/sist/...-4e26-8d8f-72f1fd0a510b/iso-iec-11586-3-1996

- *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 and B form an integral part of this part of ISO/IEC 11586.

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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 11586-3:1996
https://standards.iteh.ai/catalog/standards/sist/66d4159e-c0d7-4e26-8d8f-73fdfd0a510b/iso-iec-11586-3-1996

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – GENERIC UPPER LAYERS SECURITY: SECURITY EXCHANGE SERVICE ELEMENT (SESE) PROTOCOL 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 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 protocol 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.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

2 Normative references

ISO/IEC 11586-3:1996
https://standards.iteh.ai/catalog/standards/sist/66d4159e-c0d7-4e26-8d8f-731d1d0a510b/iso-iec-11586-3-1996

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.207 (1993) | ISO/IEC 9545:1994, *Information technology – Open Systems Interconnection – Application Layer structure.*
- 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 Element.*
- 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.227 (1995) | ISO/IEC 8650-1:...[1], *Information technology – Open Systems Interconnection – Connection-oriented protocol for the Association Control Service Element: 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.*

[1] To be published.

- 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.*

3 Definitions

This Recommendation | International Standard makes use of the following terms defined in ITU-T Rec. X.803 | ISO/IEC 10745:

- security exchange;
- security exchange item.

4 Abbreviations

ACSE	Association Control Service Element
APDU	application-protocol-data-unit
ASE	application-service-element
ASO	application-service-object
OSI	Open Systems Interconnection
PICS	Protocol Implementation Conformance Statement
SEPM	Security Exchange Protocol Machine
SEI	Security Exchange Item
SESE	Security Exchange Service Element

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 11586-3:1996
https://standards.iteh.ai/catalog/standards/sist/66d4159e-c0d7-4e26-8d8f-73f6f86e510b/iso-iec-11586-3-1996

5 Overview of the protocol

5.1 Service provision

The protocol defined in this Specification provides the services defined in ITU-T Rec. X.831 | ISO/IEC 11586-2. These services are as follows:

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

5.2 Use of underlying services

This SESE protocol defines a set of APDUs, each of which may potentially be mapped onto any Presentation Layer service which conveys user-data, or which may be embedded in or concatenated with any other application-PDU, according to the rules of the ASO-context or application-context in force.

Clause 8 defines some useful mappings to the presentation-service and ACSE.

6 Elements of procedure

6.1 APDUs used

The SESE protocol specifies the following APDUs:

SE-TRANSFER APDU (SETR)

SE-U-ABORT APDU (SEAB)

SE-P-ABORT APDU (SEPA)

6.2 Transfer procedure

This procedure is used by a requestor SEPM to initiate a security-exchange requiring the transfer of one or more security-exchange-items. This procedure is also used by either requestor or responder SEPM to transfer further security-exchange-items started by the requestor SEPM.

On receipt of a SE-TRANSFER request primitive, the SEPM retains the security exchange identifier, and generates a SE-TRANSFER APDU (SETR).

On receipt of a SE-TRANSFER APDU (SETR), the SEPM retains the security exchange identifier, and issues a SE-TRANSFER indication primitive.

If the security exchange belongs to the "Alternating" class, and the exchange does not follow the expected sequence, then the SEPM generates an SE-P-ABORT APDU (SEPA), and issues an SE-P-ABORT indication.

6.3 User-initiated abort procedure

iTeh STANDARD PREVIEW
(standards.iteh.ai)

This procedure is used for one SESE user to indicate to the peer SESE user and the SEPM that an error has occurred and that any security exchange in progress is to be abnormally terminated. Additionally, it may optionally cause the abnormal release of the ASO-association with the possible loss of information in transit. It is initiated by an SE-U-ABORT request primitive.

ISO/IEC 11586-3:1996
https://standards.iteh.ai/catalog/standards/sist/66d4159e-c0d7-4e26-8d8f-73f6f0a510b4/iso-iec-11586-3-1996

On receipt of an SE-U-ABORT request primitive, the SEPM generates an SE-ABORT APDU (SEAB).

On receipt of an SE-ABORT APDU (SEAB), the SEPM issues an SE-U-ABORT indication primitive.

