

# 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)



**Documents**

Document Sharing Hub

## 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.

## Contents

|                                                                             | Page |
|-----------------------------------------------------------------------------|------|
| <b>0</b> Introduction .....                                                 | 1    |
| <b>1</b> Scope and Field of Application .....                               | 1    |
| <b>2</b> References .....                                                   | 1    |
| <b>3</b> Definitions .....                                                  | 2    |
| <b>4</b> Notation .....                                                     | 4    |
| <b>5</b> General description of security services and mechanisms .....      | 4    |
| 5.1 Overview .....                                                          | 4    |
| 5.2 Security services .....                                                 | 4    |
| 5.3 Specific security mechanisms .....                                      | 5    |
| 5.4 Pervasive security mechanisms .....                                     | 7    |
| 5.5 Illustration of relationship of security services and mechanisms .....  | 8    |
| <b>6</b> The relationship of services, mechanisms and layers .....          | 8    |
| 6.1 Security layering principles .....                                      | 8    |
| 6.2 Model of Invocation, Management and Use of Protected (N)-Services ..... | 9    |
| <b>7</b> Placement of security services and mechanisms .....                | 12   |
| 7.1 Physical layer .....                                                    | 12   |
| 7.2 Data link layer .....                                                   | 12   |
| 7.3 Network layer .....                                                     | 12   |
| 7.4 Transport layer .....                                                   | 14   |
| 7.5 Session layer .....                                                     | 14   |
| 7.6 Presentation layer .....                                                | 14   |
| 7.7 Application layer .....                                                 | 15   |
| 7.8 Illustration of relationship of security services and layers .....      | 16   |
| <b>8</b> Security management .....                                          | 17   |
| 8.1 General .....                                                           | 17   |
| 8.2 Categories of OSI security management .....                             | 17   |
| 8.3 Specific system security management activities .....                    | 18   |
| 8.4 Security mechanism management functions .....                           | 18   |
| <br><b>Annexes</b>                                                          |      |
| <b>A</b> Background information on security in OSI .....                    | 21   |
| <b>B</b> Justification for security service placement in clause 7 .....     | 29   |
| <b>C</b> Choice of position of encipherment for applications .....          | 32   |

# 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<sup>1)</sup>*.
- 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:

<sup>1)</sup> At present at the stage of draft: publication anticipated in due course

**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).

### 5.2.3 Data confidentiality

These services provide for the protection of data from unauthorized disclosure as described below.

#### 5.2.3.1 Connection confidentiality

This service provides for the confidentiality of all (N)-user-data on an (N)-connection.

NOTE – Depending on use and layer, it may not be appropriate to protect all data, e.g. expedited data or data in a connection request.

#### 5.2.3.2 Connectionless confidentiality

This service provides for the confidentiality of all (N)-user-data in a single connectionless (N)-SDU.

#### 5.2.3.3 Selective field confidentiality

This service provides for the confidentiality of selected fields within the (N)-user-data on an (N)-connection or in a single connectionless (N)-SDU.

#### 5.2.3.4 Traffic flow confidentiality

This service provides for the protection of the information which might be derived from observation of traffic flows.

### 5.2.4 Data integrity

These services counter active threats and may take one of the forms described below.

NOTE – On a connection, the use of the peer entity authentication service at the start of the connection and the data integrity service during the life of the connection can jointly provide for the corroboration of the source of all data units transferred on the connection, the integrity of those data units, and may additionally provide for the detection of duplication of data units e.g. by the use of sequence numbers.

#### 5.2.4.1 Connection integrity with recovery

This service provides for the integrity of all (N)-user-data on an (N)-connection and detects any modification, insertion, deletion or replay of any data within an entire SDU sequence (with recovery attempted).

#### 5.2.4.2 Connection integrity without recovery

As for 5.2.4.1 but with no recovery attempted.

#### 5.2.4.3 Selective field connection integrity

This service provides for the integrity of selected fields within the (N)-user data of an (N)-SDU transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted or replayed.

#### 5.2.4.4 Connectionless integrity

This service, when provided by the (N)-layer, provides integrity assurance to the requesting (N+1)-entity.

