INTERNATIONAL TELECOMMUNICATION UNION

CCITT X.800

THE INTERNATIONAL
TELEGRAPH AND TELEPHONE
CONSULTATIVE COMMITTEE

DATA COMMUNICATION NETWORKS: OPEN SYSTEMS INTERCONNECTION (OSI); SECURITY, STRUCTURE AND APPLICATIONS

SECURITY ARCHITECTURE FOR OPEN SYSTEMS INTERCONNECTION FOR CCITT APPLICATIONS

Recommendation X.800

Geneva, 1991

FOREWORD

The CCITT (the International Telegraph and Telephone Consultative Committee) is a permanent organ of the International Telecommunication Union (ITU). CCITT is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The Plenary Assembly of CCITT which meets every four years, establishes the topics for study and approves Recommendations prepared by its Study Groups. The approval of Recommendations by the members of CCITT between Plenary Assemblies is covered by the procedure laid down in CCITT Resolution No. 2 (Melbourne, 1988).

Recommendation X.800 was prepared by Study Group VII and was approved under the Resolution No. 2 procedure on the 22nd of March 1991.

CCITT NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication Administration and a recognized private operating agency.

© ITU 1991

All rights reserved. No part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the ITU.

Recommendation X.800

SECURITY ARCHITECTURE FOR OPEN SYSTEMS INTERCONNECTION FOR CCITT APPLICATIONS [1)]

0 Introduction

Recommendation X.200 describes the Reference Model for open systems interconnection (OSI). It establishes a framework for coordinating the development of existing and future Recommendations 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 improperly obtaining or modifying data greater than the potential value of so doing, or make the time required to obtain the data improperly so great that the value of the data is lost.

This Recommendation 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 Recommendations or to develop new Recommendations 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 Recommendation. The reader who is not well versed in security is advised to read Annex A first.

This Recommendation extends the Reference Model (Recommendation X.200) to cover security aspects which are general architectural elements of communications protocols, but which are not discussed in the Reference Model.

1 Scope and field of application

This Recommendation:

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 Recommendation extends the field of application of Recommendation X.200, to cover secure communications between open systems.

Basic security services and mechanisms and their appropriate placement have been identified for all layers of the Reference Model. In addition, the architectural relationships of the security services and mechanisms to the 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 the Recommendation.

[1)] Recommendation X.800 and ISO 7498-2 (Information processing systems – Open systems interconnection – Basic Reference Model – Part 2: Security architecture) are technically aligned.

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 Recommendations.

This Recommendation adds to the concepts and principles defined in Recommendation X.200; 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

Rec. X.200 – Reference Model of open systems interconnection for CCITT applications.

ISO 7498 – Information processing systems – Open systems interconnection – Basic Reference Model (1984).

ISO 7498-4 – Information processing systems – Open systems interconnection – Basic Reference Model – Part 4: Management framework (1989).

ISO 7498/AD1 – Information processing systems – Open systems interconnection – Basic Reference Model – Addendum 1: Connectionless-mode transmission (1987).

ISO 8648 – Information processing systems – Open systems interconnection – Internal organization of the network layer (1988).

3 Definitions and abbreviations

3.1 This Recommendation builds on concepts developed in Recommendation X.200 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) Sub-network;

s) OSI resource; and

t) Transfer syntax.

3.2 This Recommendation uses the following terms drawn from the respective Recommendations/International standards:

Connectionless-mode transmission (ISO 7498/AD1)

End system (Rec. X.200/ISO 7498)

Relaying and routing function (ISO 8648)

Management information base (MIB) (ISO 7498-4)

In addition, the following abbreviations are used:

OSI 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 Recommendation, 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 Recommendation 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 chose 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**

Functionality 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 Recommendation X.200.

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 section. 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 transfered 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 integrityx*

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) Acess 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 unforceable 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 retransmissions 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 "handshaking" 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 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*

5.3.8.1 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 subsection describes a number of mechanisms which are not specific to any particular service. Thus, in § 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 § 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 may be used to extend the scope, 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 Recommendation 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*

5.4.2.1 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 that 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 log on). 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/X.800 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 § 6.

TABLE 1/X.800

Illustration of relationship of security services and mechanisms

Mechanism / Service	Encipherment	Digital signature	Acces control	Data integrity	Authenti-cation exchange	Traffic padding	Routing control	Notari-zation
Peer entity authentication	Y	Y	·	·	Y	·	·	·
Data origin authentication	Y	Y	·	·	·	·	·	·
Access control service	·	·	Y	·	·	·	·	·
Connection confidentiality	Y	.	·	·	·	·	Y	·
Connectionless confidentiality	Y	·	·	·	·	·	Y	·
Selective field confidentiality	Y	·	·	·	·	·	·	·
Traffic flow confidentiality	Y	·	·	·	·	Y	Y	·
Connection Integrity with recovery	Y	·	·	Y	·	·	·	·
Connection integrity without recovery	Y	·	·	Y	·	·	·	·
Selective field connection integrity	Y	·	·	Y	·	·	·	·
Connectionless integrity	Y	Y	·	Y	·	·	·	·
Selective field connectionless integrity	Y	Y	·	Y	·	·	·	·
Non-repudiation. Origin	·	Y	·	Y	·	·	·	Y
Non-repudiation. Delivery	·	Y	·	Y	·	·	·	Y

· The mechanism is considered not to be appropriate.

Y Yes: the mechanism is considered to be appropiate, either on its own or in combination with other mechanisms.

Note – In some instances, the mechanism provides more than is necessary for the relevant service but could nevertheless be used.

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

b) it is acceptable to build secure systems by providing security services in more than one layer;

c) additional functionality required for security should not unnecessarily duplicate the existing OSI functions;

d) violation of layer independence should be avoided;

e) the amount of trusted functionality should be minimized;

f) wherever an entity is dependent on a security mechanism provided by an entity in a lower layer, any intermediate layers should be constructed in such a way that security violation is impracticable;

g) wherever possible, the additional security functions of a layer should be defined in such a way that implementation as a self-contained module(s) is not precluded; and

h) this Recommendation is assumed to apply to open systems consisting of end systems containing all seven layers and to relay systems.

6.1.2 Service definitions at each layer may require modification to provide for requests for security services whether the services requested are provided at that layer or below.

6.2 *Model of invocation, management and use of protected (N)-services*

This subsection should be read in conjunction with § 8 which contains a general discussion of security management issues. It is intended that security services and mechanisms can be activated by the management entity through the management interface and/or by service invocation.

6.2.1 *Determination of protection features for an instance of communication*

6.2.1.1 *General*

This subsection describes the invocation of protection for connection-oriented and connectionless instances of communication. In the case of connection-oriented communication, the protection services are usually requested/granted at connection establishment time. In the case of a connectionless service invocation, the protection is requested/granted for each instance of a connectionless service request.

In order to simplify the following description, the term “service request” will be used to mean either a connection establishment or a connectionless service request. The invocation of protection for selected data can be achieved by requesting selective field protection. For example, this can be done by establishing several connections, each with a different type or level of protection.

This security architecture accommodates a variety of security policies including those which are rule-based, those which are identity-based and those which are a mixture of both. The security architecture also accommodates protection which is administratively imposed, that which is dynamically selected and a mixture of both.

6.2.1.2 *Service requests*

For each (N)-service request, the (N + 1)-entity may request the desired target security protection. The (N)-service request will specify the security services together with parameters and any additional relevant information (such as sensitivity information and/or security labels) to achieve the target security protection.

Prior to each instance of communication, the (N)-layer has to access the security management information base (SMIB) (see § 8.1). The SMIB will contain information on the administratively-imposed protection requirements associated with the (N + 1)-entity. Trusted functionality is required to enforce these administratively-imposed security requirements.

The provision of the security features during an instance of connection-oriented communication may require the negotiation of the security services that are required. The procedures required for negotiating mechanisms and parameters can either be carried out as a separate procedure or as an integral part of the normal connection establishment procedure.

When the negotiation is carried out as a separate procedure, the results of the agreement (i.e. on the type of security mechanisms and the security parameters that are necessary to provide such security services) are entered in the security management information base (see § 8.1).

When the negotiation is carried out as an integral part of the normal connection establishment procedure, the results of the negotiation between the (N)-entities, will be temporarily stored in the SMIB. Prior to the negotiation each (N)-entity will access the SMIB for information required for the negotiation.

The (N)-layer will reject the service request if it violates administratively-imposed requirements that are registered in the SMIB for the (N + 1)-entity.

The (N)-layer will also add to the requested protection services any security services which are defined in the SMIB as mandatory to obtain the target security protection.

If the (N + 1)-entity does not specify a target security protection, the (N)-layer will follow a security policy in accordance with the SMIB. This could be to proceed with communication using a default security protection within the range defined for the (N + 1)-entity in the SMIB.

