

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)

AVA Documents
Document Sharing Hub

Contents

	<i>Page</i>
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

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.

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.

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.

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.812¹⁾ | 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*.

3 Definitions

3.1 The following term is used as defined in ITU-T Rec. X.200 | ISO/IEC 7498-1:

- transfer syntax.

¹⁾ Presently at the stage of draft.

3.2 The following terms are used as defined in CCITT Rec. X.800 | ISO 7498-2:

- access control;
- confidentiality;
- data origin authentication;
- decipherment;
- digital signature;
- encipherment;
- integrity;
- key;
- key management;
- selective field protection.

3.3 The following terms are used as defined in ITU-T Rec. X.216 | ISO/IEC 8822:

- abstract syntax;
- presentation context;
- presentation data value.

3.4 The following terms are used as defined in ITU-T Rec. X.207 | ISO/IEC 9545:

- application-association
- application-context;
- application-service-element (ASE);
- application-service-object-association (ASO-association).

3.5 The following terms are used as defined in ITU-T Rec. X.811 | ISO/IEC 10181-2:

- authentication exchange;
- claimant;
- entity authentication;
- verifier.

3.6 The following term is used as defined in ITU-T Rec. X.812 | ISO/IEC 10181-3:

- access control certificate.

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

- security association;
- security communication function (SCF);
- security exchange;
- security exchange item;
- security exchange function;
- security transformation;
- system security object (SSO).

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

3.8.1 presentation-context-bound security association: A security association which is established in conjunction with the establishment of a protecting presentation context, and which applies to all presentation data values sent in one direction in that protecting presentation context; attributes of the security association are indicated explicitly along with the encoding of the first presentation data value in the protecting presentation context.

3.8.2 single-item-bound security association: A security association applying to a single independently-protected presentation data value which is not associated with a presentation context; attributes of the security association are indicated explicitly along with the presentation data value encoding.

ISO/IEC 11586-1 : 1996 (E)

3.8.3 externally-established security association: A security association which is established independently of instances of its use, and which has a globally-unique identifier enabling it to be referenced at the time of use.

3.8.4 initial encoding rules: The ASN.1 encoding rules used to generate an unprotected bit string from a value of an ASN.1 type, when that value is to be protected using a security transformation.

3.8.5 protecting presentation context: A presentation context which associates a protecting transfer syntax with an abstract syntax.

3.8.6 protecting transfer syntax: A transfer syntax which employs a security transformation.

3.8.7 protection mapping: A specification which relates a protection requirement, identified by name in an abstract syntax specification, to a specific security transformation to be used to satisfy that requirement.

4 Abbreviations

ACSE	Association Control Service Element
ASE	application-service-element
ASO	application-service-object
GULS	Generic Upper Layers Security
OSI	Open Systems Interconnection
PDU	protocol-data-unit
PDV	Presentation Data Value
PICS	Protocol Implementation Conformance Statement
SCF	Security Communication Function
SEI	Security Exchange Item
SESE	Security Exchange Service Element
SSO	System Security Object

5 General overview

The Generic Upper Layers Security (GULS) Standards define a set of protocol-construction tools and protocol components to support the provision of security protection for applications. These facilities support the provision of security services in the OSI Upper Layers (Application Layer, sometimes with Presentation Layer support).

NOTE – Security services for OSI applications may be provided using security mechanisms at either the upper or lower layers. In the latter case, the protection is obtained by specifying an appropriate protection quality-of-service (as defined in ITU-T Rec. X.214 | ISO/IEC 8072) to ACSE when establishing an application-association. This protection quality-of-service is passed transparently through the Presentation and Session Layers to the transport service. Provision of security services in the lower layers is outside the scope of this Recommendation | International Standard.

The facilities provided in the GULS Standards include:

- a general means of building Application Layer protocol components to support the exchange of security-related information between a pair of communicating application-entity-invocations (the security exchange concept, which is supported by the SESE); these facilities are described in clause 6;
- a general approach to using Presentation Layer facilities to perform security-related transformations on information items in order to protect these items (the security transformation concept, which is supported by a generic protecting transfer syntax); these facilities are described in clause 7;
- abstract syntax notation tools to assist an application protocol designer in specifying that security protection is to apply to selected fields of this protocol (a PROTECTED parameterized type, and the PROTECTED-Q variant of this type); these facilities are described in clause 8.

Security exchanges are used for such purposes as entity authentication and key management. Security transformations (and the generic protecting transfer syntax and/or PROTECTED parameterized type or its variations) are used for such purposes as integrity, confidentiality, data origin authentication and/or non-repudiation.

The Upper Layers Security Model (ITU-T Rec. X.803 | ISO/IEC 10745) provides the architectural model for the GULS specifications. It describes the roles of security exchange functions and security transformations.