6.4 Provider-initiated abort procedure

This procedure is used for the SEPM to indicate to the SESE users that an error has occurred and that any security exchange in progress is to be abnormally terminated. Additionally, it may optionally cause the abnormal release of the ASO-association with the possible loss of information in transit.

On detection of an error, the SEPM issues an SE-P-ABORT indication primitive and generates an SE-P-ABORT APDU (SEPA). If the severity of the error requires the ASO-association to be terminated, the SEPA APDU is mapped to the ASO-Association Abort service. On receiving an ASO-Association Abort indication with SEPA APDU, the SEPM issues an SE-P-ABORT indication with the fatality indicator set.

An error condition causing a SE-P-ABORT to be generated has an associated *problem code*, which may be indicated to both ends. The problems so indicated are categorized as follows:

a) *general problem* – Not peculiar to any particular APDU type;

b) *transfer problem* – Problem resulting from receipt of a SE-TRANSFER APDU;

c) *abort problem* – Problem resulting from receipt of a SE-U-ABORT APDU.

Particular error conditions, and the associated problem codes, are described in the following.

6.4.1 General problem

– *Invalid APDU* – The structure and/or encoding of the APDU do not conform to either SETR, SEAB, or SEPA APDUs.

6.4.2 Transfer problem

a) *Duplicate invocation identifier* – The same invocation identifier is in use for another active security exchange invocation.

b) *Unrecognized security exchange* – The security exchange identified is not valid for this ASO-context.

c) *Mistyped item* – The type of the SEI does not conform to that in the object class definition.

d) *Inappropriate invocation identifier* – The invocation identifier is not within the set specified for this ASO-context.

e) *Alternating sequence error* – The received SETR does not follow the sequence of the "Alternating" class of security exchange.

6.4.3 Abort problem

a) *Unrecognized invocation identifier* – The invocation identifier does not identify an active or just-completed security exchange transfer.

b) *Abort unexpected* – The identified security exchange does not generate an abort for *this* security exchange item.

c) *Unrecognized error* – The identified security exchange does not generate this error.

d) *Unexpected error* – The identified security exchange does not generate *this* error for this security exchange item.

e) *Mistyped error parameter* – The type of the error parameter does not conform to that in the error definition.

7 Structure and encoding of SESE APDUs

iTeh STANDARD PREVIEW

The parameterized data type of the generic SESE APDUs is specified in 7.1, using ASN.1 (see ITU-T Rec. X.683 | ISO/IEC 8824-4). The method of constructing a SESE abstract syntax to support a particular set of security exchanges is described in 7.2.

(standards.iteh.ai)

ISO/IEC 11586-3:1996
https://standards.iteh.ai/catalog/standards/sist/66d4159e-c0d7-4e26-8d8f-73f1f30a510b/iso-iec-11586-3-1996

