INTERNATIONAL TELECOMMUNICATION UNION

ITU-T X.814

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(11/95)

DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

SECURITY

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – SECURITY FRAMEWORKS FOR OPEN SYSTEMS: CONFIDENTIALITY FRAMEWORK

ITU-T Recommendation X.814

(Previously "CCITT Recommendation")

FOREWORD

ITU (International Telecommunication Union) is the United Nations Specialized Agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of the ITU. Some 179 member countries, 84 telecom operating entities, 145 scientific and industrial organizations and 38 international organizations participate in ITU-T which is the body which sets world telecommunications standards (Recommendations).

The approval of Recommendations by the Members of ITU-T is covered by the procedure laid down in WTSC Resolution No. 1 (Helsinki, 1993). In addition, the World Telecommunication Standardization Conference (WTSC), which meets every four years, approves Recommendations submitted to it and establishes the study programme for the following period.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC. The text of ITU-T Recommendation X.814 was approved on 21st of November 1995. The identical text is also published as ISO/IEC International Standard 10181-5.

NOTE

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

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS

(February 1994)

ORGANIZATION OF X-SERIES RECOMMENDATIONS

Subject area	Recommendation Series
PUBLIC DATA NETWORKS	
Services and Facilities	X.1-X.19
Interfaces	X.20-X.49
Transmission, Signalling and Switching	X.50-X.89
Network Aspects	X.90-X.149
Maintenance	X.150-X.179
Administrative Arrangements	X.180-X.199
OPEN SYSTEMS INTERCONNECTION	
Model and Notation	X.200-X.209
Service Definitions	X.210-X.219
Connection-mode Protocol Specifications	X.220-X.229
Connectionless-mode Protocol Specifications	X.230-X.239
PICS Proformas	X.240-X.259
Protocol Identification	X.260-X.269
Security Protocols	X.270-X.279
Layer Managed Objects	X.280-X.289
Conformance Testing	X.290-X.299
INTERWORKING BETWEEN NETWORKS	
General	X.300-X.349
Mobile Data Transmission Systems	X.350-X.369
Management	X.370-X.399
MESSAGE HANDLING SYSTEMS	X.400-X.499
DIRECTORY	X.500-X.599
OSI NETWORKING AND SYSTEM ASPECTS	
Networking	X.600-X.649
Naming, Addressing and Registration	X.650-X.679
Abstract Syntax Notation One (ASN.1)	X.680-X.699
OSI MANAGEMENT	X.700-X.799
SECURITY	X.800-X.849
OSI APPLICATIONS	
Commitment, Concurrency and Recovery	X.850-X.859
Transaction Processing	X.860-X.879
Remote Operations	X.880-X.899
OPEN DISTRIBUTED PROCESSING	X.900-X.999

CONTENTS

Summary

This Recommendation defines a general framework for the provision of confidentiality services. Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities or processes.

Introduction

Many Open Systems applications have security requirements which depend upon the prevention of disclosure of information. Such requirements may include the protection of information used in the provision of other security services such as authentication, access controls or integrity, that, if known by an attacker, could reduce or nullify the effectiveness of those services.

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

This Recommendation | International Standard defines a general framework for the provision of confidentiality services.

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – SECURITY FRAMEWORKS FOR OPEN SYSTEMS: CONFIDENTIALITY FRAMEWORK

1 Scope

This Recommendation | International Standard on Security Frameworks for Open Systems addresses the application of security services in an Open Systems environment, where the term "Open System" is taken to include areas such as Database, Distributed Applications, Open Distributed Processing and OSI. The Security Frameworks are concerned with defining the means of providing protection for systems and objects within systems, and with the interactions between systems. The Security Frameworks are not concerned with the methodology for constructing systems or mechanisms.

The Security Frameworks address both data elements and sequences of operations (but not protocol elements) which may be used to obtain specific security services. These security services may apply to the communicating entities of systems as well as to data exchanged between systems, and to data managed by systems.

This Recommendation | International Standard addresses the confidentiality of information in retrieval, transfer and management. It:

1) defines the basic concepts of confidentiality;
2) identifies possible classes of confidentiality mechanisms;
3) classifies and identifies facilities for each class of confidentiality mechanisms;
4) identifies management required to support the classes of confidentiality mechanism; and
5) addresses the interaction of confidentiality mechanism and the supporting services with other security services and mechanisms.

A number of different types of standards can use this framework, including:

1) standards that incorporate the concept of confidentiality;
2) standards that specify abstract services that include confidentiality;
3) standards that specify uses of a confidentiality service;
4) standards that specify means of providing confidentiality within an open system architecture; and
5) standards that specify confidentiality mechanisms.

Such standards can use this framework as follows:

– standards of type 1), 2), 3), 4) and 5) can use the terminology of this framework;
– standards of type 2), 3), 4) and 5) can use the facilities defined in clause 7 of this framework;
– standards of type 5) can be based upon the classes of mechanism defined in clause 8 of this framework.

As with other security services, confidentiality can only be provided within the context of a defined security policy for a particular application. The definitions of specific security policies are outside the scope of this Recommendation | International Standard.

It is not a matter for this Recommendation | International Standard to specify details of the protocol exchanges which need to be performed in order to achieve confidentiality.