Security exchange functions provide the means for communicating security information between application-entity-invocations as part of the operation of a security mechanism, i.e. they generate and process application-protocol-control-information with a security-related purpose. Security exchanges may be specified using the notation in this Recommendation | International Standard, then imported into any abstract syntax specification. The Security Exchange Service Element (SESE) is an application-service-element (ASE) defined in ITU-T Rec. X.831 | ISO/IEC 11586-2 and ITU-T Rec. X.832 | ISO/IEC 11586-3. The SESE provides a way of conveying security exchanges, which supports the goal of making application-specific ASEs independent of security mechanisms used. However, some aspects of the specification of an application which directly incorporates security provisions will be mechanism dependent.

Security transformations can be supported by the generic protecting transfer syntax described in ITU-T Rec. X.833 | ISO/IEC 11586-4.

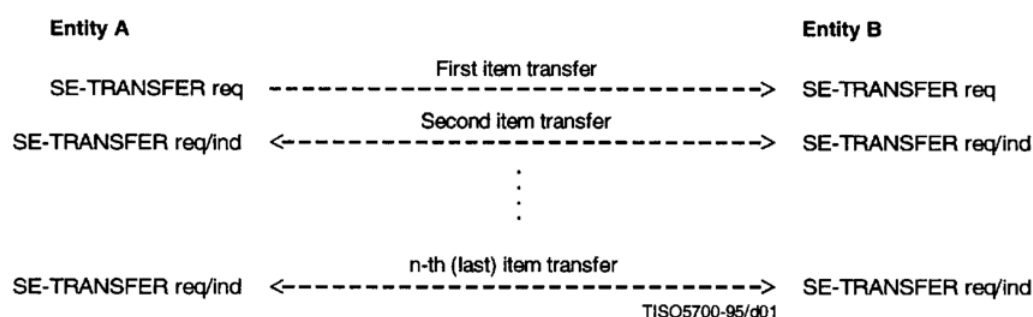
6 Security exchanges

6.1 Security exchange model

This Recommendation | International Standard defines the procedural model for a security exchange, as introduced in ITU-T Rec. X.803 | ISO/IEC 10745.

A security exchange occurs between two entities A and B. It consists of the transfer of one Security Exchange Item (SEI) from A to B, possibly followed by a sequence of one or more transfers of SEIs in either direction between A and B. The number of transfers depends upon the particular security exchange. Each SEI may comprise an arbitrarily complex data structure, representable by any ASN.1 type. It may include components which are individually protected using the PROTECTED notation described in clause 8.

The time-sequence diagram in Figure 1 illustrates the sequence of SEI transfers for an n-way security exchange, and the corresponding SESE service primitive invocations, as defined in ITU-T Rec. X.831 | ISO/IEC 11586-2.



Note – The double-sided arrow indicates that the transfer could be send by either A or B.

Figure 1 – Security exchange model

There are two classes of exchange:

- *Alternating* – Successive item transfers occur in alternating directions and only one transfer is active at any time;
- *Arbitrary* – There are no constraints upon direction of any transfer and transfers in the two directions may be active simultaneously.

While a security exchange is in progress, other information transfers may occur and other security exchanges may be in progress on the same application-association. However, application-context rules will usually constrain such overlapping activities. Presentation data values conveying SEIs may be concatenated with, interleaved with, or embedded in other presentation data values.

6.2 Notation for specifying security exchanges

A specification of a security exchange includes a specification of the types of SEIs that may be exchanged, a statement of any ordering constraints applying to transfers of these SEIs, a statement of error conditions that may result from the transfer of each SEI, and a statement of (or reference to) the associated semantics.

A security exchange definition includes:

- a) assignment of a global object identifier or a local integer value to the security exchange, to allow its use to be unambiguously identified in protocol;
- b) a specification of the abstract syntax of the SEIs and error notifications transferred in the security exchange.

To support specification of this information in a form which can be used by the SESE protocol, three ASN.1 information object class definitions (see ITU-T Rec. 681 | ISO/IEC 8824-2) are provided:

- the SECURITY-EXCHANGE information object class is used in specifying a particular security exchange; an information object of this class contains one or more SEC-EXCHG-ITEM information objects;
- the SEC-EXCHG-ITEM information object class is used to define one SEI; an information object of this class may contain one or more ERROR information objects;
- the SE-ERROR information object class is used to define an error condition which may result from the transfer of a SEI.

NOTE – Annex G provides guidelines showing how these information object classes are used in the definition of a complete Application Context.

