INTERNATIONAL STANDARD

ISO 7498-2

First edition
1989-02-15

Information processing systems — Open Systems Interconnection — Basic Reference Model —

Part 2 :
Security Architecture

Systèmes de traitement de l'information — Interconnexion de systèmes ouverts — Modèle de référence de base —

Partie 2 : Architecture de sécurité

Reference number
ISO 7498-2 : 1989 (E)

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

Draft International Standards adopted by the technical committees are circulated to the member bodies for approval before their acceptance as International Standards by the ISO Council. They are approved in accordance with ISO procedures requiring at least 75 % approval by the member bodies voting.

International Standard ISO 7498-2 was prepared by Technical Committee ISO/TC 97, *Information processing systems.*

Users should note that all International Standards undergo revision from time to time and that any reference made herein to any other International Standard implies its latest edition, unless otherwise stated.

Printed in Switzerland

Contents

Information processing systems — Open Systems Interconnection — Basic Reference Model —

Part 2 : Security Architecture

0 Introduction

ISO 7498 describes the Basic Reference Model for Open Systems Interconnection (OSI). That part of ISO 7498 establishes a framework for coordinating the development of existing and future standards for the interconnection of systems.

The objective of OSI is to permit the interconnection of heterogeneous computer systems so that useful communication between application processes may be achieved. At various times, security controls must be established in order to protect the information exchanged between the application processes. Such controls should make the cost of obtaining or modifying data greater than the potential value of so doing, or make the time required to obtain the data so great that the value of the data is lost.

This part of ISO 7498 defines the general security-related architectural elements which can be applied appropriately in the circumstances for which protection of communication between open systems is required. It establishes, within the framework of the Reference Model, guidelines and constraints to improve existing standards or to develop new standards in the context of OSI in order to allow secure communications and thus provide a consistent approach to security in OSI.

A background in security will be helpful in understanding this document. The reader who is not well versed in security is advised to read annex A first.

This part of ISO 7498 extends the Basic Reference Model to cover security aspects which are general architectural elements of communications protocols, but which are not discussed in the Basic Reference Model.

1 Scope and field of application

This part of ISO 7498:

a) provides a general description of security services and related mechanisms, which may be provided by the Reference Model; and

b) defines the positions within the Reference Model where the services and mechanisms may be provided.

This part of ISO 7498 extends the field of application of ISO 7498, to cover secure communications between open systems.

Basic security services and mechanisms and their appropriate placement have been identified for all layers of the Basic Reference Model. In addition, the architectural relationships of the security services and mechanisms to the Basic Reference Model have been identified. Additional security measures may be needed in end-systems, installations and organizations. These measures apply in various application contexts. The definition of security services needed to support such additional security measures is outside the scope of this standard.

OSI security functions are concerned only with those visible aspects of a communications path which permit end systems to achieve the secure transfer of information between them. OSI Security is not concerned with security measures needed in end systems, installations, and organizations, except where these have implications on the choice and position of security services visible in OSI. These latter aspects of security may be standardized but not within the scope of OSI standards.

This part of ISO 7498 adds to the concepts and principles defined in ISO 7498; it does not modify them. It is not an implementation specification, nor is it a basis for appraising the conformance of actual implementations.

2 References

ISO 7498 *Information processing systems – Open Systems Interconnection – Basic Reference Model.*

ISO 7498-4	*Information processing systems* *– Open Systems Interconnection* *– Basic Reference Model* *– Part 4: Management Framework*[1].
ISO 7498/Add.1	*Information processing systems* *– Open Systems Interconnection* *– Basic Reference Model* *– Addendum 1: Connectionless-mode transmission.*
ISO 8648	*Information processing systems* *– Open Systems Interconnection* *– Internal organization of the Network Layer.*

3 Definitions and abbreviations

3.1 This part of ISO 7498 builds on concepts developed in ISO 7498 and makes use of the following terms defined in it:

a) (N)-connection;
b) (N)-data-transmission;
c) (N)-entity;
d) (N)-facility;
e) (N)-layer;
f) open system;
g) peer entities;
h) (N)-protocol;
j) (N)-protocol-data-unit;
k) (N)-relay;
l) routing;
m)sequencing;
n) (N)-service;
p) (N)-service-data-unit;
q) (N)-user-data;
r) subnetwork;
s) OSI resource; and
t) transfer syntax.

3.2 This part of 7498 uses the following terms drawn from the respective International Standards.

Connectionless Mode Transmission	(ISO 7498/Add.1)
End system	(ISO 7498)
Relaying and routing function	(ISO 8648)
UNITDATA	(ISO 7498)
Management Information Base (MIB)	(ISO 7498-4)

In addition, the following abbreviations are used:

OSI for Open Systems Interconnection;
SDU for Service Data Unit;
SMIB for Security Management Information Base; and
MIB for Management Information Base.

3.3 For the purpose of this part of ISO 7498, the following definitions apply:

3.3.1 access control: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner.

3.3.2 access control list: A list of entities, together with their access rights, which are authorized to have access to a resource.

3.3.3 accountability: The property that ensures that the actions of an entity may be traced uniquely to the entity.

3.3.4 active threat: The threat of a deliberate unauthorized change to the state of the system.

NOTE – Examples of security-relevant active threats may be: modification of messages, replay of messages, insertion of spurious messages, masquerading as an authorized entity and denial of service.

3.3.5 audit: see **security audit**.

3.3.6 audit trail: see **security audit trail**.

3.3.7 authentication: see **data origin authentication,** and **peer entity authentication**.

NOTE – In this part of 7498 the term "authentication" is not used in connection with data integrity; the term "data integrity" is used instead.

3.3.8 authentication information: Information used to establish the validity of a claimed identity.

3.3.9 authentication exchange: A mechanism intended to ensure the identity of an entity by means of information exchange.

3.3.10 authorization: The granting of rights, which includes the granting of access based on access rights.

3.3.11 availability: The property of being accessible and useable upon demand by an authorized entity.

3.3.12 capability: A token used as an identifier for a resource such that possession of the token confers access rights for the resource.

3.3.13 channel: An information transfer path.

3.3.14 ciphertext: Data produced through the use of **encipherment**. The semantic content of the resulting data is not available.

NOTE – **Ciphertext** may itself be input to **encipherment,** such that super-enciphered output is produced.

3.3.15 cleartext: Intelligible data, the semantic content of which is available.

3.3.16 confidentiality: The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

[1] At present at the stage of draft: publication anticipated in due course