6.2.2 *Provision of protection services*

After the combination of administratively-imposed and dynamically selected security requirements has been determined, as described in § 6.2.1, the (N)-layer will attempt to achieve, as a minimum, the target protection. This will be achieved by either, or both, of the following methods:

a) invoking security mechanisms directly within the (N)-layer; and/or

b) requesting protection services from the (N − 1)-layer. In this case, the scope of protection must be extended to the (N)-service by a combination of trusted functionality and/or specific security mechanisms in the (N)-layer.

Note – This does not necessarily imply that all the functionality in the (N)-layer has to be trusted.

Thus, the (N)-layer determines if it is able to achieve the requested target protection. If it is not able to achieve this, no instance of communication occurs.

6.2.2.1 *Establishment of a protected (N)-connection*

The following discussion addresses the provision of services within the (N)-layer, (as opposed to relying on (N − 1)-services).

In certain protocols, to achieve a satisfactory target protection, the sequence of operations is crucial.

a) *Outgoing Access Control*

The (N)-layer may impose outgoing access controls, i.e. it may determine locally (from the SMIB) whether the protected (N)-connection establishment may be attempted or is forbidden.

b) *Peer Entity Authentication*

If the target protection includes Peer Entity Authentication, or if it is known (from the SMIB) that the destination (N)-entity will require Peer Entity Authentication, then an authentication exchange must take place. This may employ two- or three-way handshakes to provide unilateral or mutual authentication, as required.

Sometimes, the authentication exchange may be integrated into the usual (N)-connection establishment procedures. Under other circumstances, the authentication exchange may be accomplished separately from (N)-connection establishment.

c) *Access Control service*

The destination (N)-entity or intermediate entities may impose access control restrictions. If specific information is required by a remote access control mechanism then the initiating (N)-entity supplies this information within the (N)-layer protocol or via management channels.

d) *Confidentiality*

If a total or selective confidentiality service has been selected, a protected (N)-connection must be established. This must include the establishment of the proper working key(s) and negotiation of cryptographic parameters for the connection. This may have been done by prearrangement, in the authentication exchange, or by a separate protocol.

e) *Data Integrity*

If integrity of all (N)-user-data, with or without recovery, or integrity of selective fields has been selected, a protected (N)-connection must be established. This may be the same connection as that established to provide the confidentiality service and may provide authentication. The same considerations apply as for the confidentiality service for a protected (N)-connection.

f) *Non-repudiation services*

If Non-repudiation with Proof of Origin has been selected, the proper cryptographic parameters must be established, or a protected connection with a notarization entity must be established.

If Non-repudiation with Proof of Delivery is selected, the proper parameters (which are different from those required for non-repudiation with proof of origin) must be established, or a protected connection with a notarization entity must be established.

Note – The establishment of the protected (N)-connection may fail due to the lack of agreement on cryptographic parameters (possibly including the non-possession of the proper keys) or through rejection by an access control mechanism.

6.2.3 *Operation of a protected (N)-connection*

6.2.3.1 During the data transfer phase of a protected (N)-connection, the protection services negotiated must be provided.

The following will be visible at the (N)-service boundary:

a) Peer Entity Authentication (at intervals);

b) Protection of Selective Fields; and

c) Reporting of Active Attack (for example, when a manipulation of data has occurred and the service being provided is "connection integrity without recovery" – see § 5.2.4.2).

In addition, the following may be needed:

a) security audit trail recording, and

b) event detection and handling.

6.2.3.2 *Those services which are amenable to selective application are:*

a) Confidentiality;

b) Data Integrity (possibly with authentication); and

c) Non-repudiation (by receiver or by sender).

Note 1 – Two techniques are suggested for marking those data items selected for the application of a service. The first involves using strong typing. It is anticipated that the presentation layer will recognize certain types as those which require certain protection services to be applied. The second involves some form of flagging the individual data items to which specified protection services should be applied.

Note 2 – It is assumed that one reason for providing the selective application of non-repudiation services may arise from the following scenario. Some form of negotiating dialogue occurs over an association prior to both (N)-entities agreeing that a final version of a data item is mutually acceptable. At that point, the intended recipient may ask the sender to apply non-repudiation services (of both origin and delivery) to the final agreed version of the data item. The sender asks for and obtains these services, transmits the data item, and subsequently receives notice that the data item has been received and acknowledged by the recipient. The non-repudiation services assure both the originator and recipient of the data item that it has been successfully transmitted.

Note 3 – Both the non-repudiation services (i.e. of origin and of delivery) are invoked by the originator.

6.2.4 *Provision of protected connectionless data transmission*

Not all the security services available in connection-oriented protocols are available in connectionless protocols. Specifically, protection against deletion, insertion and replay attacks, if required, must be provided at connection-oriented higher layers. Limited protection against replay attacks can be provided by a time stamp mechanism. In a ddition, a number of other security services are unable to provide the same degree of security enforcement that can be achieved by connection-oriented protocols.

The protection services which are appropriate to connectionless data transmission are the following:

a) Peer Entity Authentication (see § 5.2.1.1);

b) Data Origin Authentication (see § 5.2.1.2);

c) Access Control service (see § 5.2.2);

d) Connectionless Confidentiality (see § 5.2.3.2);

e) Selective Field Confidentiality (see § 5.2.3.3);

f) Connectionless Integrity (see § 5.2.4.4);

g) Selective Field Connectionless Integrity (see § 5.2.4.5); and

h) Non-repudiation, Origin (see § 5.2.5.1).

The services are provided by encipherment, signature mechanisms, access control mechanisms, routing mechanisms, data integrity mechanisms and/or notarization mechanisms (see § 5.3).

The originator of a connectionless data transmission will have to ensure that his single SDU contains all the information required to make it acceptable at the destination.

7 Placement of security services and mechanisms

This section defines the security services to be provided within the framework of the OSI Basic Reference Model, and outlines the manner in which they are to be achieved. The provision of any security service is optional, depending upon requirements.

Where a specific security service is identified in this section as being optionally provided by a particular layer, then that security service is provided by security mechanisms operating within that layer, unless otherwise specified. As described in § 6, many layers will offer to provide particular security services. Such layers may not always provide the security services from within themselves, but may make use of appropriate security services being provided within lower layers. Even when no security services are being provided within a layer, the service definitions of that layer may require modification to permit requests for security services to be passed to a lower layer.

Note 1 – Pervasive security mechanisms (see § 5.4) are not discussed in this section.

Note 2 – The choice of position of encipherment mechanisms for applications is discussed in Annex C.

7.1 *Physical layer*

7.1.1 *Services*

The only security services provided at the physical layer, either singly or in combination, are as follows:

a) Connection Confidentiality, and

b) Traffic Flow Confidentiality.

The Traffic Flow Confidentiality service takes two forms:

1) Full Traffic Flow Confidentiality which can be provided only in certain circumstances e.g., two-way simultaneous, synchronous, point-to-point transmission; and

2) Limited Traffic Flow Confidentiality which can be provided for other types of transmission e.g., asynchronous transmission.

These security services are restricted to passive threats and can be applied to point-to-point or multi-peer communications.

7.1.2 *Mechanisms*

Total encipherment of the data stream is the principal security mechanism at the physical layer.

A specific form of encipherment, applicable at the physical layer only, is transmission security (i.e. spread spectrum security).

Physical layer protection is provided by means of an encipherment device which operates transparently. The objective of physical layer protection is to protect the entire physical service data bit stream and to provide traffic flow confidentiality.

7.2 *Data link layer*

7.2.1 *Services*

The only security services provided at the data link layer are:

a) Connection Confidentiality, and

b) Connectionless Confidentiality.

7.2.2 *Mechanisms*

The encipherment mechanism is used to provide the security services in the data link layer (see Annex C).

The additional security protection functionality of the link layer is performed before the normal layer functions for transmission and after the normal layer functions for receipt, i.e. security mechanisms build on and use all of the normal layer functions.

Encipherment mechanisms at the data link layer are sensitive to the link layer protocol.

7.3 *Network layer*

The network layer is internally organized to provide protocol(s) to perform the following operations:

a) sub-network access;

b) sub-network-dependent convergence;

c) sub-network-independent convergence; and

d) relaying and routing.

7.3.1 *Services*

The security services that may be provided by the protocol which performs the sub-network access functions associated with the provision of the OSI network service are as follows:

a) Peer Entity Authentication;

b) Data Origin Authentication;

c) Access Control service;

d) Connection Confidentiality;

e) Connectionless Confidentiality;

f) Traffic Flow Confidentiality;

g) Connection Integrity without recovery; and

h) Connectionless Integrity.

These security services may be provided singly or in combination. The security services that may be provided by the protocol which performs the relaying and routing operations associated with the provision of the OSI network service, from end system to end system, are the same as those provided by the protocol which performs the sub-network access operations.