SECURITY-EXCHANGE ::= CLASS

-- This information object class definition is for use when

-- specifying a particular instance of a security exchange.

```
{
  &SE-Items      SEC-EXCHG-ITEM,
  -- This is an ASN.1 information object set, comprising a set
  -- of security exchange items
  &SE-Identifier Identifier      UNIQUE
  -- A local or global identifier for the particular security exchange
}
```

WITH SYNTAX

-- The following syntax is used to specify a particular security exchange.

```
{
  SE-ITEMS      &SE-Items
  IDENTIFIER    &SE-Identifier
}
```

Identifier ::= CHOICE

```
{
  local          INTEGER,
  global         OBJECT IDENTIFIER
}
```

SEC-EXCHG-ITEM ::= CLASS

```
{
  &ItemType,
  -- ASN.1 type for this exchange item
  &itemId      INTEGER,
  -- Identifier for this item, e.g. 1, 2, 3, ..
  &Errors      SE-ERROR      OPTIONAL
  -- Optional list of errors which may result from transfer of this item
}
```

WITH SYNTAX

```
{
  ITEM-TYPE      &ItemType
  ITEM-ID        &itemId
  [ERRORS        &Errors]
}
```

```

SE-ERROR ::= CLASS
{
    &ParameterType    OPTIONAL,
    -- ASN.1 type of a parameter to accompany the signalling
    -- of the error condition back to the sender of the SEI
    &errorCode         Identifier    UNIQUE
    -- An identifier used in signalling the error condition
    -- back to the sender of the SEI
}
WITH SYNTAX
{
    [PARAMETER         &ParameterType]
    ERROR-CODE         &errorCode
}

```

Examples of the use of this notation are given in Annex C.

7 Security transformations

7.1 Security transformation model

A security transformation is a security function (or combination of security functions) applied to user data to protect that data during communication or storage. A security transformation involves an encoding process applied prior to communication or storage, and a decoding process which may be (but need not always be) applied upon receipt or retrieval. Examples of security transformations are:

- a) applying an encipherment process on encoding of data and a corresponding decipherment process on decoding;
- b) generating a seal or signature and appending it to data on encoding and checking and removing the appended seal or signature on decoding;
- c) combining the functions in a) and b) into one security transformation.

Security transformations defined using the notation in 7.2 are suitable for use by OSI applications (in conjunction with the generic protecting transfer syntax defined in ITU-T Rec. X.833 | ISO/IEC 11586-4) or for other purposes, including off-line protection in local storage and non-OSI communications.

NOTE – Subclause 7.1.5 describes use of security transformations on an OSI presentation connection. Subclause 7.1.6 describes their use independently of the OSI presentation protocol.

Security transformations may constitute the primary means of providing a security service (e.g. confidentiality, integrity, data origin authentication) or they may contribute to the provision of a security service (e.g. entity authentication, access control, non-repudiation).

Figure 2 illustrates the steps involved in protecting a data item for transfer or storage.

At an encoding system, the process of deriving a transformed (protected) representation of an unprotected data item is:

- a) if the unprotected item is a value of an ASN.1 type, as specified in an abstract syntax definition, encode to a bit string representation using initial encoding rules; then
- b) apply the encoding process of the security transformation to the bit string representation of the unprotected item, possibly using additional local input information, to obtain a transformed item, which is a value of the ASN.1 type *XformedDataType* (the precise type is specified as part of the security transformation definition); then
- c) encode the ASN.1 value resulting from b) (possibly as part of the process of encoding an encompassing ASN.1 value, such as the protecting transfer syntax structure defined in ITU-T Rec. X.833 | ISO/IEC 11586-4).

At a decoding system, the process of recovering the unprotected data item and/or checking for a security compromise is:

