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 commmunication via an application-association;
- *relay security association* – A security association between two systems to support protected commmunication 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.