7.3.2 *Mechanisms*

7.3.2.1 Identical security mechanisms are used by the protocol(s) which perform the sub-network access and relaying and routing operations associated with providing the OSI network service from end system to end system. Routing is performed in this layer and, therefore, routing control is located in this layer. The identified security services are provided as follows:

a) the Peer Entity Authentication service is provided by an appropriate combination of cryptographically-derived or protected authentication exchanges, protected password exchange and signature mechanisms;

b) the Data Origin Authentication service can be provided by encipherment or signature mechanisms;

c) the Access Control service is provided through the appropriate use of specific access control mechanisms;

d) the Connection Confidentiality service is provided by an encipherment mechanism and/or routing control;

e) the Connectionless Confidentiality service is provided by an encipherment mechanism and/or routing control;

f) the Traffic Flow Confidentiality service is achieved by a traffic padding mechanism, in conjunction with a confidentiality service at or below the network layer and/or routing control;

g) the Connection Integrity without Recovery service is provided by using a data integrity mechanism, sometimes in connection with an encipherment mechanism; and

h) the Connectionless Integrity service is provided by using a data integrity mechanism, sometimes in conjunction with an encipherment mechanism.

7.3.2.2 Mechanisms in the protocol which performs the sub-network access operations associated with providing the OSI network service from end system to end system, offer services across a single sub-network.

Protection of a sub-network imposed by the administration of the sub-network will be applied as dictated by the sub-network access protocols but will normally be applied before the normal sub-network functions on transmission and after the normal sub-network functions on receipt.

7.3.2.3 Mechanisms provided by the protocol which performs the relaying and routing operations associated with providing the OSI network service, from end system to end system, offer services across one or more interconnected networks.

These mechanisms will be invoked before the relaying and routing functions on transmission and after the relaying and routing functions on receipt. In the case of the routing control mechanism, the appropriate routing constraints are derived from the SMIB before the data, along with the necessary routing constraints, is passed to the relaying and routing functions.

7.3.2.4 Access control in the network layer can serve many purposes. For example, it allows an end system to control establishment of network connections and to reject unwanted calls. It also allows one or more sub-networks to control usage of network layer resources. In some cases, this latter purpose is related to charging for network usage.

Note – The establishment of a network connection may often result in charges by the sub-network administration. Cost minimization can be performed by controlling access and by selecting reverse charging or other network-specific parameters.

7.3.2.5 The requirement of a particular sub-network may impose access control mechanisms on the protocol which performs the sub-network access operations associated with the provision of the OSI network service, from end system to end system. When access control mechanisms are provided by the protocol which performs the relaying and routing operations associated with the provision of the OSI network service, from end system to end system, they can be used both to control access to sub-networks by relay entities and to control access to end systems. Clearly, the extent of isolation of access control is fairly coarse, distinguishing only between network layer entities.

7.3.2.6 If traffic padding is used in conjunction with an encipherment mechanism in the network layer (or a confidentiality service from the physical layer), then a reasonable level of traffic flow confidentiality may be achieved.

7.4 *Transport layer*

7.4.1 *Services*

The security services that may be provided, singly or in combination, in the transport layer are:

a) Peer Entity Authentication;

b) Data Origin Authentication;

c) Access Control service;

d) Connection Confidentiality;

e) Connectionless Confidentiality;

f) Connection Integrity with Recovery;

g) Connection Integrity without Recovery; and

h) Connectionless Integrity.

7.4.2 *Mechanisms*

The identified security services are provided as follows:

a) the Peer Entity Authentication service is provided by an appropriate combination of cryptographically-derived or protected authentication exchanges, protected password exchange and signature mechanisms;

b) the Data Origin Authentication service can be provided by encipherment or signature mechanisms;

c) the Access Control service is provided through the appropriate use of specific access control mechanisms;

d) the Connection Confidentiality service is provided by an encipherment mechanism;

e) the Connectionless Confidentiality service is provided by an encipherment mechanism;

f) the Connection Integrity Recovery service is provided by using a data integrity mechanism, sometimes in conjunction with an encipherment mechanism;

g) the Connection Integrity without Recovery service is provided by using a data integrity mechanism, sometimes in conjunction with an encipherment mechanism; and

h) the Connectionless Integrity service is provided by using a data integrity mechanism, sometimes in conjunction with an encipherment mechanism.

The protection mechanisms will operate in such a manner that the security services may be invoked for individual transport connections. The protection will be such that individual transport connections can be isolated from all other transport connections.

7.5 *Session layer*

7.5.1 *Services*

No security services are provided in the session layer.

7.6 *Presentation layer*

7.6.1 *Services*

Facilities will be provided by the presentation layer in support of the provision of the following security services by the application layer to the application process:

a) Connection Confidentiality;

b) Connectionless Confidentiality; and

c) Selective Field Confidentiality.

Facilities in the presentation layer may also support the provision of the following security services by the application layer to the application process:

d) Traffic Flow Confidentiality;

e) Peer Entity Authentication;

f) Data Origin Authentication;

g) Connection Integrity with Recovery;

h) Connection Integrity without Recovery;

j) Selective Field Connection Integrity;

k) Connectionless Integrity;

m) Selective Field Connectionless Integrity;

n) Non-repudiation with Proof or Origin; and

p) Non-repudiation with Proof of Delivery.

Note – The facilities provided by the presentation layer will be those that rely on mechanisms which can only operate on a transfer syntax encoding of data and will, for example, include those based on cryptographic techniques.

7.6.2 *Mechanisms*

For the following security services, supporting mechanisms may be located within the presentation layer, and if so, may be used in conjunction with application layer security mechanisms to provide application layer security services:

a) Peer Entity Authentication service can be supported by syntactic transformation mechanisms (e.g. encipherment);

b) Data Origin Authentication service can be supported by encipherment or signature mechanisms;

c) Connection Confidentiality service can be supported by an encipherment mechanism;

d) Connectionless Confidentiality service can be supported by an encipherment mechanism;

e) Selective Field Confidentiality service can be supported by an encipherment mechanism;

f) Traffic Flow Confidentiality service can be supported by an encipherment mechanism;

g) Connection Integrity with Recovery service can be supported by a data integrity mechanism, sometimes in conjunction with an encipherment mechanism;

h) Connection Integrity without Recovery service can be supported by a data integrity mechanism, sometimes in conjunction with an encipherment mechanism;

j) Selective Field Connection Integrity service can be supported by a data integrity mechanism, sometimes in conjunction with an encipherment mechanism;

k) Connectionless Integrity service can be supported by a data integrity mechanism, sometimes in conjunction with an encipherment mechanism;

m) Selective Field Connectionless Integrity service can be supported by a data integrity mechanism, sometimes in conjunction with an encipherment mechanism;

n) Non-repudiation with Proof of Origin service can be supported by an appropriate combination of data integrity, signature and notarization mechanisms; and

p) Non-repudiation with Proof of Delivery service can be supported by an appropriate combination of data integrity, signature and notarization mechanisms.

Encipherment mechanisms applied to data transfers, when located in the upper layers, will be contained in the presentation layer.

Some of the security services in the list above can alternatively be provided by security mechanisms contained entirely within the application layer.

Only the confidentiality security services can be wholly provided by security mechanisms contained within the presentation layer.

Security mechanisms in the presentation layer operate as the final stage of transformation to the transfer syntax on transmission, and as the initial stage of the transformation process on receipt.

7.7 *Application layer*

7.7.1 *Services*

The application layer may provide one or more of the following basic security services either singly or in combination:

a) Peer Entity Authentication;

b) Data Origin Authentication;

c) Access Control Service;

d) Connection Confidentiality;

e) Connectionless Confidentiality;

f) Selective Field Confidentiality;

g) Traffic Flow Confidentiality;

h) Connection Integrity with Recovery;

j) Connection Integrity without Recovery;

k) Selective Field Connection Integrity;

m) Connectionless Integrity;

n) Selective Field Connectionless Integrity;

p) Non-repudiation with Proof of Origin; and

q) Non-repudiation with Proof of Delivery.

The authentication of intended communications partners provides support for access controls to both OSI and non-OSI resources (e.g. files, software, terminals, printers) in real open systems.

The determination of specific security requirements in an instance of communication, including data confidentiality, integrity, and authentication, may be made by OSI security management or application layer management on the basis of information in the SMIB in addition to requests made by the application process.