7.1 Generic APDU specification

The following parameterized APDU specification supports the definition of abstract syntaxes for tailored SESEs supporting any set of security exchanges defined using the specification framework in Part 1 of this Recommendation | International Standard. In the following, the parameter ValidSEs identifies the set of security exchanges supported. The parameter InvocationIdSet defines the available values for identifying distinct security exchange invocations which may be active simultaneously, and for use in correlating subsequent responses and error indications with the active security exchange invocations. If such correlation is not needed in some realization (e.g. different security exchange invocations never overlap), then InvocationIdSet should be set to the value set NoInvocationId.

```
SeseAPDUs {joint-iso-ccitt genericULS(20) modules(1) seseAPDUs(6) }
DEFINITIONS AUTOMATIC TAGS::=
BEGIN

-- EXPORTS ALL --

IMPORTS

        notation
            FROM ObjectIdentifiers {joint-iso-ccitt genericULS (20)
                modules (1) objectIdentifiers (0) }
        dirAuthenticationTwoWay
            FROM GulsSecurityExchanges {joint-iso-ccitt genericULS (20)
                modules (1) gulsSecurityExchanges (2) }
        SECURITY-EXCHANGE {}, SE-ERROR {}
            FROM NOTATION notation;

SESEapdus {SECURITY-EXCHANGE:ValidSEs, InvocationId:InvocationIdSet }::=

        CHOICE {
            se-transfer         SETransfer {{ValidSEs},{InvocationIdSet}},
            se-u-abort          SEUAbort {{ValidSEs},{InvocationIdSet}},
            se-p-abort          SEPAbort {{ValidSEs},{InvocationIdSet}}
            }
```

```
SETransfer {SECURITY-EXCHANGE:ValidSEs, InvocationId:InvocationIdSet }::=
SEQUENCE {
        seIdentifier        SECURITY-EXCHANGE.&sE-Identifier ( {ValidSEs}),
                            -- This identifies one of the security-
                            -- exchanges supported by the particular SESE
                            -- abstract syntax
        itemIdentifier      SECURITY-EXCHANGE.&SE-Items.&itemId
                            ( {ValidSEs}{@seIdentifier}),
                            -- This identifies one of the security-
                            -- exchange-items of the security exchange
                            -- indicated by "seIdentifier"
        seItem              SECURITY-EXCHANGE.&SE-Items.&ItemType
                            ({ValidSEs}{@seIdentifier, @itemIdentifier}),
        invocationId        InvocationId (InvocationIdSet)
                            (CONSTRAINED BY {-- Must be the same as the
                            -- invocationId on an active security exchange
                            -- if start flag is not true --})
                            DEFAULT noInvocationId,
        startFlag           BOOLEAN DEFAULT FALSE,
                            -- This field is set only as the first security-
                            -- exchange-item of a security-exchange is
                            -- transferred.
        endFlag             BOOLEAN DEFAULT FALSE
                            -- This field is set as the last security-exchange-
                            -- item of a security-exchange is transferred. It is
                            -- needed to accommodate those mechanisms requiring
                            -- n exchanges, where n is not known a priori -- }

SEUAbort {SECURITY-EXCHANGE:ValidSEs, InvocationId:InvocationIdSet }::=
SEQUENCE {
        invocationId        InvocationId (InvocationIdSet)
                            (CONSTRAINED BY {-- Must be the same as the
                            -- invocationId on an active or just completed
                            -- security exchange --})
                            DEFAULT noInvocationId,
        itemIdentifier      SECURITY-EXCHANGE.&SE-Items.&itemId
                            ( {ValidSEs.&SE-Items}) OPTIONAL,
                            -- This component will only be present
                            -- when the Abort is generated subsequent
                            -- to receipt of a SETransfer APDU.
        errors              SEQUENCE OF SEerror {{ValidSEs}}    OPTIONAL
                            -- needed to handle multiple error codes -- }

SEPAbort {SECURITY-EXCHANGE:ValidSEs, InvocationId:InvocationIdSet }::=
SEQUENCE {
        invocationId        InvocationId (InvocationIdSet) OPTIONAL,
        itemIdentifier      SECURITY-EXCHANGE.&SE-Items.&itemId
                            ( {ValidSEs.&SE-Items}) OPTIONAL,
                            -- This component will only be present
                            -- when the Abort is generated subsequent
                            -- to receipt of a SETransfer APDU.
        problemCode         ProblemCode }

InvocationId ::= CHOICE {
        present             INTEGER,
        absent              NULL }

noInvocationId InvocationId ::= absent:NULL

NoInvocationId InvocationId ::= {noInvocationId}

SEerror {SECURITY-EXCHANGE:ValidSEs }::= SEQUENCE {
        errorCode           SE-ERROR.&errorCode
                            ({Errors{{ValidSEs}}}) OPTIONAL,
        errorParameter      SE-ERROR.&ParameterType
                            ({Errors{{ValidSEs}}}{@errorCode}) OPTIONAL}
```

iTeh STANDARD PREVIEW
(standards.iteh.ai)
ISO/IEC 11586-3:1996
https://standards.iteh.ai/catalog/standards/sist/66d4159e-c0d7-4e26-8d8f-75fdfd0a510b/iso-iec-11586-3-1996

```
Errors{SECURITY-EXCHANGE:ValidSEs} SE-ERROR ::= {ValidSEs.&SE-Items.&Errors}

ProblemCode ::= CHOICE {
        general         GeneralProblem,
        transfer        TransferProblem,
        abort           AbortProblem }

GeneralProblem ::= ENUMERATED {
        invalidAPDU (0) }

TransferProblem ::= ENUMERATED {
        duplicateInvocationId (0),
        unrecognizedSecurityExchange (1),
        mistypedItem (2),
        inappropriateInvocationId (3),
        alternatingSequenceError (4) }

AbortProblem ::= ENUMERATED {
        unrecognizedInvocationId (0),
        abortUnexpected (1),
        unrecognizedError (2),
        unexpectedError (3),
        mistypedErrorParameter (4) }

END
```

iTeh STANDARD PREVIEW
(standards.iteh.ai)

7.2 Abstract syntax construction

An abstract syntax for a SESE supporting a given set of security exchanges is specified using the ABSTRACT-SYNTAX information object class defined in ITU-T Rec. 681 | ISO/IEC 8824-2, Annex B.