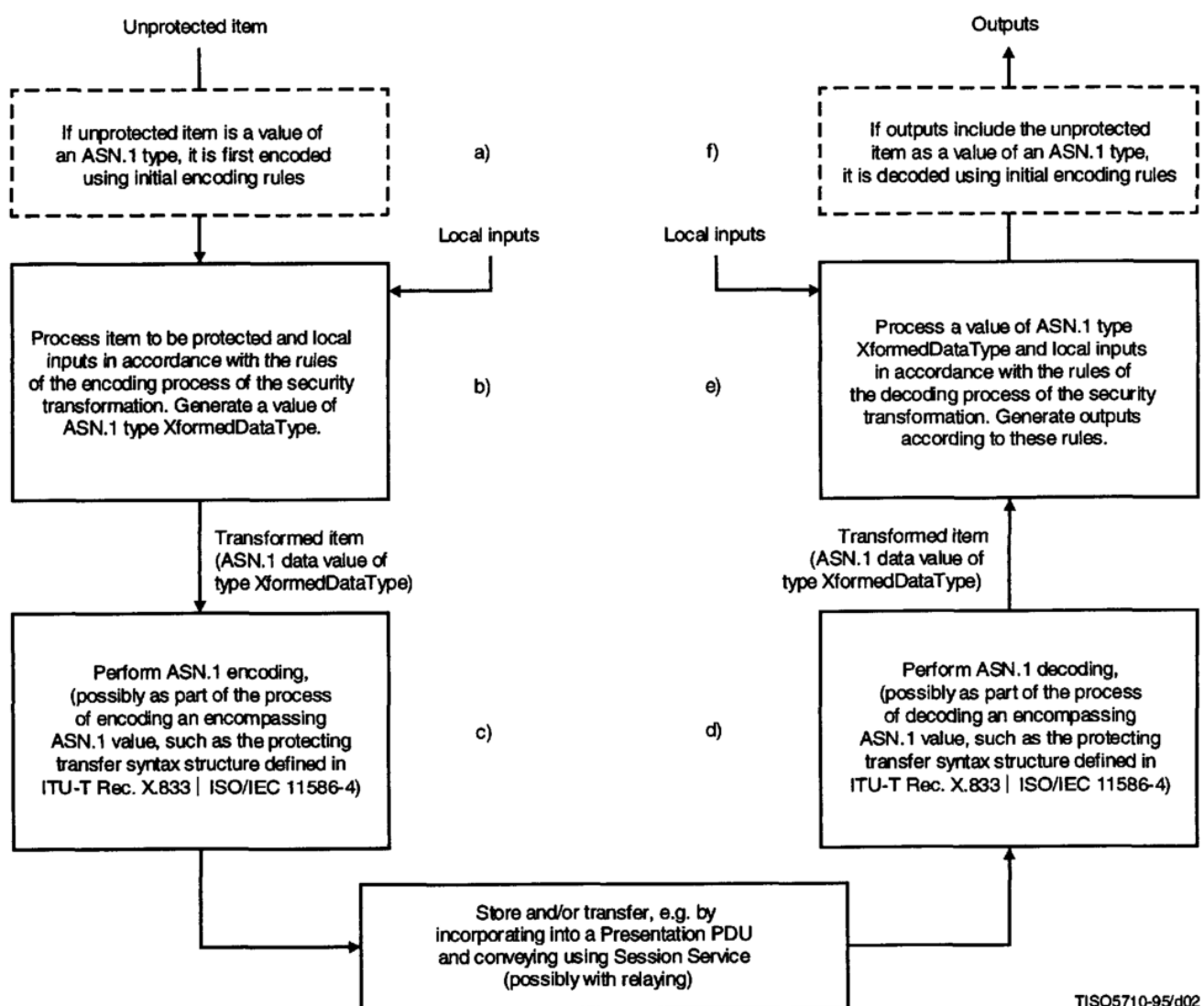
- d) decode the received or retrieved transformed item, which is an ASN.1 value of type *XformedDataType* (this decoding process may form part of the decoding of an encompassing ASN.1 value, such as the protecting transfer syntax structure defined in ITU-T Rec. X.833 | ISO/IEC 11586-4); then

ISO/IEC 11586-1 : 1996 (E)

- e) apply the decoding process of the security transformation to the received or retrieved value, possibly using additional local input information, and generate outputs according to that decoding process (depending upon the particular transformation, outputs might include a recovered copy of the unprotected item, an indication of success/failure of signature or seal verification, and/or a copy of a signature for storing locally for later use); then
- f) if an output of step e) is a recovered copy of the unprotected item, and if that item is a value of an ASN.1 type as specified in an abstract syntax definition, decode that data item using the same initial encoding rules as in step a).

Determination of the initial encoding rules in steps a) and f) is described in 7.1.4. Note that, in general, security transformations may operate upon data items other than values of ASN.1 types (e.g. arbitrary bit strings), so this encoding process is not always needed.

Determination of the encoding rules for steps c) and d) depends upon the storage or communication environment, and is independent of the particular security transformation used.



TISO5710-95/d02

Figure 2 – Protected storage or transfer of a data item

7.1.1 Architectural placement of security transformations in OSI upper layers

A security transformation operates in the context of a security association between two or more systems. There is a System Security Object (SSO) in each system, supporting such a security association. These SSOs perform the security transformation encoding/decoding processes (e.g. encipherment, digital signature generation/verification), and store necessary security state information (e.g. keys, algorithms, parameters, chaining state). The internal behaviour of such SSOs is governed by specific security transformation specifications, together with supporting specifications, e.g. for algorithms (which are outside the scope of this Recommendation | International Standard). In terms of Figure 2, the functions indicated in boxes b) and e) are modeled in SSOs.