7.7.2 *Mechanisms*

The security services in the application layer are provided by means of the following mechanisms:

a) Peer Entity Authentication service can be provided using authentication information transferred between application entities, protected by presentation or lower layer encipherment mechanisms;

b) Data Origin Authentication service can be supported by using signature mechanisms or lower layer encipherment mechanisms;

c) Access Control service to those aspects of a real open system that are pertinent to OSI, such as the ability to communicate with specific systems or remote application entities, may be provided by a combination of access control mechanisms in the application layer and in lower layers;

d) Connection Confidentiality service can be supported by using a lower layer encipherment mechanism;

e) Connectionless Confidentiality service can be supported by using a lower layer encipherment mechanism;

f) Selective Field Confidentiality service can be supported by using an encipherment mechanism at the presentation layer;

g) a limited Traffic Flow Confidentiality service can be supported by the use of a traffic padding mechanism at the application layer in conjunction with a confidentiality service at a lower layer;

h) Connection Integrity with Recovery service can be supported using a lower layer data integrity mechanism (sometimes in conjunction with an encipherment mechanism);

j) Connection Integrity without Recovery service can be supported using a lower layer data integrity mechanism (sometimes in conjunction with an encipherment mechanism);

k) Selective Field Connection Integrity service can be supported using a data integrity mechanism (sometimes in conjunction with an encipherment mechanism) at the presentation layer;

m) Connectionless Integrity service can be supported using a lower layer data integrity mechanism (sometimes in conjunction with an encipherment mechanism);

n) Selective Field Connectionless Integrity service can be supported using a data integrity mechanism (sometimes in conjunction with an encipherment mechanism) at the presentation layer;

p) Non-repudiation with Proof of Origin service can be supported by an appropriate combination of signature and lower layer data integrity mechanisms possibly in conjunction with third party notaries; and

q) Non-repudiation with Proof of Delivery service can be supported by an appropriate combination of signature and lower layer data integrity mechanisms possibly in conjunction with third party notaries.

If a notarization mechanism is used to provide a non-repudiation service, it will be acting as a trusted third party. It may have a record of data units relayed in their transferred form (i.e. transfer syntax) in order to resolve disputes. It may use protection services from the lower layers.

7.7.3 *Non-OSI security services*

Application processes themselves may provide essentially all of the services, and use the same kinds of mechanisms, that are described in this Recommendation, as appropriately placed in various layers of the architecture. Such use is outside of the scope of, but not inconsistent with, the OSI service and protocol definitions and the OSI architecture.

7.8 *Illustration of the relationship of security services and layers*

Table 2/X.800 illustrates the layers of the Reference Model in which particular security services can be provided. Descriptions of the security services are found in § 5.2. Justifications for the placement of a service at a particular layer are given in Annex B.

TABLE 2/X.800

Illustration of the relationship of security services and layers

Service	Layer						
	1	2	3	4	5	6	7*
Peer entity authentication	·	·	Y	Y	·	·	Y
Data origen authentication	·	·	Y	Y	·	·	Y
Access control service	·	·	Y	Y	·	·	Y
Connection confidentiality	Y	Y	Y	Y	·	Y	Y
Connectionless confidentiality	·	Y	Y	Y	·	Y	Y
Selective field confidentiality	·	·	·	·	·	Y	Y
Traffic flow confidentiality	Y	·	Y	·	·	·	Y
Connection Integrity with recovery	·	·	·	Y	·	·	Y
Connection integrity without recovery	·	·	Y	Y	·	·	Y
Selective field connection integrity	·	·	·	·	·	·	Y
Connectionless integrity	·	·	Y	Y	·	·	Y
Selective field connectionless integrity	·	·	·	·	·	·	Y
Non-repudiation Origin	·	·	·	·	·	·	Y
Non-repudiation. Delivery	·	·	·	·	·	·	Y

Y Yes, service should be incorporated in the standards for the layer as a provider option.

· Not provided.

* It should be noted, with respect to layer 7, that the application process may, itself, provide security services.

Note 1 – Table 2/X.800 makes no attempt to indicte that entries are of equal weight or importance; on the contrary there is a considerable gradation of scale within the table entries.

Note 2 – The placement of security services within the network layer is described in § 7.3.2. The position of the security services within the network layer significantly affects the nature and scope of the services that will be provided.

Note 3 – The presentation layer contains a number of security facilities which support the provision of security services by the application layer.

8 Security management

8.1 *General*

8.1.1 OSI security management is concerned with those aspects of security management relative to OSI and to security of OSI management. Management aspects of OSI security are concerned with those operations which are outside normal instances of communication but which are needed to support and control the security aspects of those communications.

Note – The availability of communication service is determined by network design and/or network management protocols. Appropriate choices for these are needed to protect against denial of service.

8.1.2 There can be many security policies imposed by the administration(s) of distributed open systems and OSI security management recommendations should support such policies. Entities that are subject to a single security policy, administered by a single authority, are sometimes collected into what has been called a "security domain". Security domains and their interactions are an important area for future extensions.

8.1.3 OSI security management is concerned with the management of OSI security services and mechanisms. Such management requires distribution of management information to these services and mechanisms as well as the collection of information concerning the operation of these services and mechanisms. Examples are the distribution of cryptographic keys, the setting of administratively-imposed security selection parameters, the reporting of both normal and abnormal security events (audit trails), and service activation and deactivation. Security management does not address the passing of security-relevant information in protocols which call up specific security services (e.g., in parameters in connection requests).

8.1.4 The security management information base (SMIB) is the conceptual repository for all security-relevant information needed by open systems. This concept does not suggest any form for the storage of the information or its implementation. However, each end system must contain the necessary local information to enable it to enforce an appropriate security policy. The SMIB is a distributed information base to the extent that it is necessary to enforce a consistent security policy in a (logical or physical) grouping of end systems. In practice, parts of the SMIB may or may not be integrated with the MIB.

Note – There can be many realizations of the SMIB, e.g.:

a) a table of data;

b) a file;

c) data or rules embedded within the software or hardware of the real open system.

8.1.5 Management protocols, especially security management protocols, and the communication channels carrying the management information, are potentially vulnerable. Particular care shall therefore be taken to ensure that the management protocols and information are protected such that the security protection provided for usual instances of communication is not weakened.

8.1.6 Security management may require the exchange of security-relevant information between various system administrations, in order that the SMIB can be established or extended. In some cases, the security-relevant information will be passed through non-OSI communication paths, and the local systems administrators will update the SMIB through methods not standardized by OSI. In other cases, it may be desirable to exchange such information over an OSI communication path in which case the information will be passed between two security management applications running in the real open systems. The security management application will use the communicated information to update the SMIB. Such updating of the SMIB may require the prior authorization of the appropriate security administrator.

8.1.7 Application protocols will be defined for the exchange of security-relevant information over OSI communications channels.

8.2 *Categories of OSI security management*

There are three categories of OSI security management activities:

a) system security management;

b) security service management; and

c) security mechanism management.

In addition, security of OSI management itself must be considered (see § 8.2.4). The key functions performed by these categories of security management are summarized below.

8.2.1 *System security management*

System security management is concerned with the management of security aspects of the overall OSI environment. The following list is typical of the activities which fall into this category of security management:

a) overall security policy management, including updates and maintenance of consistency;

b) interaction with other OSI management functions;

c) interaction with security service management and security mechanism management;

d) event handling management (see § 8.3.1);

e) security audit management (see § 8.3.2); and

f) security recovery management (see § 8.3.3).

8.2.2 *Security service management*

Security service management is concerned with the management of particular security services. The following list is typical of the activities which may be performed in managing a particular security service:

a) determination and assignment of the target security protection for the service;

b) assignment and maintenance of rules for the selection (where alternatives exist) of the specific security mechanism to be employed to provide the requested security service;

c) negotiation (locally and remotely) of available security mechanisms which require prior management agreement;

d) invocation of specific security mechanisms via the appropriate security mechanism management function, e.g. for the provision of administratively-imposed security services; and

e) interaction with other security service management functions and security mechanism management functions.

8.2.3 *Security mechanism management*

Security mechanism management is concerned with the management of particular security mechanisms. The following list of security mechanism management functions is typical but not exhaustive:

a) key management;

b) encipherment management;

c) digital signature management;

d) access control management;

e) data integrity management;

f) authentication management;

g) traffic padding management;

h) routing control management; and

j) notarization management.

Each of the listed security mechanism management functions is discussed in more detail in § 8.4.

8.2.4 *Security of OSI management*

Security of all OSI management functions and of the communication of OSI management information are important parts of OSI security. This category of security management will invoke appropriate choices of the listed OSI security services and mechanisms in order to ensure that OSI management protocols and information are adequately protected (see § 8.1.5). For example, communications between management entities involving the management information base will generally require some form of protection.

8.3 *Specific system security management activities*

8.3.1 *Event handling management*

The management aspects of event handling visible in OSI are the remote reporting of apparent attempts to violate system security and the modification of thresholds used to trigger event reporting.

8.3.2 *Security audit management*

Security audit management may include:

a) the selection of events to be logged and/or remotely collected;

b) the enabling and disabling of audit trail logging of selected events;

c) the remote collection of selected audit records; and

d) the preparation of security audit reports.

8.3.3 *Security recovery management*

Security recovery management may include:

a) maintenance of the rules used to react to real or suspected security violations;

b) the remote reporting of apparent violations of system security;

c) security administrator interactions.