This service provides for the integrity of a single connectionless SDU and may take the form of determination of whether a received SDU has been modified. Additionally, a limited form of detection of replay may be provided.

#### 5.2.4.5 Selective field connectionless integrity

This service provides for the integrity of selected fields within a single connectionless SDU and takes the form of determination of whether the selected fields have been modified.

### 5.2.5 Non-repudiation

This service may take one or both of two forms.

#### 5.2.5.1 Non-repudiation with proof of origin

The recipient of data is provided with proof of the origin of data. This will protect against any attempt by the sender to falsely deny sending the data or its contents.

#### 5.2.5.2 Non-repudiation with proof of delivery

The sender of data is provided with proof of delivery of data. This will protect against any subsequent attempt by the recipient to falsely deny receiving the data or its contents.

### 5.3 Specific security mechanisms

The following mechanisms may be incorporated into the appropriate (N)-layer in order to provide some of the services described in 5.2.

#### 5.3.1 Encipherment

5.3.1.1 Encipherment can provide confidentiality of either data or traffic flow information and can play a part in or complement a number of other security mechanisms as described in the following sections.

5.3.1.2 Encipherment algorithms may be reversible or irreversible. There are two general classifications of reversible encipherment algorithm:

- a) symmetric (i.e. secret key) encipherment, in which knowledge of the encipherment key implies knowledge of the decipherment key and vice-versa; and

b) Asymmetric (e.g. public key) encipherment, in which knowledge of the encipherment key does not imply knowledge of the decipherment key, or vice-versa. The two keys of such a system are sometimes referred to as the "public key" and the "private key".

Irreversible encipherment algorithms may or may not use a key. When they use a key, this key may be public or secret.

**5.3.1.3** The existence of an encipherment mechanism implies the use of a key management mechanism except in the case of some irreversible encipherment algorithms. Some guidelines on key management methodologies are given in 8.4.

### 5.3.2 Digital signature mechanisms

These mechanisms define two procedures:

- a) signing a data unit; and
- b) verifying a signed data unit.

The first process uses information which is private (i.e. unique and confidential) to the signer. The second process uses procedures and information which are publicly available but from which the signer's private information cannot be deduced.

**5.3.2.1** The signing process involves either an encipherment of the data unit or the production of a cryptographic checkvalue of the data unit, using the signer's private information as a private key.

**5.3.2.2** The verification process involves using the public procedures and information to determine whether the signature was produced with the signer's private information.

**5.3.2.3** The essential characteristic of the signature mechanism is that the signature can only be produced using the signer's private information. Thus when the signature is verified, it can subsequently be proven to a third party (e.g. a judge or arbitrator) at any time that only the unique holder of the private information could have produced the signature.

### 5.3.3 Access control mechanisms

**5.3.3.1** These mechanisms may use the authenticated identity of an entity or information about the entity (such as membership in a known set of entities) or capabilities of the entity, in order to determine and enforce the access rights of the entity. If the entity attempts to use an unauthorized resource, or an authorized resource with an improper type of access, then the access control function will reject the attempt and may additionally report the incident for the purposes of generating an alarm and/or recording it as part of a security audit trail. Any notification to the sender of a denial of access for a connectionless data transmission can be provided only as a result of access controls imposed at the origin.

**5.3.3.2** Access control mechanisms may, for example, be based on use of one or more of the following:

- a) access control information bases, where the access rights of peer entities are maintained. This information may be maintained by authorization centres or by the entity being accessed, and may be in the form of an access control list or matrix of hierarchical or distributed structure. This presupposes that peer entity authentication has been assured;

- b) authentication information such as passwords, possession and subsequent presentation of which is evidence of the accessing entity's authorization;

- c) capabilities, possession and subsequent presentation of which is evidence of the right to access the entity or resource defined by the capability;

Note: A capability should be unforgeable and should be conveyed in a trusted manner;

- d) Security labels, which when associated with an entity may be used to grant or deny access, usually according to a security policy;

- e) time of attempted access;

- f) route of attempted access; and

- g) duration of access.

**5.3.3.3** Access control mechanisms may be applied at either end of a communications association and/or at any intermediate point.

Access controls involved at the origin or any intermediate point are used to determine whether the sender is authorized to communicate with the recipient and/or to use the required communications resources.

