INTERNATIONAL STANDARD

ISO/IEC 10745

First edition
1995-08-15

Information technology — Open Systems Interconnection — Upper layers security model

Technologies de l'information — Interconnexion de systèmes ouverts — Modèle de sécurité pour les couches hautes

Reference number
ISO/IEC 10745:1995(E)

CONTENTS

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 10745 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.803.

Annexes A and B of this International Standard are for information only.

Introduction

The OSI Security Architecture (CCITT Rec. X.800 | ISO 7498-2) defines the security-related architectural elements which are appropriate for application when security protection is required in an open systems environment.

This Recommendation | International Standard describes the selection, placement, and use of security services and mechanisms in the upper layers (Application, Presentation, and Session Layers) of the OSI Reference Model.

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – UPPER LAYERS SECURITY MODEL

1 Scope

1.1 This Recommendation | International Standard defines an architectural model that provides a basis for:

a) the development of application-independent services and protocols for security in the upper layers of OSI; and

b) the utilization of these services and protocols to fulfil the security requirements of a wide variety of applications, so that the need for application-specific ASEs to contain internal security services is minimized.

1.2 In particular, this Recommendation | International Standard specifies:

a) the security aspects of communication in the upper layers of OSI;

b) the support in the upper layers of the security services defined in the OSI Security Architecture and the Security Frameworks for Open Systems;

c) the positioning of, and relationships among, security services and mechanisms in the upper layers, according to the guidelines of CCITT Rec. X.800 | ISO 7498-2 and ITU-T Rec. X.207 | ISO/IEC 9545.

d) the interactions among the upper layers, and interactions between the upper layers and the lower layers, in providing and using security services;

e) the requirement for management of security information in the upper layers.

1.3 With respect to access control, the scope of this Recommendation | International Standard includes services and mechanisms for controlling access to OSI resources and resources accessible via OSI.

1.4 This Recommendation | International Standard does not include:

a) definition of OSI services or specification of OSI protocols;

b) specification of security techniques and mechanisms, their operation, and their protocol requirements; or

c) aspects of providing security which are not concerned with OSI communications.

1.5 This Recommendation | International Standard is neither an implementation specification for systems nor a basis for appraising the conformance of implementations.

NOTE – The scope of this Recommendation | International Standard includes security for connectionless applications and for distributed applications (such as store-and-forward applications, chained applications, and applications acting on behalf of other applications).

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 entities to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent editions 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.811[1)] (1993) | ISO/IEC 10181-2....[1)], *Information technology – Security frameworks in Open Systems: Authentication framework.*
- ITU-T Recommendation X.812[1)] (1993) | ISO/IEC 10181-3....[1)], *Information technology – Security frameworks in Open Systems: Access control framework.*

2.2 Paired Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.200 (1988), *Basic reference model of open systems interconnection for CCITT applications.*

  ISO 7498:1984/Corr.1:1988, *Information processing systems – Open Systems Interconnection – Basic Reference Model.*
- CCITT Recommendation X.216 (1988), *Presentation service definition for open systems interconnection for CCITT applications.*

  ISO 8822:1988, *Information processing systems – Open Systems Interconnection – Connection oriented presentation service definition.*
- CCITT Recommendation X.217 (1988), *Association control service definition for open systems interconnection for CCITT applications.*

  ISO 8649:1988, *Information processing systems – Open Systems Interconnection – Service definition for the Association Control Service Element.*
- CCITT Recommendation X.700 (1992), *Management framework definition for Open Systems Interconnection for CCITT applications.*

  ISO/IEC 7498-4:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 4: Management framework.*
- 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 terms are used as defined in CCITT Rec. X.200 | ISO 7498:

a) abstract syntax;

b) application-entity;

c) application-process;

d) application-process-invocation;

c) application-protocol-control-information;

f) application-protocol-data-unit;

g) local system environment;

h) (N)-function;

i) (N)-relay;

j) open system;

k) presentation context;

l) presentation-entity;

---

1) Presently at stage of draft.

m) real open system;

n) systems-management;

o) transfer syntax.

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

a) access control;

b) authentication;

c) confidentiality;

d) data integrity;

e) data origin authentication;

f) decipherment;

g) encipherment;

h) key;

i) non-repudiation;

j) notarization;

k) peer-entity authentication;

l) security audit;

m) Security Management Information Base;

n) security policy;

o) selective field protection;

p) signature;

q) traffic flow confidentiality;

r) trusted functionality.

3.3 The following terms are used as defined in CCITT Rec. X.700 | ISO/IEC 7498-4:

a) Management Information;

b) OSI Management.

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

a) application-association;

b) application-context;

c) application-entity-invocation (AEI);

d) application-service-element (ASE);

e) ASE-type;

f) application-service-object (ASO);

g) ASO-association;

h) ASO-context;

i) ASO-invocation;

j) ASO-type;

k) control function (CF).

3.5 The following term is used as defined in CCITT Rec. X.216 | ISO 8822:

– presentation data value.

