

Implementation of ISO 7498-2:1989

**Information processing
systems —
Open systems
Interconnection —
Basic reference
model —**

Part 2: Security architecture

Committees responsible for this British Standard

The preparation of this British Standard was entrusted by the Information Technology Systems Standards Policy Committee (IST/-) to Technical Committee IST/21, upon which the following bodies were represented:

- Association for Payment Clearing Services
- British Computer Society
- British Gas plc
- British Railways Board
- British Telecommunications plc
- Computing Services Association
- Department of Trade and Industry Alvey (Advanced Network Systems Architecture)
- Department of Trade and Industry (Information Technology Division)
- Department of Trade and Industry (National Physical Laboratory)
- EEA (the Electronics and Business Equipment Association)
- HM Treasury (Central Computer and Telecommunications Agency)
- Institute of Chartered Secretaries and Administrators
- Institution of Electrical Engineers
- Inter-universities Computing Committee
- Joint Network Team
- Mercury Communications Limited
- Ministry of Defence
- National Health Services
- Post Office
- United Kingdom Atomic Energy Authority
- University of London Computer Centre

This British Standard, having been prepared under the direction of the Information Technology Systems Standards Policy Committee, was published under the authority of the Board of BSI and comes into effect on 30 November 1990

© BSI 03-1999

The following BSI references relate to the work on this standard:
Committee reference IST/21
Draft for comment DD 148

ISBN 0 580 19068 4

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
Committees responsible	Inside front cover
National foreword	ii
Foreword	iii
Text of ISO 7498-2	1

National foreword

This British Standard reproduces verbatim ISO 7498-2:1989 and implements it as the UK national standard.

This British Standard is published under the direction of the Information Technology Systems Standards Policy Committee whose Technical Committee IST/21 has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international committee any enquiries on interpretation, or proposals for change, and keep UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

NOTE International and European Standards, as well as overseas standards, are available from BSI Sales Department, BSI, Linford Wood, Milton Keynes, MK14 6LE.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, the ISO title page, pages ii to iv, pages 1 to 32 and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

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)

AVA Documents
Document Sharing Hub

Contents

	Page
Foreword	iii
0 Introduction	1
1 Scope and Field of Application	1
2 References	1
3 Definitions	1
4 Notation	5
5 General description of security services and mechanisms	5
5.1 Overview	5
5.2 Security services	5
5.3 Specific security mechanisms	6
5.4 Pervasive security mechanisms	8
5.5 Illustration of relationship of security services and mechanisms	10
6 The relationship of services, mechanisms and layers	10
6.1 Security layering principles	10
6.2 Model of Invocation, Management and Use of Protected (N)-Services	11
7 Placement of security services and mechanisms	13
7.1 Physical layer	13
7.2 Data link layer	13
7.3 Network layer	14
7.4 Transport layer	15
7.5 Session layer	15
7.6 Presentation layer	15
7.7 Application layer	16
7.8 Illustration of relationship of security services and layers	17
8 Security management	17
8.1 General	17
8.2 Categories of OSI security management	19
8.3 Specific system security management activities	20
8.4 Security mechanism management functions	20
Annex A (informative) Background information on security in OSI	22
Annex B (informative) Justification for security service placement in clause 7	29
Annex C (informative) Choice of position of encipherment for applications	31
Figure 1 — Direct Signature Scheme	27
Figure 2 — Arbitrated Signature Scheme	28
Table 1	10
Table 2	19

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.

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 endsystems, 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;

¹⁾ At present at the stage of draft: publication anticipated in due course.

- h) (N)-protocol;
- i) (N)-protocol-data-unit;
- j) (N)-relay;
- k) routing;
- l) sequencing;
- m) (N)-service;
- n) (N)-service-data-unit;
- o) (N)-user-data;
- p) subnetwork;
- q) OSI resource; and
- r) 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

3.3.17**credentials**

data that is transferred to establish the claimed identity of an entity

3.3.18**cryptanalysis**

the analysis of a cryptographic system and/or its inputs and outputs to derive confidential variables and/or sensitive data including **cleartext**

3.3.19**cryptographic checkvalue**

information which is derived by performing a cryptographic transformation (see **cryptography**) on the data unit

NOTE The derivation of the checkvalue may be performed in one or more steps and is a result of a mathematical function of the key and a data unit. It is usually used to check the integrity of a data unit.

3.3.20**cryptography**

the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and/or prevent its unauthorized use

NOTE Cryptography determines the methods used in encipherment and decipherment. An attack on a cryptographic principle, means, or method is cryptanalysis.

3.3.21**data integrity**

the property that data has not been altered or destroyed in an unauthorized manner

3.3.22**data origin authentication**

the corroboration that the source of data received is as claimed

3.3.23**decipherment**

the reversal of a corresponding reversible **encipherment**

3.3.24**decryption**

see **decipherment**

3.3.25**denial of service**

the prevention of authorized access to resources or the delaying of time-critical operations

3.3.26**digital signature**

data appended to, or a cryptographic transformation (see **cryptography**) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient

3.3.27**encipherment**

the cryptographic transformation of data (see **cryptography**) to produce **ciphertext**

NOTE Encipherment may be irreversible, in which case the corresponding decipherment process cannot feasibly be performed.

3.3.28**encryption**

see **encipherment**

3.3.29**end-to-end encipherment**

encipherment of data within or at the source end system, with the corresponding **decipherment** occurring only within or at the destination end system. (See also **link-by-link encipherment**.)