ISO/IEC 11586-3:1996
https://standards.iteh.ai/catalog/standards/sist/66d4159e-c0d7-4e26-84f6-73f1f0a510b/iso-iec-11586-3-1996

For example, to specify a SESE abstract syntax supporting two of the security exchanges defined in Annexes D and F of Part 1 of this Specification, for a realization not requiring invocation identifiers, the following notation would be used:

```
AccCtl-Authent-Abstract-Syntax
ABSTRACT-SYNTAX ::=
    { SESEapdus {
        { boundAccessControlCert | dirAuthenticationTwoWay },
        NoInvocationId }
    IDENTIFIED BY {..Abstract Syntax Object Identifier..}
```

8 Mapping to underlying services

8.1 General

The SESE protocol defines a set of APDUs, each of which may potentially be mapped onto any Presentation Layer service which conveys user-data, or which may be embedded in or concatenated with any other APDU, according to the rules of the ASO-context or application-context in force.

Unless specified otherwise in the ASO-context (or application-context) definition, an SEAB, with a fatality indicator set, or an SEPA, with a severity of error requiring the abnormal termination of the association, are mapped to the A-ABORT service, while an SETR is mapped to the P-DATA service.

If the SESE is included in an application-context specification, then the inclusion of the ACSE-Authentication functional unit in this application context is neither required nor precluded.

The SESE does not use other ASEs directly, but only indirectly via a control function (as indicated in the Application Layer Structure). Some examples of useful mappings which may be specified are however shown below.

8.2 Mapping to ACSE services

8.2.1 Mapping of SE-TRANSFER to A-ASSOCIATE

When the first one or two transfers of a security-exchange are to occur in conjunction with association establishment, an SE-TRANSFER APDU may be mapped to the authentication-value field or user-information field of A-ASSOCIATE request/indication.

When an SE-TRANSFER APDU is in reply to the SE-TRANSFER APDU conveyed on A-ASSOCIATE request/indication, the former SE-TRANSFER APDU may be mapped to the authentication-value field or user-information field of A-ASSOCIATE response/confirm.

When an SE-TRANSFER APDU is mapped to the authentication-value field of A-ASSOCIATE, the EXTERNAL option should be used and the authentication-mechanism name field should not be used.

8.2.2 Mapping of Additional SE-TRANSFERs

When the security-exchange occuring in conjunction with association establishment requires the transfer of more than two security-exchange-items, then the third transfer (SE-TRANSFER) and beyond may be mapped onto P-DATA. In this case, the application-context is likely to have a rule that stipulates that, even though the association was successfully established after the first two transfers, it is not to be used by other ASEs until the security exchange has successfully completed.

9 Conformance

A system claiming to implement the procedures specified in this Recommendation | International Standard shall comply with the requirements in 9.1 through 9.3.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

9.1 Statement Requirements

ISO/IEC 11586-3:1996
https://standards.iteh.ai/catalog/standards/sist/66d4159e-c0d7-4e26-8d8f-73fdfd0a510b/iso-iec-11586-3-1996

The following shall be stated by the implementor:

a) the set of security exchanges provided;

b) for each security exchange provided, whether the system is capable of initiating the security exchange and/or responding to the security exchange initiated by the other end;

c) the range of invocation identifiers that can be generated/active simultaneously;

d) whether the system can support the "Alternating" and/or "Arbitrary" class of security exchange.

9.2 Static Requirements

The system shall:

a) act in the role of initiator and/or responder for one or more security exchanges.

b) support (as a minimum) that encoding which results from applying the basic ASN.1 encoding rules to the ASN.1 specified in clause 7 for the purpose of exchanging SESE APDUs.

9.3 Dynamic Requirements

The system shall follow all the procedures specified in clause 6.