There are also Security Communication Functions (SCFs) in the presentation entities of encoding and decoding systems. These SCFs support the communication requirements of the SSOs. In terms of Figure 2, the functions indicated in boxes a), c), d) and f) are modeled in SCFs. Definitions of SCF behaviour are contained in clause 8 of this Recommendation | International Standard, and in ITU-T Rec. X.833 | ISO/IEC 11586-4.

7.1.2 Security associations

A security transformation may be applied repeatedly to a sequence of logically-ordered data values, e.g. presentation data values transferred sequentially in one direction between two systems. The same protection is applied to each data value. Application of a security transformation to such a sequence is governed by a security association. More than one security association may exist at the same time between a pair of systems, typically providing different types of protection.

This Recommendation | International Standard addresses aspects of a security association which are relevant to upper layers communications or information storage. From the OSI upper layers perspective, a security association is a form of ASO-association.

Three kinds of security association are recognized by this Recommendation | International Standard:

- a) *externally-established security association* – A security association which is established independently of instances of its use, and which has a globally-unique identifier enabling it to be referenced at the time of use. The means of establishing such a security association are not specified in this Recommendation | International Standard, and its lifetime is not restricted by provisions in this Recommendation | International Standard. The identifier of an externally established security association comprises an integer value, together with the identity of the system assigning that integer value. (The latter identity may be known implicitly, e.g. the sender or receiver of data, hence this identity need not always be carried in protocol.)
- b) *single-item-bound security association* – A security association applying to a single independently-protected presentation data value which is not associated with a presentation context; attributes of the security association are indicated explicitly along with the presentation data value encoding. The lifetime of a single-item-bound security association is limited to the lifetime of the one presentation data value.
- c) *presentation-context-bound security association* – A security association which is established in conjunction with the establishment of a protecting presentation context, and which applies to all presentation data values sent in one direction in that protecting presentation context; attributes of the security association are indicated explicitly along with the encoding of the first presentation data value in the protecting presentation context. This type of security association can apply only when protection is provided in conjunction with use of the OSI presentation service and protocol specified in ITU-T Rec. X.216 | ISO/IEC 8822 and ITU-T Rec. X.226 | ISO/IEC 8823-1 respectively. The lifetime of the security association is the same as the lifetime of the corresponding protecting presentation context.

The operation of a security transformation may be governed by local security state information and/or by parameters which are transferred or stored with encoded data values. Local security state information may be maintained from one application of a security transformation to its next application, in the one security association. For example, for transformations providing integrity of the sequence of presentation data values within a security association, state information such as an integrity sequence number or a cryptographic chaining value will be retained from one application of the transformation to the next. Values of static parameters (see 7.1.3) are also retained throughout a security association.

7.1.3 Security transformation parameters

When using a security transformation, parameter values may need to be conveyed between the encoding and decoding functions, along with the transformed data values. Parameters are of two types:

- a) *static parameters* – These parameters maintain constant values throughout a security association, and are specified by the encoder of data when or before the security transformation is first applied in a security association;
- b) *dynamic parameters* – The values of these parameters may change dynamically while the transformation is in use in a security association; the encoder of the data indicates such changes within the data stream.

Examples of static parameters are:

- identifier(s) of the algorithm(s) used in a security transformation;
- if necessary, the mode of operation of an algorithm;
- the key(s), or identifier(s) of key(s), to be used with the above-mentioned algorithm(s);
- if necessary, the value(s) of initialization vector(s).

An example of a dynamic parameter is a key which is changed after a certain period of use.

Parameter values may be encoded unprotected or may themselves require protection. Unprotected parameters are conveyed in explicit fields of the protecting transfer syntax which supports the security transformation. Protected parameters are considered as inputs to the security transformation encoding process, along with the value to be protected. The security transformation rules must stipulate how these parameters are represented, how their representation is combined with the encoded abstract syntax value, and how the result is processed to generate an ASN.1 data value for transfer or storage.

NOTE – As an example of conveying protected parameters, see the definition of the GULS SIGNED Security Transformation in D.4.

Parameter data (e.g. keys) required by security transformations may also be obtained by other means, including:

- earlier Application Layer protocol exchanges (e.g. a key derivation security exchange conveyed by the SESE);
- local means (e.g. manual insertion of keys).

7.1.4 Determination of initial encoding rules

The rules for the initial encoding (and final decoding) processes (modelled in boxes a) and f) of Figure 2 are determined in one of the following ways:

- a) a security transformation may provide for the conveying of an indication of initial encoding rules as a static (protected or unprotected) parameter of the security transformation;
- b) as a default, every security transformation specification identifies default initial encoding rules.