8.4 *Security mechanism management functions*

8.4.1 *Key management*

Key management may involve:

a) generating suitable keys at intervals commensurate with the level of security required;

b) determination, in accordance with access control requirements, of which entities should receive a copy of each key; and

c) making available or distributing the keys in a secure manner to entity instances in real open systems.

It is understood that some key management functions will be performed outside the OSI environment. These include the physical distribution of keys by trusted means.

Exchange of working keys for use during an association is a normal layer protocol function. Selection of working keys may also be accomplished by access to a key distribution centre or by pre-distribution via management protocols.

8.4.2 *Encipherment management*

Encipherment management may involve:

a) interaction with key management;

b) establishment of cryptographic parameters;

c) cryptographic synchronization.

The existence of an encipherment mechanism implies the use of key management and of common ways to reference the cryptographic algorithms.

The degree of discrimination of protection afforded by encipherment is determined by which entities within the OSI environment are independently keyed. This is in turn determined, in general, by the security architecture and specifically by the key management mechanism.

A common reference for cryptographic algorithms can be obtained by using a register for cryptographic algorithms or by prior agreements between entities.

8.4.3 *Digital signature management*

Digital signature management may involve:

a) interaction with key management;

b) establishment of cryptographic parameters and algorithms; and

c) use of protocol between communicating entities and possibly a third party.

Note – Generally, there exist strong similarities between digital signature management and encipherment management.

8.4.4 *Access control management*

Access control management may involve distribution of security attributes (including passwords) or updates to access control lists or capabilities lists. It may also involve the use of a protocol between communicating entities and other entities providing access control services.

8.4.5 *Data integrity management*

Data integrity management may involve:

a) interaction with key management;

b) establishment of cryptographic parameters and algorithms; and

c) use of protocol between communicating entities.

Note – When using cryptographic techniques for data integrity, there exist strong similarities between data integrity management and encipherment management.

8.4.6 *Authentication management*

Authentication management may involve distribution of descriptive information, passwords or keys (using key management) to entities required to perform authentication. It may also involve use of a protocol between communicating entities and other entities providing authentication services.

8.4.7 *Traffic padding management*

Traffic padding management may include maintenance of the rules to be used for traffic padding. For example this may include:

a) pre-specified data rates;

b) specifying random data rates;

c) specifying message characteristics such as length; and

d) variation of the specification, possibly in accordance with time of day and/or calendar.

8.4.8 *Routing control management*

Routing control management may involve the definition of the links or sub-networks which are considered to be either secured or trusted with respect to particular criteria.

8.4.9 *Notarization management*

Notarization management may include:

a) the distribution of information about notaries;

b) the use of a protocol between a notary and the communicating entities; and

c) interaction with notaries.

ANNEX A

Background information on security in OSI

(This annex does not form an integral part of this Recommendation)

A.1 *Background*

This annex provides:

a) information on OSI security in order to give some perspective to this Recommendation; and

b) background on the architectural implications of various security features and requirements.

Security in an OSI environment is just one aspect of data processing/data communications security. If they are to be effective the protective measures used in an OSI environment require supporting measures which lie outside OSI. For example, information flowing between systems may be enciphered but if no physical security restrictions are placed on access to the systems themselves, encipherment may be in vain. Also, OSI is concerned only with the interconnection of systems. For OSI security measures to be effective they shall be used in conjunction with measures that fall outside the scope of OSI.

A.2 *The requirement for security*

A.2.1 *What is meant by security?*

The term “security” is used in the sense of minimizing the vulnerabilities of assets and resources. An asset is anything of value. A vulnerability is any weakness that could be exploited to violate a system or the information it contains. A threat is a potential violation of security.

A.2.2 *The motivation for security in open systems*

CCITT has identified a need for a series of Recommendations to enhance security within the Open Systems Interconnection architecture. This stems from:

a) society's increasing dependence on computers that are accessed by, or linked by, data communications and which require protection against various threats;

b) the appearance in several countries of “data protection” legislation which obliges suppliers to demonstrate system integrity and privacy; and

c) the wish of various organizations to use OSI recommendations, enhanced as needed, for existing and future secure systems.

A.2.3 *What is to be protected?*

In general, the following may require protection:

a) information and data (including software and passive data related to security measures such as passwords);

b) communication and data processing services; and

c) equipment and facilities.

A.2.4 *Threats*

The threats to a data communication system include the following:

a) destruction of information and/or other resources;

b) corruption or modification of information;

c) theft, removal or loss of information and/or other resources;

d) disclosure of information; and

e) interruption of services.

Threats can be classified as accidental or intentional and may be active or passive.

A.2.4.1 *Accidental threats*

Accidental threats are those that exist with no premeditated intent. Examples of realized accidental threats include system malfunctions, operational blunders and software bugs.

A.2.4.2 *Intentional threats*

Intentional threats may range from casual examination using easily available monitoring tools to sophisticated attacks using special system knowledge. An intentional threat, if realized, may be considered to be an "attack".

A.2.4.3 *Passive threats*

Passive threats are those which, if realized, would not result in any modification to any information contained in the system(s) and where neither the operation nor the state of the system is changed. The use of passive wire tapping to observe information being transmitted over a communications line is a realization of a passive threat.

A.2.4.4 *Active threats*

Active threats to a system involve the alteration of information contained in the system, or changes to the state or operation of the system. A malicious change to the routing tables of a system by an unauthorized user is an example of an active threat.

A.2.5 *Some specific types of attack*

The following briefly reviews some of the attacks of particular concern in a data processing/data communications environment. In the following sections, the terms authorized and unauthorized appear. "Authorization" means "the granting of rights". Two things implied by this definition are: that the rights are rights to perform some activity (such as to access data); and that they have been granted to some entity, human agent, or process. Authorized behaviour, then, is the performance of those activities for which rights have been granted (and not revoked). For more about the concept of authorization see § A.3.3.1.

A.2.5.1 *Masquerade*

A masquerade is where an entity pretends to be a different entity. A masquerade is usually used with some other forms of active attack, especially replay and modification of messages. For instance, authentication sequences can be captured and replayed after a valid authentication sequence has taken place. An authorized entity with few privileges may use a masquerade to obtain extra privileges by impersonating an entity that has those privileges.

A.2.5.2 *Replay*

A replay occurs when a message, or part of a message, is repeated to produce an unauthorized effect. For example, a valid message containing authentication information may be replayed by another entity in order to authenticate itself (as something that it is not).

A.2.5.3 *Modification of messages*

Modification of a message occurs when the content of a data transmission is altered without detection and results in an unauthorized effect, as when, for example, a message "Allow 'John Smith' to read confidential file 'Accounts'" is changed to "Allow 'Fred Brown' to read confidential file 'Accounts'".

A.2.5.4 *Denial of service*

Denial of service occurs when an entity fails to perform its proper function or acts in a way that prevents other entities from performing their proper functions. The attack may be general, as when an entity suppresses all messages, or there may be a specific target, as when an entity suppresses all messages directed to a particular destination, such as the security audit service. The attack may involve suppressing traffic as described in this example or it may generate extra traffic. It is also possible to generate messages intended to disrupt the operation of the network, especially if the network has relay entities that make routing decisions based upon status reports received from other relay entities.

A.2.5.5 *Insider attacks*

Insider attacks occur when legitimate users of a system behave in unintended or unauthorized ways. Most known computer crime has involved insider attacks that compromised the security of the system. Protection methods that can be used against insider attacks include:

a) careful vetting of staff;

b) scrutinization of hardware, software, security policy and system configurations so that there is a degree of assurance that they will operate correctly (called trusted functionality); and

c) audit trails to increase the likelihood of detecting such attacks.

A.2.5.6 *Outsider attacks*

Outsider attacks may use techniques such as:

a) wire tapping (active and passive);

b) intercepting emissions;

c) masquerading as authorized users of the system or as components of the system; and

d) bypassing authentication or access control mechanisms.

A.2.5.7 *Trapdoor*

When an entity of a system is altered to allow an attacker to produce an unauthorized effect on command or at a predetermined event or sequence of events, the result is called a trapdoor. For example, a password validation could be modified so that, in addition to its normal effect, it also validates an attacker's password.

A.2.5.8 *Trojan horse*

When introduced to the system, a Trojan horse has an unauthorized function in addition to its authorized function. A relay that also copies messages to an unauthorized channel is a Trojan Horse.

A.2.6 *Assessment of threats, risks and countermeasures*

Security features usually increase the cost of a system and may make it harder to use. Before designing a secure system, therefore, one should identify the specific threats against which protection is required. This is known as threat assessment. A system is vulnerable in many ways but only some of them are exploitable because the attacker lacks the opportunity, or because the result does not justify the effort and risk of detection. Although detailed issues of threat assessment are beyond the scope of this annex, in broad outline they include:

a) identifying the vulnerabilities of the system;

b) analysing the likelihood of threats aimed at exploiting these vulnerabilities;

c) assessing the consequences if each threat were to be successfully carried out;

d) estimating the cost of each attack;

e) costing out potential countermeasures; and

f) selecting the security mechanisms that are justified (possibly by using cost benefit analysis).