The requirements of the peer level access control mechanisms at the destination end of a connectionless data transmission must be known a priori at the origin, and must be recorded in the Security Management Information Base (see 6.2 and 8.1).

### 5.3.4 Data integrity mechanisms

**5.3.4.1** Two aspects of data integrity are: the integrity of a single data unit or field; and the integrity of a stream of data units or fields. In general, different mechanisms are used to provide these two types of integrity service, although provision of the second without the first is not practical.

**5.3.4.2** Determining the integrity of a single data unit involves two processes, one at the sending entity and one at the receiving entity. The sending entity appends to a data unit a quantity which is a function of the data itself. This quantity may be supplementary information such as a block check code or a cryptographic checkvalue and may itself be enciphered. The receiving entity generates a corresponding quantity and compares it with the received

quantity to determine whether the data has been modified in transit. This mechanism alone will not protect against the replay of a single data unit. In appropriate layers of the architecture, detection of manipulation may lead to recovery action (for example, via retransmission or error correction) at that or a higher layer.

**5.3.4.3** For connection-mode data transfer, protecting the integrity of a sequence of data units (i.e. protecting against misordering, losing, replaying and inserting or modifying data) requires additionally some form of explicit ordering such as sequence numbering, time stamping, or cryptographic chaining.

**5.3.4.4** For connectionless data transmission, time stamping may be used to provide a limited form of protection against replay of individual data units.

### 5.3.5 Authentication exchange mechanism

**5.3.5.1** Some of the techniques which may be applied to authentication exchanges are:

- a) use of authentication information, such as passwords – supplied by a sending entity and checked by the receiving entity;
- b) cryptographic techniques; and
- c) use of characteristics and/or possessions of the entity.

**5.3.5.2** The mechanisms may be incorporated into the (N)-layer in order to provide peer entity authentication. If the mechanism does not succeed in authenticating the entity, this will result in rejection or termination of the connection and may also cause an entry in the security audit trail and/or a report to a security management centre.

**5.3.5.3** When cryptographic techniques are used, they may be combined with “hand-shaking” protocols to protect against replay (i.e. to ensure liveness).

**5.3.5.4** The choices of authentication exchange techniques will depend upon the circumstances in which they will be used. In many circumstances they will need to be used with:

- a) time stamping and synchronized clocks;
- b) two- and three-way handshakes (for unilateral and mutual authentication respectively); and
- c) non-repudiation services achieved by digital signature and/or notarization mechanisms.

### 5.3.6 Traffic padding mechanism

Traffic padding mechanisms can be used to provide various levels of protection against traffic analysis. This mechanism can be effective only if the traffic padding is protected by a confidentiality service.

### 5.3.7 Routing control mechanism

**5.3.7.1** Routes can be chosen either dynamically or by prearrangement so as to use only physically secure sub-networks, relays or links.

**5.3.7.2** End-systems may, on detection of persistent manipulation attacks, wish to instruct the network service provider to establish a connection via a different route.

**5.3.7.3** Data carrying certain security labels may be forbidden by the security policy to pass through certain sub-networks, relays or links. Also the initiator of a connection (or the sender of a connectionless data unit) may specify routing caveats which request that specific sub-networks, links or relays be avoided.

### 5.3.8 Notarization mechanism

Properties about the data communicated between two or more entities, such as its integrity, origin, time and destination, can be assured by the provision of a notarization mechanism. The assurance is provided by a third party notary, which is trusted by the communicating entities, and which holds the necessary information to provide the required assurance in a testifiable manner. Each instance of communication may use digital signature, encipherment, and integrity mechanisms as appropriate to the service being provided by the notary. When such a notarization mechanism is invoked, the data is communicated between the communicating entities via the protected instances of communication and the notary.

## 5.4 Pervasive security mechanisms

This subclause describes a number of mechanisms which are not specific to any particular service. Thus, in clause 7, they are not explicitly described as being in any particular layer. Some of these pervasive security mechanisms can be regarded as aspects of security management (see also clause 8). The importance of these mechanisms is, in general, directly related to the level of security required.