NOTE – When using digital signatures for non-repudiation, the transformed item (i.e. the signed data) may need to be stored in a recipient system and/or relayed to another entity. In such circumstances, knowledge of the initial encoding rules used in computing the signature needs to be preserved. For digital signatures, it is recommended that the default encoding rules identified in the security transformation specification be used. Then, the required knowledge can be preserved by storing/relaying the security transformation identifier along with the signature.

7.1.5 Use of security transformations on an OSI presentation-connection

The OSI Presentation Layer associates a transfer syntax with each abstract syntax used. When a security transformation is employed, the transfer syntax is denoted a protecting transfer syntax.

In accordance with CCITT Rec. X.208 | ISO/IEC 8824, presentation data values may be transferred either:

- a) within a negotiated presentation context; or
- b) (as an option when using ASN.1 EXTERNAL or EMBEDDED PDV notation) outside a presentation context.

In both cases, a presentation data value which is to be protected is represented using a protecting transfer syntax. A protecting transfer syntax defined in accordance with ITU-T Rec. X.833 | ISO/IEC 11586-4 supports the communication of static and dynamic security transformation parameters.

Case a) above involves a protecting presentation context. All presentation data values transferred in one direction within a protecting presentation context are protected using the same security transformation, and are governed by the one security association. When a protecting presentation context is established (using the procedures for establishing a presentation context specified in ITU-T Rec. X.216 | ISO/IEC 8822 and ITU-T Rec. X.226 | ISO 8823-1), then the first presentation data value in each direction in that presentation context shall either:

- a) reference an externally established security association; or
- b) define a new presentation-context-bound security association.

When a presentation data value is encoded outside a presentation context, then the presentation data value shall either:

- a) reference an externally established security association; or
- b) define a new single-item-bound security association.

On an OSI presentation connection, different security associations apply to each direction of flow. These security associations may use the same security transformation but are not required to do so.

NOTE – The above restriction (i.e. that, when using the OSI presentation protocol, different security associations apply to each direction of flow) ensures that there can be no common cryptographic state variables shared between the two directions of flow. If such shared state could exist, there would be a need for complex state-maintenance protocol elements in the Presentation Layer to handle such events as Session Layer resynchronization. In practice, it is likely that the separate security associations for the two directions will have common attributes derived from one encompassing security association.

7.1.6 Use of security transformations independently of OSI presentation protocol

Security transformations may be used independently of the OSI presentation protocol, e.g. for protection in storage. Concepts and procedures described in 7.1.2 through 7.1.5 apply, with the following restrictions.

All protected presentation data values are represented outside presentation contexts.

A single-item-bound security association or externally established security association may be employed. Presentation-context-bound security associations cannot apply. Where the protected information is not being exchanged but is being protected only for use by the originator, then security transformations may also be employed without security associations.

If an externally established security association is employed, the lifetime of the externally established security association must span the storage lifetime of the protected data.

7.2 Notation for specifying security transformations

Security transformation specifications include specifications of data items needing to be recognized by the protecting transfer syntax structure. For this purpose, the following ASN.1 information object class definition (see ITU-T Rec. 681 | ISO/IEC 8824-2) is provided:

```
SECURITY-TRANSFORMATION ::= CLASS
-- This information object class definition is for use when
-- specifying a particular instance of a security transformation.
{
    &sT-Identifier OBJECT IDENTIFIER UNIQUE,
    -- Identifier to be used in signalling the application
    -- of the particular security transformation
    &initialEncodingRules OBJECT IDENTIFIER
    DEFAULT {joint-iso-ccitt asn1 (1) ber-derived (2)
    canonical-encoding (0)},
    -- Default initial encoding rules to generate a bit
    -- string prior to applying the encoding process of a
    -- security transformation.
    &StaticUnprotectedParm OPTIONAL,
    -- ASN.1 type for conveying static unprotected parameters
    &DynamicUnprotectedParm OPTIONAL,
    -- ASN.1 type for conveying dynamic unprotected parameters
    &XformedDataType,
    -- ASN.1 type of the ASN.1 value produced by the security
    -- transformations encoding process
    &QualifierType OPTIONAL
    -- &QualifierType specifies the ASN.1 type of the qualifier
    -- parameter used with the PROTECTED-Q notation.
}
```

ISO/IEC 11586-1 : 1996 (E)

WITH SYNTAX

-- The following syntax is used to specify a particular security transformation.

```
{
  IDENTIFIER                                &sT-Identifier
  [ INITIAL-ENCODING-RULES                  &initialEncodingRules ]
  [ STATIC-UNPROT-PARM                      &StaticUnprotectedParm ]
  [ DYNAMIC-UNPROT-PARM                    &DynamicUnprotectedParm ]
  XFORMED-DATA-TYPE                        &XformedDataType
  [ QUALIFIER-TYPE                          &QualifierType ]
}
```

Examples of the use of this notation are given in Annex D.