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

a) authentication exchange;

b) claim authentication information;

c) claimant;

d) exchange authentication information;

e) entity authentication;

f) principal;

g) verification authentication information;

f) verifier.

3.7 The following terms are used as defined in ITU-T Rec. X.812 | ISO/IEC 10181-3:

a) access control certificate;

b) access control information.

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

association security state: Security state relating to a security association.

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

protecting transfer syntax: A transfer syntax based on encoding/decoding processes that employ a security transformation.

seal: A cryptographic check value that supports integrity but does not protect against forgery by the recipient (i.e. it does not support non-repudiation).

security association: A relationship between two or more entities for which there exist attributes (state information and rules) to govern the provision of security services involving those entities.

security communication function: A function supporting the transfer of security-related information between open systems.

security domain: A set of elements, a security policy, a security authority and a set of security relevant activities in which the set of elements are subject to the security policy, administered by the security authority, for the specified activities.

security exchange: A transfer or sequence of transfers of application-protocol-control-information between open systems as part of the operation of one or more security mechanisms.

security exchange item: A logically-distinct piece of information corresponding to a single transfer (in a sequence of transfers) in a security exchange.

security exchange function: A security communication function, located in the Application Layer, that provides the means for communicating security information between AE-invocations.

secure interaction rules: Common aspects of the rules necessary in order for interactions to take place between security domains.

security state: State information that is held in an open system and that is required for the provision of security services.

system security function: A capability of an open system to perform security-related processing.

system security object: An object that represents a set of related system security functions.

security transformation: A set of functions (system security functions and security communication functions) which, in combination, operate upon user data items to protect those data items in a particular way during communication or storage.

NOTE – Specifications of system security functions and system security object are not part of OSI layer service definitions or protocol specifications.

4 Abbreviations

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

ACSE Association control service element

AE Application-entity

AEI Application-entity-invocation

ASE	Application-service-element
ASN.1	Abstract Syntax Notation One
ASO	Application-service-object
CF	Control function
FTAM	File transfer, access and management
OSI	Open Systems Interconnection
PE	Presentation-entity
PEI	Presentation-entity-invocation
PDV	Presentation data value
SEI	Security exchange item
SSO	System security object

5 Concepts

This Security Model addresses the provision of security services to counter threats relating to the upper layers of OSI such as those described in Annex A of CCITT Rec. X.800 | ISO 7498-2. It includes protection of information passing through application-relay systems.

5.1 Security policy

If two or more real open systems are to communicate securely, they must be subject to the security policies in effect in their respective security domains, as well as a secure interaction policy if communication is to take place between different security domains. A secure interaction policy embodies the common aspects of security policies in different security domains and determines the conditions under which communications between them can take place.

The provisions of a secure interaction policy can be described by a set of secure interaction rules. These rules govern, amongst other things, the selection of ASO-contexts (including application-contexts) to be used for particular instances of communication.

5.2 Security associations

A security association is a relationship between two or more entities for which there exist attributes (state information and rules) to govern the provision of security services involving those entities. A security association implies the existence of secure interaction rules, and the maintenance of consistent security state in both systems.

From the OSI upper layers perspective, a security association maps to an ASO-association. Two special cases are:

- *application-association security association* – A security association between two systems to support protected communication via an application-association;
- *relay security association* – A security association between two systems to support protected communication via an application-relay (e.g. in store-and-forward or chaining applications);

Other examples of different types of security associations are:

- a security association between two systems which communicate directly with each other via multiple application-associations and/or the the communication of multiple connectionless data units;
- a security association between an entity writing protected information to a data store (e.g. a file store or directory) and entities reading that information;
- a security association between two peer lower layer security protocol entities.

Within an application-process, one security association may be dependent upon the maintenance of another security association with another system, such as an authentication server or other type of trusted third party.

5.3 Security state

Security state is state information that is held in a real open system and that is required for the provision of security services. Existence of a security association between application-processes implies the existence of shared security state.

Certain security state information may be required to be available to one or more application-processes prior to attempting to establish communications, maintained while these communications are active, and/or retained after the end of communications. The exact nature of this state information depends upon the particular security mechanisms and applications.

Two categories of security state are:

a) *System security state* – Security-related state information that is established and maintained in a real open system, regardless of the existence or state of any communication activities;

b) *Association security state* – Security state relating to a security association. In the OSI upper layers, the shared security state governs the (security properties of) ASO-contexts used between ASO-invocations and/or the initial security state of newly established application-associations. Two special cases are:

   – when the security association maps to a single application-association – The security state is denoted **application-association security state**. It pertains to the control of communications security for that application-association.

   – when the security association maps to an ASO-association which involves information transfer between two end-user systems via an application-relay system – The shared security state pertains to the use of security mechanisms between the end-user systems, independently of security mechanisms relating to individual application-associations established with the application-relay system.

Examples of security state include:

a) state information associated with cryptographic chaining or integrity recovery;

b) the set of security labels for information permitted to be exchanged;

c) key(s) or key identifier(s) to be employed in the provision of security services in the upper layers. This might include keys for known trusted certification authorities (see CCITT Rec. X.509 | ISO/IEC 9594-8 Directory Authentication Framework), or keys enabling communications with a key distribution centre;

d) previously authenticated identities;

d) sequence numbers and cryptographic synchronization variables.