### 5.4.1 Trusted functionality

**5.4.1.1** Trusted functionality must be used to extend the scope of, or to establish the effectiveness of other security mechanisms. Any functionality which directly provides, or provides access to, security mechanisms, should be trustworthy.

**5.4.1.2** The procedures used to ensure that trust may be placed in such hardware and software are outside the scope of this standard and, in any case, vary with the level of perceived threat and value of information to be protected.

**5.4.1.3** These procedures are, in general, costly and difficult to implement. The problems can be minimized by choosing an architecture which permits implementation of security functions in modules which can be made separate from, and provided from, non-security-related functions.

**5.4.1.4** Any protection of associations above the layer at which the protection is applied must be provided by other means, e.g. by appropriate trusted functionality.

## 5.4.2 Security Labels

Resources including data items, may have security labels associated with them e.g. to indicate a sensitivity level. It is often necessary to convey the appropriate security label with data in transit. A security label may be additional data associated with the data transferred or may be implicit e.g. implied by the use of a specific key to encipher data or implied by the context of the data such as the source or route. Explicit security labels must be clearly identifiable in order they they can be appropriately checked. In addition they must be securely bound to the data with which they are associated.

## 5.4.3 Event Detection

**5.4.3.1** Security-relevant event detection includes the detection of apparent violations of security and may also include detection of "normal" events, such as a successful access (or logon). Security-relevant events may be detected by entities within OSI including security mechanisms. The specification of what constitutes an event is maintained by Event Handling Management (see 8.3.1). Detection of various security-relevant events may, for example, cause one or more of the following actions:

- a) local reporting of the event;
- b) remote reporting of the event;
- c) logging the event (see 5.4.3); and
- d) recovery action (see 5.4.4)

Examples of such security-relevant events are:

- a) a specific security violation;
- b) a specific selected event; and
- c) an overflow on a count of a number of occurrences.

**5.4.3.2** Standardization in this field will take into consideration the transmission of relevant information for event reporting and event logging, and the syntactic and semantic definition to be used for the transmission of event reporting and event logging.

## 5.4.4 Security Audit Trail

**5.4.4.1** Security audit trails provide a valuable security mechanism as potentially they permit detection and investigation of breaches of security by permitting a subsequent security audit. A security audit is 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 aid in damage assessment, and to recommend any indicated changes in controls, policy and procedures. A security audit requires the recording of security-relevant information in a security audit trail, and the analysis and reporting of information from the security audit trail. The logging or recording is considered to be a security mechanism and is described in this section. The analysis and report generation is considered a security management function (see 8.3.2).

**5.4.4.2** Collection of security audit trail information may be adapted to various requirements by specifying the kind(s) of security-relevant events to be recorded (e.g. apparent security violations or completion of successful operations).

The known existence of a security audit trail may serve as a deterrent to some potential sources of security attacks.

**5.4.4.3** OSI security audit trail considerations will take into account what information shall optionally be logged, under what conditions that information shall be logged, and the syntactic and semantic definition to be used for the interchange of the security audit trail information.

## 5.4.5 Security recovery

**5.4.5.1** Security recovery deals with requests from mechanisms such as event handling and management functions, and takes recovery actions as the result of applying a set of rules. These recovery actions may be of three kinds:

- a) immediate;
- b) temporary; and
- c) long term.

For example:

Immediate actions may create an immediate abort of operations, like disconnection.

Temporary actions may produce temporary invalidation of an entity.

Long term actions may be an introduction of an entity into a "black list" or the changing of a key.

**5.4.5.2** Subjects for standardization include protocols for recovery actions and for security recovery management (see 8.3.3).

## 5.5 Illustration of relationship of security services and mechanisms

Table 1 *illustrates* which mechanisms, alone or in combination with others, are considered to be sometimes appropriate for the provision of each service. This Table presents an overview of these relationships and is *not definitive*. The services and mechanisms referred to in this table are described in 5.2 and 5.3. The relationships are more fully described in clause 6.

## 6 The relationship of services, mechanisms and layers

### 6.1 Security layering principles

**6.1.1** The following principles were used in order to determine the allocation of security services to layers and the consequent placement of security mechanisms in the layers:

- a) that the number of alternative ways of achieving a service should be minimized;