The security transformation specification needs to also specify the following details (although no formal notation to support such specification is provided in this Recommendation / International Standard):

- *Encoding process* – A description of the transformation process applied, at the encoding end, to the unprotected item and the transferred protected parameters in order to generate the resultant transformed value (which is an ASN.1 value of type &XformedDataType).
- *Encoding process local inputs* – A list of locally-derived inputs to the encoding process.
- *Decoding process* – A description of the transformation process applied, at the decoding end, to the received or retrieved transformed value (which is of type &XformedDataType) in order to generate the resultant unprotected data bit string (if any) and the values of the transferred protected parameters.
- *Decoding process local inputs* – A list of locally-derived inputs to the decoding process.
- *Decoding process outputs* – A list of outputs of the decoding process (may or may not include a recovered value of the unprotected item).
- *Parameters* – A description of the semantic significance of all parameters, default values for parameters, and the circumstances under which dynamic parameter changes should occur.
- *Transformation qualifiers* – A description of rules applying to invoker-specified transformation qualifiers (if any) applying to this transformation.
- *Errors* – A description of error conditions which may be detected during the decoding process.

8 Abstract syntax notation for selective field protection

The following abstract syntax notation is for the specification of the abstract protection requirements for a selected ASN.1 data type. The protection required is mapped to one of a set of security transformations which provide (at an abstract level) the required form of protection. Some security transformations accept input qualifiers to control the operation of the required protection, for example, the identifier for the security association for which the protection is to be applied. For these cases, an extension of the basic notation is defined, to enable qualifiers to be specified by the user of the notation.

This clause specifies:

- a) the basic protected abstract syntax notation, for specifying abstract protection requirements for a selected field in an abstract syntax specification;
- b) the qualified protected abstract syntax notation, for specifying abstract protection requirements, along with an associated qualifier, for a selected field in an abstract syntax specification;
- c) the protection mapping notation, for specifying the possible mappings to one or more security transformations which provide the required protection.

8.1 Basic notation

In order to assist the writer of an abstract syntax in indicating selective field protection requirements, the following ASN.1 parameterized type (see ITU-T Rec. X.683 / ISO/IEC 8824-4) is defined:

PROTECTED {BaseType, PROTECTION-MAPPING: protectionReqd} ::= CHOICE

```

{
  dirEncrypt BIT STRING (CONSTRAINED BY {BaseType
    -- dirEncrypt is for use only with the
    -- dirEncryptedTransformation,
    -- and generates the same encoding as the
    -- X.509/9594-8 ENCRYPTED type--}),
  dirSign SEQUENCE
  {
    baseType BaseType OPTIONAL,
    -- must be present for dirSignedTransformation
    -- and must be omitted for
    -- dirSignatureTransformation
    algorithmId AlgorithmIdentifier,
    encipheredHash BIT STRING (CONSTRAINED BY
      {BaseType -- contains enciphered hash
        -- of a value of BaseType --})
  }
  -- dirSign is for use only with the
  -- dirSignedTransformation or
  -- dirSignatureTransformation, and generates
  -- the same encoding as the corresponding
  -- X.509/9594-8 SIGNED or SIGNATURE type--,
  noTransform [0] BaseType,
  -- noTransform invokes no security transformation.
  -- Subject to security policy, noTransform may be used
  -- if adequate protection is provided by lower layers
  -- and any application relays through which the data
  -- may pass are trusted to maintain the required
  -- protection. This alternative may only be used
  -- if protectionReqd.&bypassPermitted is TRUE,
  direct [1] SyntaxStructure
    {{protectionReqd.&SecurityTransformation}},
  -- direct generates a protecting transfer syntax
  -- value, which is encoded using the same encoding
  -- rules as the surrounding ASN.1 (The type
  -- SyntaxStructure is imported from Rec. X.833 |
  -- ISO/IEC 11586-4),
  embedded [2] EMBEDDED PDV (WITH COMPONENTS {
    identification (WITH COMPONENTS {
      presentation-context-id,
      context-negotiation (WITH COMPONENTS {
        transfer-syntax (CONSTRAINED BY
          {OBJECT IDENTIFIER :
            protectionReqd.&protTransferSyntax})),
        transfer-syntax (CONSTRAINED BY
          {OBJECT IDENTIFIER :
            protectionReqd.&protTransferSyntax})),
      data-value (WITH COMPONENTS {notation (BaseType)})
    })
    -- The data value encoded is a value of type BaseType
  })
}
-- BaseType is the type to be protected, and protectionReqd is an ASN.1
-- object of class PROTECTION-MAPPING. The use of PROTECTED requires
-- the importation into the user's module of the PROTECTED parameterized
-- type, together with the necessary PROTECTION-MAPPING object
-- definition.