Security state may be initialized in various ways, such as:

a) using a security management function, in which case the state information resides in the Security Management Information Base;

b) as residual information from previous communication activities;

c) means outside of OSI.

5.4 Application Layer requirements

In order for application-processes to engage in secure communications, they must have the appropriate security provisions in the ASO-context (or application-context) in use.

An ASO-context definition may include:

a) the ASO-types and/or ASE-types required to support the security protocols;

b) rules for the negotiation and selection of security functions related to the Application and Presentation Layers;

c) rules for the selection of underlying security services;

d) rules for applying particular security services to particular categories of information to be exchanged;

e) rules for re-authenticating relevant identities during the lifetime of an association;

f) rules for changing keys throughout the lifetime of an ASO-association (if cryptographic-based mechanisms are used);

g) rules to be followed in the event of communications failures or detected security violations.

NOTE – An ASO-context may be defined by reference to an ASO-type definition.

An application-context is the particular case of an ASO-context that describes the permissible collective communications behaviour of two ASO-invocations that are party to an application-association. The security aspects described in 5.4.1 apply to application-contexts.

6 Architecture

6.1 Overall model

The provision of OSI security services involves the generation, exchange, and processing of security information according to the procedures of specific security mechanisms. Two distinct types of function are involved:

a) *System security function* – A capability of a system to perform security-related processing, such as encipherment/decipherment, digital signature, or the generation or processing of a security token or certificate conveyed in an authentication exchange. The realization of such functions is not part of the realization of OSI layer services or protocols.

b) *Security communication function* – A function supporting the transfer of security-related information between open systems. Such functions are realized in OSI application-entities or presentation-entities. Examples of security communication functions are:

- security exchange functions, as described in 6.3;
- the encoding/decoding of Presentation Layer protocol elements designed to convey enciphered or digitally signed information;
- protocols for communicating with a security server, e.g. an authentication server or key distribution centre.

The distinction between system security functions and security communication functions is significant in two respects. Firstly, it delineates two different types of standard. System security functions are specified in security mechanism or security technique standards. These standards are usually designed to be general-purpose in nature and are not necessarily linked to any particular communication protocol or layer. System security function standards are possibly useful for purposes other than communications security. Security communication functions, on the other hand, are part of particular communications protocol specifications (e.g. OSI upper layers) and are not necessarily linked to particular security mechanisms or techniques.

The other significance of the distinction is that it models the separation between security functionality and communications functionality in an implementation. A collection of system security functions will typically be implemented as a secure module, e.g. as a trusted software subsystem or a tamper-proof hardware module, potentially applicable in a variety of communications or other environments. Hence, the boundary between system security functions and security communications functions may provide a valuable starting point for the definition of standardized implementation interfaces, e.g. a security application program interface (API).

For architectural purposes, the concept of a **system security object** (SSO) is introduced. An SSO is an object that represents a set of related system security functions.

SSOs can interact with security communication functions, through an abstract service boundary (interface), to provide the required security service(s). SSOs generate and process security information exchanged using OSI protocols in the Application and Presentation Layers. The logical structure of exchanged security information can be standardized in OSI so it can be represented in OSI protocol exchanges.

An SSO-invocation is an instance of execution of an SSO. In a dynamic model, an SSO-invocation may interact with an OSI entity invocation, e.g. an AE-invocation.

The operation of an SSO may include:

- accepting information from and providing information to OSI security communication functions, which may send and/or receive information on behalf of the SSO;
- causing an application-association to be established with another open system, e.g. a third party authentication server, and using that application-association in the provision of the SSO's system security functions;
- establishing a security association to be used subsequently in the provision of a security service.

NOTE 1 – The specification of particular system security functions, SSOs or abstract service boundaries is beyond the scope of this Security Model.

NOTE 2 – Realizations of SSOs may be used for purposes other than OSI security, however any such use is outside the scope of this Security Model.

Figure 1 shows a basic model for security functions associated with the Application and Presentation Layers. Objects in the model include application-entities (AEs), presentation-entities (PEs), SSOs, and supporting OSI services (in OSI layers 1 through 5). Supporting OSI services provide the basic communications infrastructure for exchanging security-related (as well as non-security-related) information.