Non-technical measures, such as insurance coverage, may be cost effective alternatives to technical security measures. Perfect technical security, like perfect physical security, is not possible. The objective, therefore, should be to make the cost of an attack high enough to reduce the risk to acceptable levels.

A.3 *Security policy*

This section discusses security policy: the need for a suitably defined security policy; its role; policy approaches in use; and refinements to apply in specific situations. The concepts are then applied to communications systems.

A.3.1 *The need for and purpose of security policy*

The whole field of security is both complex and far-reaching. Any reasonably complete analysis will yield a daunting variety of details. A suitable security policy should focus attention on those aspects of a situation that the highest level of authority considers should receive attention. Essentially, a security policy states, in general terms, what is and is not permitted in the field of security during the general operation of the system in question. Policy is usually not specific; it suggests what is of paramount importance without saying precisely how the desired results are to be obtained. Policy sets the topmost level of a security specification.

A.3.2 *Implications of policy definition: the refinement process*

Because policy is so general it is not at all clear at the outset how the policy can be married to a given application. Often, the best way to accomplish this is to subject the policy to a successive refinement adding more details from the application at each stage. To know what those details ought to be requires a detailed study of the application area in the light of the general policy. This examination should define the problems arising from trying to impose the conditions of the policy on the application. The refinement process will produce the general policy restated in very precise terms directly drawn from the application. This re-stated policy makes it easier to determine the implementation detail.

A.3.3 *Security policy components*

There are two aspects to existing security policies. Both depend on the concept of authorized behaviour.

A.3.3.1 *Authorization*

The threats already discussed all involve the notion of authorized or unauthorized behaviour. The statement as to what constitutes authorization is embodied in the security policy. A generic security policy might say "information may not be given to, accessed by, or permitted to be inferred by, nor may any resource be used by, those not appropriately authorized." The nature of authorization is what distinguishes various policies. Policies can be divided into two separate components, based upon the nature of the authorization involved, as either rule-based policies or identity-based policies. The first of these uses of rules based on a small number of general attributes or sensitivity classes, that are universally enforced. The second involves authorization criteria based on specific, individualized attributes. Some attributes are assumed to be permanently associated with the entity to which they apply; others may be possessions, (such as capabilities) that can be transmitted to other entities. One can also distinguish between administratively-imposed and dynamically-selected authorization service. A security policy will determine those elements of system security that are always applied and in force (for example, the rule-based and identity-based security policy components, if any) and those that the user may choose to use as he sees fit.

A.3.3.2 *Identity-based security policy*

The identity-based aspect of security policies corresponds, in part, to the security concept known as "need-to-know". The goal is to filter access to data or resources. There are essentially two fundamental ways of implementing identity-based policies, depending on whether the information about access rights is held by the accessors or is part of the data that are accessed. The former is exemplified by the ideas of privileges or capabilities, given to users and used by processes acting on their behalf. Access control lists (ACLs) are examples of the latter. In both cases, the size of the data item (from a full file to a data element) that may be named in a capability or that carried its own ACL may be highly variable.

A.3.3.3 *Ruled-based security policy*

Authorization in rule-based security policy usually rests on sensitivity. In a secure system, data and/or resources should be marked with security labels. Processes acting on behalf of human users may acquire the security label appropriate to their originators.

A.3.4 *Security policy, communications and labels*

The concept of labelling is important in a data communications environment. Labels carrying attributes play a variety of roles. There are data items that move during communication; there are processes and entities that initiate communication, and those that respond; and there are channels and other resources of the system itself, used during communication. All may be labelled, one way or another, with their attributes. Security policies must indicate how the

attributes of each can be used to provide requisite security. Negotiations may be necessary to establish the proper security significance of particular labelled attributes. When security labels are attached both to accessing processes and to accessed data, the additional information needed to apply identity-based access control should be in relevant labels. When a security policy is based upon the identity of the user accessing the data, either directly or through a process, then security labels should include information about the user's identity. The rules for particular labels should be expressed in a security policy in the security management information base (SMIB) and/or negotiated with end systems, as required. The label may be suffixed by attributes that qualify its sensitivity, specify handling and distribution caveats, constrain timing and disposition, and spell out requirements specific to the end system.

A.3.4.1 *Process labels*

In authentication, the full identification of those processes or entities initiating and responding to an instance of communication, together with all appropriate attributes are, typically, of fundamental importance. SMIBs will therefore contain sufficient information about those attributes important to any Administration-imposed policy.

A.3.4.2 *Data item labels*

As data items move during instances of communication, each will be tightly bound to its label. (This binding is significant and, in some instances of rule-based policies, it is a requirement that the label be made a special part of the data item before it is presented to the application.) Techniques to preserve the integrity of the data item will also maintain the accuracy and the coupling of the label. These attributes can be used by the routing control functions in the data link layer of the OSI Basic Reference Model.

A.4 *Security mechanisms*

A security policy may be implemented using various mechanisms, singly or in combination, depending on the policy objectives and the mechanisms used. In general, a mechanism will belong to one of three (overlapping) classes:

a) prevention;

b) detection; and

c) recovery.

Security mechanisms appropriate to a data communications environment are discussed below.

A.4.1 *Cryptographic techniques and encipherment*

Cryptography underlies many security services and mechanisms. Cryptographic functions may be used as part of encipherment, decipherment, data integrity, authentication exchanges, password storage and checking, etc. to help achieve confidentiality, integrity, and/or authentication. Encipherment, used for confidentiality, transforms sensitive data (i.e. data to be protected) to less sensitive forms. When used for integrity or authentication, cryptographic techniques are used to compute unforceable functions.

Encipherment is performed initially on cleartext to produce ciphertext. The result of decipherment is either cleartext, or ciphertext under some cover. It is computationally feasible to use cleartext for general-purpose processing; its semantic content is accessible. Except in specified ways, (e.g. primarily decipherment, or exact matching) it is not computationally feasible to process ciphertext as its semantic content is hidden. Encipherment is sometimes intentionally irreversible (e.g. by truncation or data loss) when it is undesirable ever to derive original cleartext such as passwords.

Cryptographic functions use cryptovariables and operate over fields, data units, and/or streams of data units. Two cryptovariables are the key, which directs specific transformations, and the initialization variable, which is required in certain cryptographic protocols to preserve the apparent randomness of ciphertext. The key must usually remain confidential and both the cryptographic function and the initialization variable may increase delay and bandwidth consumption. This complicates “transparent” or “drop-in” cryptographic add-ons to existing systems.

Cryptographic variables can be symmetric or asymmetric over both encipherment and decipherment. Keys used in asymmetric algorithms are mathematically related; one key cannot be computed from the other. These algorithms are sometimes called “public key” algorithms because one key can be made public while the other kept secret.

Ciphertext can be cryptoanalysed when it is computationally feasible to recover cleartext without knowing the key. This may happen if a weak or defective cryptographic function is used. Interceptions and traffic analysis can lead to attacks on the cryptosystem including message/field insertion, deletion and change, playback of previously valid ciphertext and masquerade.

Therefore, cryptographic protocols are designed to resist attacks and also, sometimes, traffic analysis. A specific traffic analysis countermeasure, “traffic flow confidentiality”, aims to conceal the presence or absence of data and its characteristics. If ciphertext is relayed, the address must be in the clear at relays and gateways. If the data are enciphered only on each link, and are deciphered (and thus vulnerable) in the relay or gateway, the architecture is said to use “link-by-link encipherment”. If only the address (and similar control data) are in the clear in the relay or gateway, the architecture is said to use ”end-to-end encipherment”. End-to-end encipherment is more desirable from a security point of view, but considerably more complex architecturally, especially if in-band electronic key distribution (a function of key management) is included. Link-by-link encipherment and end-to-end encipherment may be combined to achieve multiple security objectives. Data integrity is often achieved by calculating a cryptographic checkvalue. The checkvalue may be derived in one or more steps and is a mathematical function of the cryptovariables and the data. These checkvalues are associated with the data to be guarded. Cryptographic checkvalues are sometimes called manipulation detection codes.

Cryptographic techniques can provide, or help provide, protection against:

a) message stream observation and/or modification;

b) traffic analysis;

c) repudiation;

d) forgery;

e) unauthorized connection; and

f) modification of messages.

A.4.2 *Aspects of key management*

Key management is implied by the use of cryptographic algorithms. Key management encompasses the generation, distribution and control of cryptographic keys. The choice of a key management method is based upon the participants' assessment of the environment in which it is to be used. Considerations of this environment include the threats to be protected against (both internal to the organization and external), the technologies used, the architectural structure and location of the cryptographic services provided, and the physical structure and location of the cryptographic service providers.