```

The PROTECTION-MAPPING object class and its significance are discussed in 8.3. The set of allowable objects for "protectionReqd" will vary in different abstract syntax specifications, dependent upon the range of distinct transformations required. The mappings from PROTECTION-MAPPING objects to transformations are contained in a set of PROTECTION-MAPPING object definitions. This set of definitions may be specified in a separate ASN.1 module from the (mechanism-independent) abstract syntax specification and from the (application-independent) transformation definition.

ISO/IEC 11586-1 : 1996 (E)

The various alternatives in the CHOICE are made available for use in different circumstances as follows:

- *dirEncrypt* and *dirSign* – These alternatives generate the &XformedDataType of the security transformation used. These alternatives are made available to provide a means whereby the PROTECTED notation can generate identical bit-encodings to the ENCRYPTED, SIGNED, and SIGNATURE parameterized types defined in ITU-T Rec. X.509 | ISO/IEC 9594-8.
- *noTransform* – This alternative uses no security transformation. It is permitted if the protection mapping in use (see 8.3 and 8.4) indicates &bypassPermitted = TRUE. The item is encoded in its unprotected form. According to security policy, noTransform may be used if adequate protection is provided by lower layers and any application relays through which the data may pass are trusted to maintain the required protection.
- *direct* – This alternative directly imports a protecting transfer syntax value, as defined in ITU-T Rec. X.833 | ISO/IEC 11586-4, into the encompassing ASN.1 specification. It supports use of an externally established security association or single-item-bound security association. It does not permit use of a negotiated presentation context. The encoding rules used for encoding the protecting transfer syntax structure [modelled in boxes c) and d) of Figure 2 in 7.1] are forced to be the same as those used for the ASN.1 type encompassing the PROTECTED notation.
- *embedded* – This alternative provides the greatest flexibility, including the ability to associate protection with a negotiated presentation context and the ability to use a different protecting transfer syntax to that defined in ITU-T Rec. X.833 | ISO/IEC 11586-4.

NOTE – It is recommended that use of these options be selected as follows:

- a) Use the direct option if none of b), c) or d) applies.
- b) When requiring bit-compatibility with the ENCRYPTED, SIGNED, or SIGNATURE parameterized types for backward-compatibility reasons, use the dirEncrypt or dirSign option as applicable.
- c) When the protection mapping in use indicates &bypassPermitted = TRUE and when security policy permits, use the noTransform option.
- d) When there is a requirement to associate protection with a negotiated presentation context, use the embedded option.

Error conditions may be detected in the decoding system in processing a value in a protected field. The ASN.1 exception handling notation defined in ITU-T Rec. X.682 | ISO/IEC 8824-3 can be used to deal with such error conditions.

Examples of the use of this notation appear in I.1.

8.2 Notation with transformation qualifier

As an alternative to the PROTECTED notation described in 8.1, the PROTECTED-Q notation allows its user to additionally provide a qualifier parameter. These qualifier parameters are used for one or both of the following purposes:

- a) to identify a specific externally established security association;
- b) to provide one or more parameters for use by the security transformation, e.g. algorithm, mode of operation, and/or key identifiers.

NOTE – Some algorithm identifiers may imply a particular mode of operation. In other cases, the mode of operation may be specified as an additional parameter.

Multiple qualifiers may be specified using an appropriate ASN.1 SEQUENCE or SET type. Within the encoding system, a qualifier is used by local system functions to determine the appropriate SSO and/or to convey a parameter to that SSO. A qualifier conveyed to a SSO needs to be compatible with the security transformation in use, as stated in the security transformation specification. When the specified protection mapping permits a choice of security transformations, the one selected for any instance of use must be one with a &QualifierType consistent with the value specified by the user of the PROTECTED-Q notation. The value of the qualifier may be (but is not necessarily) conveyed to the decoding system within the protecting transfer syntax (e.g. as the externally established security association identifier, or as a security transformation parameter).

The following ASN.1 parameterized type (see ITU-T Rec. X.683 | ISO/IEC 8824-4) is defined:

```
PROTECTED-Q {BaseType, PROTECTION-MAPPING: protectionReqd,
PROTECTION-MAPPING.&SecurityTransformation.&QualifierType: qualifier} ::=
PROTECTED {BaseType, protectionReqd} (CONSTRAINED BY
{PROTECTION-MAPPING.&SecurityTransformation.&QualifierType: qualifier
-- The value of qualifier must be made available to
-- the security transformation used
})
```