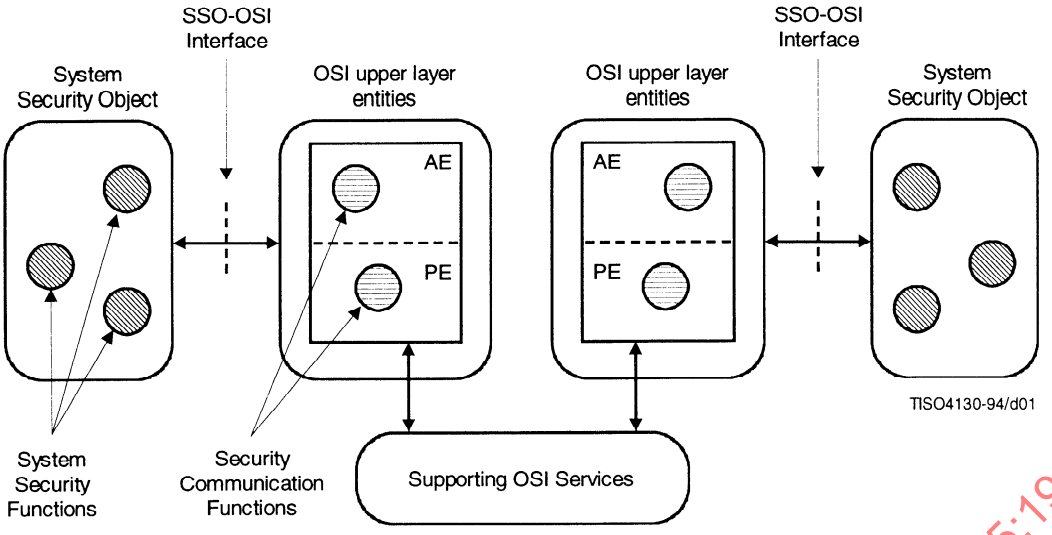

Figure 1 – Security functions associated with the OSI upper layers

OSI layer entities in the upper layers contribute to the provision of security services as follows:

- In the Application Layer, AEs model the communications aspects of application-processes and can be refined in terms of ASEs, ASOs, and control functions as described in CCITT Rec. 207 | ISO/IEC 9545. An AE may contain ASEs and/or ASOs dedicated to the provision of security communication functions. ASEs and/or ASOs may also arrange for information to be protected by the use of security transformations (see 6.4), and/or by requesting an appropriate quality-of-service from underlying layers.
- In the Presentation Layer, security communication functions are provided by the presentation-entity. These functions may work in conjunction with system security functions (e.g. encipherment) used in mapping an abstract syntax to a transfer syntax (see 6.4).
- In the Session Layer, no security services are provided. However, 6.2.1 notes some aspects of Session Layer operation that may have an impact on security provisions within the OSI environment.

The above basic model facilitates the generic definition of abstract service boundaries between OSI components and SSOs, and allows various trust schemes to be accommodated (e.g. as specified in ITU-T Rec. X.811 | ISO/IEC 10181-2 Authentication Framework).

NOTE 3 – Interactions between an AE and PE as shown in Figure 1 are discussed in 6.4 and 8.1.

6.2 Security associations

In the upper layers, a security association maps to an ASO-association. This Security Model does not stipulate specific means for establishing or terminating security associations. In general, such establishment/termination may be achieved in conjunction with standardized ASO-association establishment processes or may be achieved by other means. Special architectural considerations apply to the two special types of security association identified in 5.2.

6.2.1 Application-association security association

An application-association security association maps to one application-association. Security services may be realized through the use of:

a) security communication functions in the Application Layer, and associated system security functions;

b) security communication functions in the Presentation Layer, and associated system security functions;

c) security services provided by the Lower Layers.

NOTE 1 – As indicated in CCITT Rec. X.800 | ISO 7498-2, there are no security mechanisms in the Session Layer. However, two aspects of Session Layer operation need to be taken into account in the design of upper layers security protocols: the potential effect of using session services that may result in non-delivery of data (see 8.2), and the serial reuse of transport connections to support several session connections (see 8.3).

In some cases a combination of security communication functions in the Application and Presentation Layers, and associated system security functions, may be required to provide a security service.

The security services and security mechanisms to be used on an application-association are specified by the application-context. These security services may be provided by the use of functions associated with one or more ASEs and/or ASOs, either separately or in combination.

The security requirements for an application-association need to be taken into account during association establishment in either or both of the following ways:

a) through the use of security services to protect application-association establishment;

b) through the selection of an application-context which includes appropriate security services.

Services provided by ACSE are used to establish an application-association and to select a suitable application-context. The rules of the selected application-context may include security-related rules. Such rules may require that other ASEs, which may (among other things) provide security services, operate in conjunction with ACSE during association establishment.

NOTE 2 – Security communication functions in the Presentation Layer, and associated system security functions, may be used as part of the application-association establishment procedure.

The initial association security state is determined by the application-association establishment procedure. It may depend upon the system security state and/or the association security state of any encompassing security association. The rules of the application-context may permit, or require, further protocol exchanges between ASEs to change this association security state. Such changes may take place both as part of initialization procedures following application-association establishment and/or as an integral part of the normal operation of cooperating AE-invocations.

The modification of some kinds of security state information may be permitted during the lifetime of a security association (e.g. integrity sequence numbers). The modification of other kinds of security state information may not be allowed (e.g. security labels).

Services provided by ACSE are used to terminate an application-association. The rules of the application-context of the application-association may require that other ASEs, which may (among other things) provide security services, operate in conjunction with ACSE during application-association termination.

6.2.2 Relay security associations

A relay security association may arise in a distributed application such as a store-and-forward application or a chaining application. A relay security association potentially occurs in conjunction with application-association security associations as illustrated in Figure 2.