Points to be considered concerning key management include:

a) the use of a "lifetime" based on time, use, or other criteria, for each key defined, implicitly or explicitly;

b) the proper identification of keys according to their function so that their use may be reserved only for their function, e.g., keys intended to be used for a confidentiality service should not be used for an integrity service or vice versa; and

c) non-OSI considerations, such as the physical distribution of keys and archiving of keys.

Points to be considered concerning key management for symmetric key algorithms include:

a) the use of a confidentiality service in the key management protocol to convey the keys;

b) the use of a key hierarchy. Different situations should be allowed such as:

   1) "flat" key hierarchies using only data-enciphering keys, implicitly or explicitly selected from a set by key identity or index;

   2) multilayer key hierarchies; and

   3) key-encrypting keys should never be used to protect data and data-encrypting keys should never be used to protect key-encrypting keys;

c) the division of responsibilities so that no one person has a complete copy of an important key.

Points to be considered concerning key management for asymmetric key algorithms include:

a) the use of a confidentiality service in the key management protocol to convey the secret keys; and

b) the use of an integrity service, or of a non-repudiation service with proof of origin, in the key management protocol to convey the public keys. These services may be provided through the use of symmetric and/or asymmetric cryptographic algorithms.

A.4.3 *Digital signature mechanisms*

The term digital signature is used to indicate a particular technique which can be used to provide security services such as non-repudiation and authentication. Digital signature mechanisms require the use of asymmetric cryptographic algorithms. The essential characteristic of the digital signature mechanism is that the signed data unit cannot be created without using the private key. This means that:

a) the signed data unit cannot be created by any individual except the holder of the private key, and

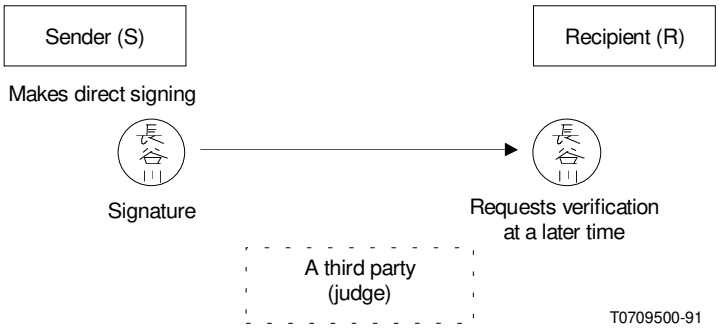
b) the recipient cannot create the signed data unit.

Therefore, using publicly available information only, it is possible to identify the signer of a data unit uniquely as the possessor of the private key. In the case of later conflict between participants it is thus possible to prove the identity of the signer of a data unit to a reliable third party, who is called upon to judge the authenticity of the signed data unit. This type of digital signature is called direct signature scheme (see Figure A-1/X.800). In other cases, an additional property c) might be needed:

c) the sender cannot deny sending the signed data unit.

A reliable third party (arbitrator) proves to the recipient the source and integrity of the information in this case. This type of digital signature is sometimes arbitrated signature scheme (see Figure A-2/X.800).

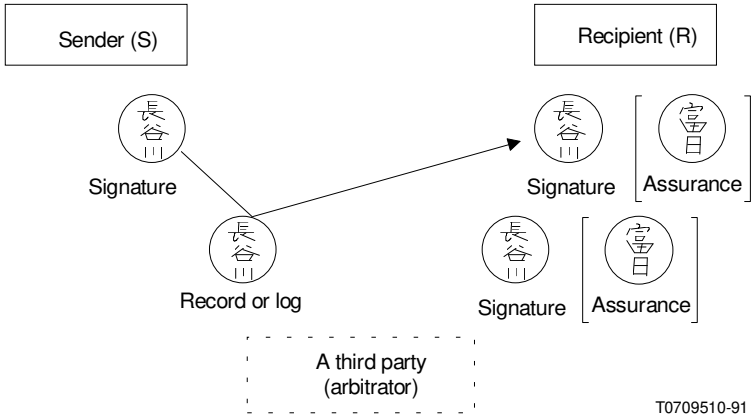
Note – The sender may require that the recipient cannot later deny receiving the signed data unit. This can be accomplished with a non-repudiation service with proof of delivery by means of an appropriate combination of digital signature, data integrity and notarization mechanisms.



Note — Verifies the signature when a conflict arises between the participants (S may be a perjurer or R may be a perjurer).

FIGURE A-1/X.800

Direct signature scheme



Note — A third party authenticates the source (and gives assurance (i.e., positive result) for the recipient). Necessary information to prove the source and integrity of data is logged by a third party. In this case, S cannot later successfully deny sending the signed data unit.

FIGURE A-2/X.800

Arbitrated signature scheme

A.4.4 *Access control mechanisms*

Access control mechanisms are those mechanisms which are used to enforce a policy of limiting access to a resource to only those users who are authorized. Techniques include the use of access control lists or matrices (which usually contain the identities of controlled items and authorized users e.g. people or processes), passwords, and capabilities, labels or tokens, the possession of which may be used to indicate access rights. Where capabilities are used, they should be unforceable and should be conveyed in a trusted manner.

A.4.5 *Data integrity mechanisms*

Data integrity mechanisms are of two types: those used to protect the integrity of a single data unit and those that protect both the integrity of single data units and the sequence of an entire stream of data units on a connection.

A.4.5.1 *Message stream modification detection*

Corruption detection techniques, normally associated with detection of bit errors, block errors and sequencing errors introduced by communications links and networks, can also be used to detect message stream modification. However, if protocol headers and trailers are not protected by integrity mechanisms, an informed intruder can successfully bypass these checks. Successful detection of message stream modification can thus be achieved only by using corruption detection techniques in conjunction with sequence information. This will not prevent message stream modification but will provide notification of attacks.

A.4.6 *Authentication exchange mechanisms*

A.4.6.1 *Choice of mechanism*

There are many choices and combinations of authentication exchange mechanisms appropriate to different circumstances. For instance:

a) When peer entities and the means of communication are both trusted, the identification of a peer entity can be confirmed by a password. The password protects against error, but is not proof against malevolence, (specifically, not against replay). Mutual authentication may be accomplished by using a distinct password in each direction.

b) When each entity trusts its peer entities but does not trust the means of communication, protection against active attacks can be provided by combinations of passwords and encipherment or by cryptographic means. Protection against replay attacks requires two-way handshakes (with protection parameters) or time stamping (with trusted clocks). Mutual authentication with replay protection can be achieved using three-way handshakes.

c) When entities do not (or feel that they may not in the future) trust their peers or the means of communication, non-repudiation services can be used. The non-repudiation service can be achieved using digital signature and/or notarization mechanisms. These mechanisms can be used with the mechanisms described in b) above.

A.4.7 *Traffic padding mechanisms*

Generating spurious traffic and padding protocol data units to a constant length can provide limited protection against traffic analysis. To be successful, the level of spurious traffic must approximate to the highest anticipated level of real traffic. In addition, the contents of the protocol data units must be enciphered or disguised so that spurious traffic cannot be identified and differentiated from real traffic.

A.4.8 *Routing control mechanism*

The specification of routing caveats for the transfer of data (including the specification of an entire route) may be used to ensure that data is conveyed only over routes that are physically secure or to ensure that sensitive information is carried only over routes with an appropriate level of protection.

A.4.9 *Notarization mechanism*

The notarization mechanism is based on the concept of a trusted third party (a notary) to assure certain properties about information exchanged between two entities, such as its origin, its integrity, or the time it was sent or received.

A.4.10 *Physical and personnel security*

Physical security measures will always be necessary to ensure complete protection. Physical security is costly, and attempts are often made to minimize the need for it by using other (cheaper) techniques. Physical and personnel security considerations are outside the scope of OSI, although all systems will ultimately rely on some form of physical security and on the trustworthiness of the personnel operating the system. Operating procedures should be defined to ensure proper operation and to delineate personnel responsibilities.

A.4.11 *Trusted hardware/software*

Methods used to gain confidence in the correct functioning of an entity include formal proof methods, verification and validation, detection and logging of known attempted attacks, and the construction of the entity by trusted personnel in a secure environment. Precautions are also needed to ensure that the entity is not accidentally or deliberately modified so as to compromise security during its operational life, for example, during maintenance or upgrade. Some entities in the system must also be trusted to function correctly if security is to be maintained. The methods used to establish trust are outside the scope of OSI.

ANNEX B

Justification for security service and mechanisms placement in § 7

(This annex does not form an integral part of this Recommendation)

B.1 *General*

This annex provides some reasons for providing the identified security services within the various layers as indicated in § 7. The security layering principles identified in § 6.1.1 of the standard have governed this selection process.

A particular security service is provided by more than one layer if the effect on general communication security can be considered as different (e.g. connection confidentiality at layers 1 and 4). Nevertheless, considering existing OSI data communication functionalities, (e.g. multilink procedures, multiplexing function, different ways to enhance a connectionless service to a connection-oriented one) and in order to allow these transmission mechanisms to operate, it may be necessary to allow a particular service to be provided at another layer, though the effect on security cannot be considered as different.