3.3.30**identity-based security policy**

a security policy based on the identities and/or attributes of users, a group of users, or entities acting on behalf of the users and the resources/objects being accessed

3.3.31**integrity**

see **data integrity**

3.3.32**key**

a sequence of symbols that controls the operations of **encipherment** and **decipherment**

3.3.33**key management**

the generation, storage, distribution, deletion, archiving and application of keys in accordance with a **security policy**

3.3.34**link-by-link encipherment**

the individual application of **encipherment** to data on each link of a communications system. (See also **end-to-end encipherment**.)

NOTE The implication of link-by-link encipherment is that data will be in cleartext form in relay entities.

**3.3.35
manipulation detection**

a mechanism which is used to detect whether a data unit has been modified (either accidentally or intentionally)

**3.3.36
masquerade**

the pretence by an entity to be a different entity

**3.3.37
notarization**

the registration of data with a trusted third party that allows the later assurance of the accuracy of its characteristics such as content, origin, time and delivery

**3.3.38
passive threat**

the threat of unauthorized disclosure of information without changing the state of the system

**3.3.39
password**

confidential authentication information, usually composed of a string of characters

**3.3.40
peer-entity authentication**

the corroboration that a peer entity in an association is the one claimed

**3.3.41
physical security**

the measures used to provide physical protection of resources against deliberate and accidental threats

**3.3.42
policy**

see **security policy**

**3.3.43
privacy**

the right of individuals to control or influence what information related to them may be collected and stored and by whom and to whom that information may be disclosed

NOTE Because this term relates to the right of individuals, it cannot be very precise and its use should be avoided except as a motivation for requiring security.

**3.3.44
repudiation**

denial by one of the entities involved in a communication of having participated in all or part of the communication

**3.3.45
routing control**

the application of rules during the process of routing so as to choose or avoid specific networks, links or relays

**3.3.46
rule-based security policy**

a **security policy** based on global rules imposed for all users. These rules usually rely on a comparison of the sensitivity of the resources being accessed and the possession of corresponding attributes of users, a group of users, or entities acting on behalf of users

**3.3.47
security audit**

an independent review and examination of system records and activities in order to test for adequacy of system controls, to ensure compliance with established policy and operational procedures, to detect breaches in security, and to recommend any indicated changes in control, policy and procedures

**3.3.48
security audit trail**

data collected and potentially used to facilitate a security audit

**3.3.49
security label**

the marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource

NOTE The marking and/or binding may be explicit or implicit.

**3.3.50
security policy**

the set of criteria for the provision of security services (see also **identity-based** and **rule-based** security policy)

NOTE A complete security policy will necessarily address many concerns which are outside of the scope of OSI.

**3.3.51
security service**

a service, provided by a layer of communicating open systems, which ensures adequate security of the systems or of data transfers

**3.3.52
selective field protection**

the protection of specific fields within a message which is to be transmitted

**3.3.53
sensitivity**

the characteristic of a resource which implies its value or importance, and may include its vulnerability

3.3.54**signature**

see **digital signature**

3.3.55**threat**

a potential violation of security

3.3.56**traffic analysis**

the inference of information from observation of traffic flows (presence, absence, amount, direction and frequency)

3.3.57**traffic flow confidentiality**

a confidentiality service to protect against traffic analysis

3.3.58**traffic padding**

the generation of spurious instances of communication, spurious data units and/or spurious data within data units

3.3.59**trusted functionality**

that which is perceived to be correct with respect to some criteria, e.g. as established by a security policy

4 Notation

The layer notation used is the same as that defined in ISO 7498.

The term “service” where not otherwise qualified, is used to refer to a security service.

5 General description of security services and mechanisms**5.1 Overview**

Security services that are included in the OSI security architecture and mechanisms which implement those services are discussed in this clause. The security services described below are basic security services. In practice they will be invoked at appropriate layers and in appropriate combinations, usually with non-OSI services and mechanisms, to satisfy security policy and/or user requirements. Particular security mechanisms can be used to implement combinations of the basic security services. Practical realizations of systems may implement particular combinations of the basic security services for direct invocation.

5.2 Security services

The following are considered to be the security services which can be provided optionally within the framework of the OSI Reference Model. The authentication services require authentication information comprising locally stored information and data that is transferred (credentials) to facilitate the authentication.

5.2.1 Authentication

These services provide for the authentication of a communicating peer entity and the source of data as described below.

5.2.1.1 Peer entity authentication

This service, when provided by the (N)-layer, provides corroboration to the (N + 1)-entity that the peer entity is the claimed (N + 1)-entity.

This service is provided for use at the establishment of, or at times during, the data transfer phase of a connection to confirm the identities of one or more of the entities connected to one or more of the other entities. This service provides confidence, at the time of usage only, that an entity is not attempting a masquerade or an unauthorized replay of a previous connection. One-way and mutual peer entity authentication schemes, with or without a liveness check, are possible and can provide varying degrees of protection.

5.2.1.2 Data origin authentication

This service, when provided by the (N)-layer, provides corroboration to an (N + 1)-entity that the source of the data is the claimed peer (N + 1)-entity. The data origin authentication service provides the corroboration of the source of a data unit. The service does not provide protection against duplication or modification of data units.

5.2.2 Access control

This service provides protection against unauthorized use of resources accessible via OSI. These may be OSI or non-OSI resources accessed via OSI protocols. This protection service may be applied to various types of access to a resource (e.g. the use of a communications resource; the reading, the writing, or the deletion of an information resource; the execution of a processing resource) or to all accesses to a resource.

The control of access will be in accordance with various security policies (see 6.2.1.1).