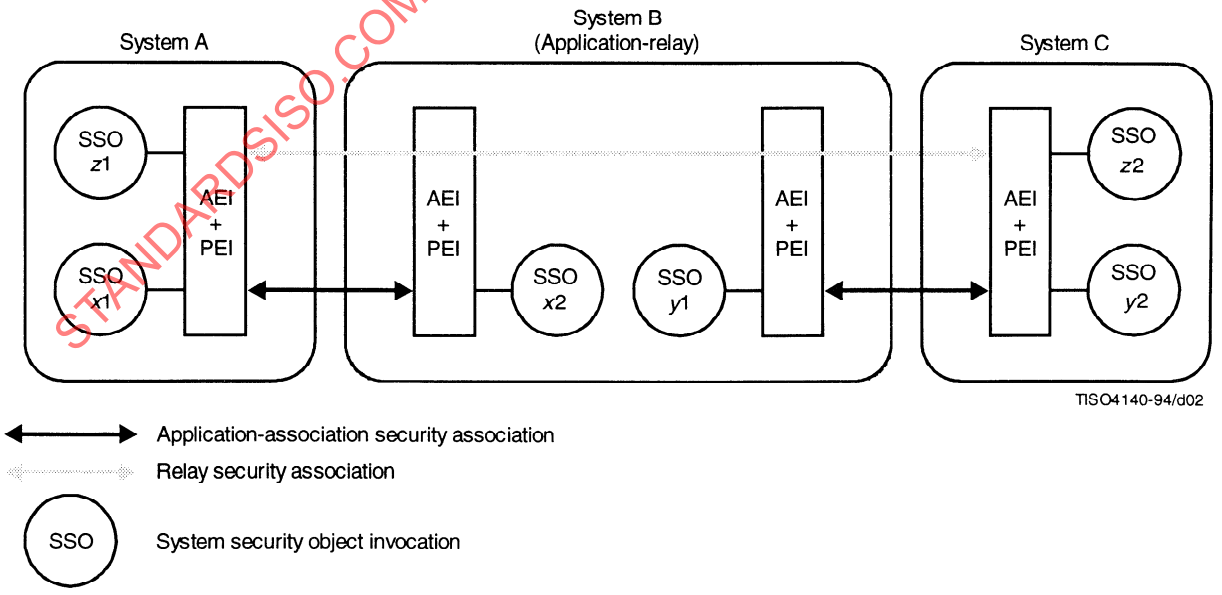

Figure 2 – Application relay scenario

Protected relayed information is information conveyed between the parties to the relay security association (system A and system C in Figure 2). The protection is provided using system security functions in SSOs $z1$ and $z2$. The protected relayed information is embedded in PDVs conveyed in an application-association between systems A and B, and is also embedded in PDVs conveyed in an application-association between systems B and C. When protected relayed information is conveyed in an application-association, it may be subjected to further security protection, e.g. that using security functions in SSOs $x1$ and $x2$ when conveyed between systems A and B. This occurs when the PDV conveying protected relayed information is embedded in another PDV which is protected in accordance with an application-association security association.

The application-relay system may not possess the necessary arguments (e.g. cryptographic keys) to enable the presentation-entity(s) in that open system to decode/encode the presentation data values conveying the protected relayed information. In an open system of this type, encoded presentation data values may be retained for later transmission. The later transmission is restricted to a presentation context with the same abstract and transfer syntax as that in which the presentation data value was received. Hence, information identifying the abstract syntax and transfer syntax must be preserved together with the encoding within the relay system.

A variation of the above may arise when the relay system possesses the information necessary to decode the relayed information. For example, it may possess a public key which it uses to verify a signature on that information (e.g. in support of data origin authentication). However, it may be necessary to relay the signed information on to another system, in which case the encoding needs to be preserved as described above.

6.3 Security exchange functions

A security exchange function is a type of security communication function, located in the Application Layer, that provides the means for communicating security information between AE-invocations. A security exchange function generates and processes application-protocol-control-information to support communication of this information.

These functions are provided by ASOs or ASEs.

An example of such a function is the communications support for an authentication exchange as described in ITU-T Rec. X.811 | ISO/IEC 10181-2, where an item of exchange authentication information generated at a claimant AE-invocation is conveyed to a verifier AE-invocation.

6.3.1 Security exchanges

A security exchange models the transfer of application-protocol-control-information between open systems as part of the operation of a security mechanism.

A security exchange may involve either of:

a) the transfer of a single piece of information between one open system and another; for example:
   - an access control certificate;
   - a public-key certificate; or
   - a security token.

b) a sequence of transfers of information between open systems, with the entire sequence forming part of the operation of one security mechanism; for example:
   - transfers of information associated with a 2-way or 3-way authentication exchange; or
   - 2-way session-key negotiation [e.g. Diffie-Hellman exponential key exchange[2)]].

Different types of security exchange are assigned unique identifiers to allow their use to be indicated in protocol.