B.2 *Peer entity authentication*

– *Layers 1 and 2:* No, peer entity authentication is not considered useful in these layers.

– *Layer 3:* Yes, over individual sub-networks and for routing and/or over the internetwork.

– *Layer 4:* Yes, end system to end system authentication in layer 4 can serve to mutually authenticate two or more session entities, prior to the commencement of a connection, and for the duration of that connection.

– *Layer 5:* No, there are no benefits over providing this at layer 4 and/or higher layers.

– *Layer 6:* No, but encipherment mechanisms can support this service in the application layer.

– *Layer 7:* Yes, peer entity authentication should be provided by the application layer.

B.3 *Data origin authentication*

– *Layers 1 and 2:* No, data origin authentication is not considered useful in these layers.

– *Layers 3 and 4:* Data origin authentication can be provided end-to-end in the relaying and routing role of layer 3 and/or in layer 4 as follows:

a) the provision of peer entity authentication at connection establishment time together with encipherment-based continuous authentication during the life of a connection provides, *de facto*, the data origin authentication service; and

b) even where a) is not provided, encipherment-based data origin authentication can be provided with very little additional overhead to the data integrity mechanisms already placed in these layers.

– *Layer 5:* No, there are no benefits over providing this at layer 4 or layer 7.

– *Layer 6:* No, but encipherment mechanisms can support this in the application layer.

– *Layer 7:* Yes, possibly in conjunction with mechanisms in the presentation layer.

B.4 *Access control*

– *Layers 1 and 2:* Access control mechanisms cannot be provided at layers 1 or 2 in a system conforming to full OSI protocols, since there are no end facilities available for such a mechanism.

– *Layer 3:* Access control mechanisms may be imposed on the sub-network access role by the requirements of a particular sub-network. When performed by the relaying and routing role, access mechanisms in the network layer can be used both to control accesses to sub-networks by relay entities and to control access to end systems. Clearly, the granularity of access is fairly coarse, distinguishing only between network layer entities.

The establishment of a network connection may often result in charges by the sub-network administration. Cost minimization can be performed by controlling access and by selecting reverse charging or other network or sub-network specific parameters.

– *Layer 4:* Yes, access control mechanisms can be employed upon a per transport connection end-to-end basis.

– *Layer 5:* No, there are no benefits over providing this at layer 4 and/or layer 7.

– *Layer 6:* No, this is not appropriate at layer 6.

– *Layer 7:* Yes, application protocols and/or application processes can provide application-oriented access control facilities.

B.5 *Confidentiality of all (N)-user-data on an (N)-connection*

– *Layer 1:* Yes, should be provided since the electrical insertion of transparent pairs of transformation devices can give complete confidentiality upon a physical connection.

– *Layer 2*: Yes, but it provides no additional security benefits over confidentiality at layer 1 or layer 3.

– *Layer 3:* Yes, for sub-network access role over individual sub-networks and for relaying and routing roles over the internetwork.

– *Layer 4:* Yes, since the individual transport connection gives an end-to-end transport mechanism and can provide isolation of session connections.

– *Layer 5:* No, since it provides no additional benefit over confidentiality at layers 3, 4 and 7. It does not appear appropriate to provide this service at this layer.

– *Layer 6:* Yes, since encipherment mechanisms provide purely syntactic transformations.

– *Layer 7:* Yes, in conjunction with mechanisms at lower layers.

B.6 *Confidentiality of all (N)-user-data in a single, connectionless (N)-SDU*

The justification is as for confidentiality of all (N)-user-data except for layer 1 where there is no connectionless service.

B.7 *Confidentiality of selective fields within the (N)-user-data of an SDU*

This confidentiality service is provided by encipherment in the presentation layer and is invoked by mechanisms in the application layer according to the semantics of the data.

B.8 *Traffic flow confidentiality*

Full traffic flow confidentiality can be achieved only at layer 1. This can be achieved by the physical insertion of a pair of encipherment devices into the physical transmission path. It is assumed that the transmission path will be two-way simultaneous and synchronous so that the insertion of the devices will render all transmissions (and even their presence) upon the physical media unrecognizable.

Above the physical layer, full traffic flow security is not possible. Some of its effects can be partly produced by the use of a complete SDU confidentiality service at one layer and the injection of spurious traffic at a high layer. Such a mechanism is costly, and potentially consumes large amounts of carrier and switching capacity.

If traffic flow confidentiality is provided at layer 3, traffic padding and/or routing control will be used. Routing control may provide limited traffic flow confidentiality by routing messages around insecure links or sub-networks. However, the incorporation of traffic padding into layer 3 enables better use of the network to be achieved, for example, by avoiding unnecessary padding and network congestion.

Limited traffic flow confidentiality can be provided at the application layer by the generation of spurious traffic, in conjunction with confidentiality to prevent identification of the spurious traffic.

B.9 *Integrity of all (N)-user-data on an (N)-connection (with error recovery)*

– *Layers 1 and 2:* Layers 1 and 2 are not able to provide this service. Layer 1 has no detection or recovery mechanisms, and the layer 2 mechanism operates only on a point-to-point basis, not an end-to-end basis and, therefore, is not considered appropriate to provide this service.

– *Layer 3:* No, since error recovery is not universally available.

– *Layer 4:* Yes, since this provides the true end-to-end transport connection.

– *Layer 5:* No, since error recovery is not a function of layer 5.

– *Layer 6:* No, but encipherment mechanisms can support this service in the application layer.

– *Layer 7:* Yes, in conjunction with mechanisms in the presentation layer.

B.10 *Integrity of all (N)-user-data on an (N)-connection (no error recovery)*

- *Layers 1 and 2:* Layers 1 and 2 are not able to provide this service. Layer 1 has no detection or recovery mechanisms, and the layer 2 mechanism operates only on a point-to-point basis, not an end-to-end basis and, therefore, is not considered appropriate to provide this service.

- *Layer 3:* Yes, for sub-network access role over individual sub-networks and for routing and relay roles over the internetwork.

- *Layer 4:* Yes, for those cases of use where it is acceptable to cease communication after detection of an active attack.

- *Layer 5:* No, since it provides no additional benefit over data integrity at layers 3, 4 or 7.

- *Layer 6:* No, but encipherment mechanisms can support this service in the application layer.

- *Layer 7:* Yes, in conjunction with mechanisms in the presentation layer.

B.11 *Integrity of selected fields within the (N)-user-data of (N)-SDU transferred over an (N)-connection (without recovery)*

Integrity of selected fields can be provided by encipherment mechanisms in the presentation layer in conjunction with invocation and checking mechanisms in the application layer.

B.12 *Integrity of all (N)-user-data in a single connectionless (N)-SDU*

In order to minimize the duplication of functions, the integrity of connectionless transfers should be provided only at the same layers as for integrity without recovery, i.e. at the network, transport and application layers. Such integrity mechanisms can be of only very limited effectiveness, and this must be realized.

B.13 *Integrity of selected fields in a single connectionless (N)-SDU*

Integrity of selected fields can be provided by encipherment mechanisms in the presentation layer in conjunction with invocation and checking mechanisms in the application layer.

B.14 *Non-repudiation*

Origin and delivery non-repudiation services can be provided by a notarization mechanism which will involve a relay at layer 7.

Use of the digital signature mechanism for non-repudiation requires a close cooperation between layers 6 and 7.

ANNEX C

Choice of position of encipherment for applications

(This annex does not form an integral part of this Recommendation)

C.1 Most applications will not require encipherment to be used at more than one layer. The choice of layer depends on some major issues as described below:

1) If full traffic flow confidentiality is required, physical layer encipherment or transmission security (e.g. suitable spread spectrum techniques) will be chosen. Adequate physical security and trusted routing and similar functionality at relays can satisfy all confidentiality requirements.

2) If a high granularity of protection is required (i.e. potentially a separate key for each application association) and nonrepudiation or selective field protection then presentation layer encipherment will be chosen. Selective field protection can be important because encipherment algorithms consume large amounts of processing power. Encipherment in the presentation layer can provide integrity without recovery, non-repudiation, and all confidentiality.

3) If simple bulk protection of all end-system to end-system communications and/or an external encipherment device is desired (e.g. in order to give physical protection to algorithm and keys or protection against faulty software), then network layer encipherment will be chosen. This can provide confidentiality and integrity without recovery.

   Note – Although recovery is not provided in the network layer, the normal recovery mechanisms of the transport layer can be used to recover from attacks detected by the network layer.

4) If integrity with recovery is required together with a high granularity of protection, then transport layer encipherment will be chosen. This can provide confidentiality and integrity, with or without recovery.

5) Encipherment at the data link layer is not recommended for future implementations.

C.2 When two or more of these key issues are of concern, encipherment may need to be provided in more than one layer.