6.3.2 Security exchange information

Security exchange information is the information communicated between open systems in a security exchange.

The logically-distinct piece of security exchange information corresponding to a single transfer (possibly in a sequence of transfers) is called a **security exchange item** (SEI). For data definition purposes, one SEI may be decomposable into smaller elements.

---

2) DIFFIE (W.), HELLMAN (M.): New Directions in Cryptography, *IEEE Transactions on Information Theory*, Vol. IT-22, No. 6, pp. 644-654, 1976.

While no particular abstract syntax notation is stipulated for defining security exchange information, the construction of a complete abstract syntax containing security exchange information will be facilitated if the same notation is used for that information as for the rest of the abstract syntax. ITU-T Rec. X.830 | ISO/IEC 11586-1 provides notational tools for use with ASN.1 notation.

6.3.3 Provision of security exchange functions

To provide support for a security exchange in any given ASO-context, it is necessary to incorporate the function of the security exchange into some ASE and/or ASO in that ASO-context. This involves:

a) incorporating the SEI type definitions into an abstract syntax;

b) incorporating any procedural or other rules regarding operation of the security exchange into an ASE-type or ASO-type definition, or elsewhere in the ASO-context definition;

c) if necessary, incorporating the definition of coordination rules related to the security exchange into the specification of a CF.

In general, security exchanges may be incorporated into any ASE and/or ASO, and SEI definitions should be expressed so as to facilitate their incorporation into as many different ASEs and/or ASOs as possible.

ITU-T Rec. X.831 | ISO/IEC 11586-2 and ITU-T Rec. X.832 | ISO/IEC 11586-3 define an ASE designed specifically for conveying security exchanges.

6.4 Security transformations

A security transformation is a set of functions (system security functions and security communication functions) that, in combination, operate upon user data items to protect those data items in a particular way during communication or storage.

Security transformations involve security-related processing of user information conveyed by OSI upper layers protocols. They may constitute the primary means of providing a confidentiality, integrity, or data origin authentication service and/or may contribute to the provision of other security services including entity authentication, access control, and non-repudiation.

Security transformations employ system security functions of various types, such as:

a) encipherment/decipherment functions (e.g. for confidentiality services);

b) sealing or signing functions (e.g. for integrity or data origin authentication services).

A security transformation may employ a single system security function or multiple system security functions of different types in combination. When system security functions are applied in combination, there is no architectural restriction as to which type needs to be applied first.

Security transformations also employ security communication functions located within the upper layers.

NOTE 1 – The examples a) and b) above do not provide an exhaustive list of system security function types.

NOTE 2 – It is desirable to limit the number of system security function types defined, and apply them to a wide range of security needs.

NOTE 3 – Security communication functions forming part of security transformations deal with representations of information, so are logically associated with the Presentation Layer. However, these functions are applied at a variety of different granularities. They are sometimes applied to complete presentation data values as recognized by the presentation protocol. They are sometimes applied to selected fragments of Application Layer information. In the latter case, from an implementor's perspective, it may be more convenient to view these security communication functions as if they are within the Application Latyer.

Different types of security transformation are assigned unique identifiers to allow their use to be indicated in protocol.

A specification indicating use of security transformations may need to include:

a) an indication of the particular security transformation or the means by which the particular security transformation will be determined;

b) specification of the information item(s) to which the security transformation is to apply;

c) if an information item to be protected is specified at an abstract syntax level, it may be necessary to also identify encoding/decoding rules to be applied prior/subsequent to applying a security transformation;

d) identification of algorithm(s) to be employed, and the sources of any required parameters, e.g. keys.

NOTE 4 – Encoding/decoding rules used in generating/checking integrity check-values or digital signatures must have the property that there is a one-to-one mapping between abstract information value and encoded value. The ASN.1 Distinguished and Canonical Encoding Rules have this property but the ASN.1 Basic Encoding Rules do not.

There are two ways of specifying the information items to which security transformations are to apply:

a) selected fields are indicated within an abstract syntax specification;

b) a security transformation of a particular type is associated with all information items transferred in one presentation context; in this case, security transformation requirements are specified outside abstract syntax specifications.

These two cases are expanded upon below.

6.4.1 Selective field indication in abstract syntax specification

When protection is to be applied to selected fields within an abstract syntax, the abstract syntax specification must indicate the items to be protected using suitable notation. This approach is needed if selective field confidentiality and/or integrity is to apply at a granularity smaller than that of the complete presentation data values generated by an abstract syntax.

Examples of notations for specifying the selective use of security transformations in an abstract syntax are the signing and enciphering functions defined in ITU-T Rec. X.509 | ISO/IEC 9594-8 and the PROTECTED notation defined in ITU-T Rec. X.830 | ISO/IEC 11586-1.

6.4.2 Protecting Presentation Contexts

When a security transformation is to be applied uniformly to all information items of an abstract syntax, this involves the establishment and use of a **protecting presentation context**.

Establishment of any presentation context involves establishing a transfer syntax to be used with a given abstract syntax. With a protecting presentation context, the transfer syntax, which is called a **protecting transfer syntax**, is based on encoding/decoding processes that employ a security transformation. Establishment of the protecting presentation context includes determining the security transformation (and implied system security function(s)) that will form part of the processes of encoding/decoding between abstract syntax and transfer syntax on transmission/reception of all presentation data values in that presentation context.

After a protecting presentation context is established, a system security function which processes outgoing data may need to convey parameter information to its corresponding system security function. This might include, for example:

a) on the first usage of a presentation context, initial parameters such as the initialization vector of a cryptographic process, or identifier(s) of key(s);

b) within a sequence of protected presentation data values, information signaling a parameter change, e.g. a change to a new key.

The definition of a protecting transfer syntax may therefore need to accommodate the means for conveying transformation parameter data in addition to conveying representations of presentation-service-user information.

Parameter information, e.g. keys, required by system security functions may alternatively be obtained by such means as:

a) a result of earlier Application Layer protocol exchanges, e.g. a key resulting from a key derivation security exchange;

b) local means, e.g. manual insertion of keys.

ITU-T Rec. X.833 | ISO/IEC 11586-4 specifies a generic protecting transfer syntax, capable of supporting a variety of different security transformations.

NOTE – It is possible to embed one presentation data value within another and security transformations can be applied at both levels. In this case, the encoding of the inner (embedded) presentation data value (for which a security transformation is used in the encoding process) will also be protected under the security transformation applying to the encoding of the outer presentation data value. An example might be when data (comprising an inner presentation data value) forwarded between two systems needs to be signed in order to prove the origin of the data, and when protection against replay between two systems is achieved by sealing applied to an outer presentation data value or all presentation data values in a presentation context.

7 Services and mechanisms

The OSI Security Architecture (CCITT Rec. X.800 | ISO 7498-2) specifies that:

– the Application Layer may provide one or more security services from the basic set: authentication, access control, confidentiality, data integrity, and non-repudiation.

– the Presentation Layer does not provide security services, but security mechanisms to support the provision of Application Layer security services may be located at the Presentation Layer;

– the Session Layer does not provide security services and contains no security mechanisms.

7.1 Authentication

7.1.1 Entity Authentication

7.1.1.1 Role of upper layers in entity authentication

The purpose of authentication is to provide assurance of the identity of an entity. It is the role of the Application Layer to provide for the authentication of entities known to the Application Layer. Such authentication is available both at the time of ASO-association establishment and during the use of an ASO-association.

The Application Layer allows for a wide range of principals to be authenticated. This depends upon the nature of the application and the security policy in effect.

NOTE – The concept of *peer-entity authentication* defined in CCITT Rec. X.800 | ISO 7498-2 is a special case of *entity authentication* as defined in ITU-T Rec. X.811 | ISO/IEC 10181-2.

The upper layers do not provide for authentication of any entities below the Application Layer.

7.1.1.2 Provision of entity authentication

Entity authentication can be provided in the Application Layer by the communication of exchange authentication information, which may employ security exchange functions in accordance with 6.3.

Entity authentication only provides assurance of an identity at an instant of time. To maintain this assurance throughout the duration of an ASO-association, use of a connection integrity service (as defined in CCITT Rec. X.800 | ISO 7498-2) is required. In some cases it may be necessary to obtain further assurance of the identity of an entity after a period of time through additional authentication exchanges.

7.1.1.3 Management of entity authentication

When providing entity authentication, management of claim authentication information and/or verification authentication information, e.g. cryptographic keys, may be required. As described in ITU-T Rec. X.811 | ISO/IEC DIS 10181-2, this may involve any of the following procedures:

- *installation*, in which claim authentication information and verification authentication information are defined;
- *change authentication-information*, in which a principal or a manager causes claim authentication information and verification authentication information to change;
- *distribution*, in which any entity may acquire sufficient verification authentication information upon which to verify exchange authentication information;
- *disable*, in which a state is established whereby a principal which previously could be authenticated is temporarily unable to authenticate;
- *re-enable*, in which the state established in a disable procedure is terminated;
- *deinstallation*, in which a principal is removed from the population of authenticatable principals.

When such procedures are implemented using OSI protocols, this may involve security exchange functions in accordance with 6.3. These procedures may also employ OSI Security Management services.

The security policy in force may also require that failed authentication attempts be reported for the purpose of generating an alarm and/or recording in a security audit trail.

7.1.2 Data origin authentication

7.1.2.1 Role of upper layers in data origin authentication

Data origin authentication is concerned with authenticating the entity that is claimed to have originated a particular set of data. This is not necessarily the direct peer in an instance of communication, hence data origination authentication has a different purpose from entity authentication.

Each element of data in an instance of communication may, or may not, have data origin authentication applied to it. To ensure the timeliness of received data, data origin authentication may need to be able to also validate the time of origination as well as the source.

7.1.2.2 Provision of data origin authentication

Data origin authentication in the Application Layer is provided by the exchange of security information which may convey, for example, a digital signature based on the data and on an identifier of the origin of the data. Data origin authentication may be provided either at ASO-association establishment time or at any other time during an ASO-association.

Data origin authentication services use security transformations, which typically employ encipherment or digital signature mechanisms.

7.1.2.3 Management of data origin authentication

Management of data origin authentication is, in general, the same as management of entity authentication (see 7.1.1.3).

7.2 Access control

7.2.1 General

Application Layer protocol may provide for the exchange of access control information, e.g. an access control certificate. This conveys information related to the granting, enforcing, and/or revoking of access control rights.

Access control information may be exchanged either at ASO-association establishment time or at any other time during an ASO-association. Access rights presented during an ASO-association may either modify (increase or decrease) the rights valid for the rest of the ASO-association or be valid only for a specific request.

Access control may be applied at a number of different levels of granularity. Two levels are distinguished here, called ASO-association and resource levels, but it is recognized that particular protocols may introduce extra levels into the resource category.

7.2.2 ASO-association access control

7.2.2.1 Role of upper layers in ASO-association access control

ASO-association access control applies at the ASO-association level, and is concerned with controlling access to systems and processes (e.g. application-processes) rather than objects within systems. It is concerned with whether the requested ASO-association from a particular remote system with the requested ASO-context and security characteristics will be allowed to proceed, or to continue if used subsequent to ASO-association establishment.

7.2.2.2 Provision of ASO-association access control

ASO-association access control may be supported by security exchange functions as described in 6.3. These functions may support any of the classes of mechanism identified in ITU-T Rec. X.812 | ISO/IEC 10181-3, the Access Control Framework.

Such a security exchange function can be provided by an ASE used in conjunction with the ACSE, in order to provide for access control at application-association establishment time. In addition, a security exchange at this time enables certain access control information to be retained for subsequent use in making access control decisions during the lifetime of the application-association.

7.2.2.3 Management of ASO-association access control

The security policy in force at a system may require that every access attempt, and particularly every failed access attempt, is reported for the purpose of generating an alarm and/or recording as part of a security audit trail. OSI Security Management services provide a means of maintaining access control information.

7.2.3 Resource access control

7.2.3.1 Role of upper layers in resource access control

Resource access control is concerned with controlling access to a particular resource, such as an information object or objects in an information base. Where an information object is structured into parts, further levels of access control may be provided. One example of such a resource is a file. Access control may be used to determine whether the access initiator has the right to perform a particular operation on the file, such as read or modify.

7.2.3.2 Provision of resource access control

Resource access control may be the purview of a particular ASE or ASO that provides the protocol for exchanging manipulation requests and responses for a particular resource. For example, access control to files is the purview of FTAM (ISO 8571).

These ASEs or ASOs may make use of one or more of the classes of mechanism defined in ITU-T Rec. X.812 | ISO/IEC 10181-3. They may make use of retained access control information resulting from the use of ASO-association access control.

7.2.3.3 Management of resource access control

The security policy in force at a system may require that every access attempt, and particularly every failed access attempt, is reported for the purpose of generating an alarm and/or recording as part of a security audit trail. Management of the access control information itself may be achieved via the specific application protocol, or via a general purpose Application Layer management protocol.

7.3 Non-repudiation

7.3.1 Role of upper layers in non-repudiation

Non-repudiation is an Application Layer service. It includes, but is not limited to, the following cases (as defined in CCITT Rec. X.800 | ISO 7498-2):

a) non-repudiation with proof of origin;

b) non-repudiation with proof of delivery.

In non-repudiation with proof of origin, the recipient of information is provided with proof of its origin. This will protect against any subsequent attempt by the sender to falsely deny sending that information. The role of the upper layers in non-repudiation with proof of origin is to provide proof that a particular item of information was sent by a particular application-entity.

In non-repudiation with proof of delivery, the sender of information is provided with proof of delivery of that information. This will protect against any subsequent attempt by the recipient to falsely deny receiving that information. The role of the Upper Layers in non-repudiation with proof of delivery is to provide proof that a particular item of information was received by a particular application-entity.

7.3.2 Provision of non-repudiation

The provision of non-repudiation services can use digital signature or encipherment mechanisms. This may involve the use of security transformations as described in 6.4. Depending on the security policy in force, non-repudiation may use a notarization mechanism.

An interaction with a trusted third party may be required for non-repudiation with proof of origin, and is always required for non-repudiation with proof of delivery.

There may be a need for a sender and/or recipient to use multiple ASO-associations for interactions with, for example, a signature generation service, a time-stamping service, and/or a directory service.

7.3.3 Management of non-repudiation

If digital signature and/or encipherment mechanisms are used to provide a non-repudiation service the management of such mechanisms may include:

– key management; and

– the establishment of cryptographic parameters and algorithms.

If a notarization mechanism is used to provide a non-repudiation service then the management of such a service may include:

– the distribution of information about notaries; and

– interaction with notaries.

7.4 Integrity

7.4.1 Role of upper layers in integrity

Integrity may be provided as an Application Layer service. Provision of this service may employ security communication functions in the Presentation Layer and associated system security functions. The following services may be provided:

a) connection integrity with recovery;

b) connection integrity without recovery;