This Recommendation | International Standard does not specify particular mechanisms to support these confidentiality services nor the full details of security management services and protocols. Generic mechanisms to support confidentiality are described in clause 8.

Some of the procedures described in this security framework achieve confidentiality by the application of cryptographic techniques. This framework is not dependent on the use of particular cryptographic or other algorithms, although certain classes of confidentiality mechanisms may depend on particular algorithm properties.

NOTE – Although ISO does not standardize cryptographic algorithms, it does standardize the procedures used to register them in ISO/IEC 9979:1991, Procedures for the registration of criptographic algorithms.

This framework addresses the provision of confidentiality when the information is represented by data that are read-accessible to potential attackers. Its scope includes traffic flow confidentiality.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*.
- ITU-T Recommendation X.233 (1993) | ISO/IEC 8473-1:1994, *Information technology – Protocol for providing the connectionless-mode Network service: Protocol specification*.
- ITU-T Recommendation X.273 (1994) | ISO/IEC 11577:1995, *Information technology – Open Systems Interconnection – Network layer security protocol*.
- ITU-T Recommendation X.274 (1994) | ISO/IEC 10736:1995, *Information technology – Telecommunication and information exchange between systems – Transport layer security protocol.*
- ITU-T Recommendation X.810 (1995) | ISO/IEC 10181-1:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Overview.*
- ITU-T Recommendation X.812 (1995) | ISO/IEC 10181-3:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Access control framework.*

2.2 Paired Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*

  ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*

3 Definitions

For the purposes of this Recommendation | International Standard, the following definitions apply.

3.1 Basic Reference Model definitions

This Recommendation | International Standard makes use of the following general security-related terms defined in ITU-T Rec. X.200 | ISO/IEC 7498-1:

a) (N)-connection;

b) (N)-entity;

c) (N)-facility;

d) (N)-layer;

e) (N)-PDU;

f) (N)-SDU;

g) (N)-service;

h) (N)-unitdata;

i) (N)-userdata;

j) segmenting.

3.2 Security architecture definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.800 | ISO 7498-2:

a) active threat;

b) confidentiality;

c) decipherment;

d) decryption;

e) encipherment;

f) encryption;

g) identity-based security policy;

h) key;

i) passive threat;

j) routing control;

k) rule-based security policy;

l) sensitivity;

m) traffic analysis;

n) traffic padding.

3.3 Security frameworks overview definitions

This Recommendation | International Standard makes use of the following general security-related terms defined in ITU-T Rec. X.810 | ISO/IEC 10181-1:

a) secret key;

b) private key;

c) public key.

3.4 Additional definitions

For the purposes of this Recommendation | International Standard, the following definitions apply:

3.4.1 confidentiality-protected-environment: An environment which prevents unauthorized information disclosure either by preventing unauthorized data inspection or by preventing unauthorized derivation of sensitive information through data inspection. Sensitive information may include some or all of the data attributes (e.g. value, size, or existence).

3.4.2 confidentiality-protected-data: Data within a confidentiality-protected-environment.

NOTE – A confidentiality-protected environment may also protect some (or all) of the attributes of the confidentiality-protected data.

3.4.3 confidentiality-protected-information: Information all of whose concrete encodings (i.e. data) are confidentiality protected.

3.4.4 hide: An operation that applies confidentiality protection to unprotected data or additional confidentiality protection to already protected data.

3.4.5 reveal: An operation that removes some or all of previously applied confidentiality protection.

3.4.6 hiding confidentiality information: Information that is used to perform the **hide** operation.

3.4.7 revealing confidentiality information: Information that is used to perform the reveal operation.

3.4.8 direct attack: An attack on a system based on deficiencies in the underlying algorithms, principles, or properties of a security mechanism.

3.4.9 indirect attack: An attack on a system which is not based on the deficiencies of a particular security mechanism (e.g. attacks which bypass the mechanism, or attacks which depend on the system using the mechanism incorrectly).

4 Abbreviations

For the purposes of this Recommendation | International Standard, the following abbreviations apply:

HCI Hiding Confidentiality Information

PDU Protocol Data Unit

RCI Revealing Confidentiality Information

SDU Service Data Unit

5 General discussion of confidentiality

5.1 Basic concepts

The purpose of the confidentiality service is to ensure that information is available only to those authorized. Insofar as information is represented through data and insofar as data may result in contextual changes (e.g. file manipulations may result in directory changes or in changes in the number of available storage locations), information can be derived from data in a number of different ways:

1) by understanding the semantics of the data (e.g. the value of the data);
2) by using the associated attributes of the data (such as existence, date of creation, size, date of last update, etc.) to permit inferencing; and
3) by considering the context of the data, i.e. those other data objects that are associated with it; and
4) by observing the dynamic variations of the representation.

The information can be protected either by ensuring that the data is limited to those authorized or by representing the data in such a way that their semantics remain accessible only to those who possess some critical information. Effective confidentiality protection requires that the necessary control information (such as keys and other RCI) be protected. This protection may be provided by mechanisms that are different from those used to protect the data (e.g. cryptographic keys may be protected by physical means).

The notions of protected environments and of overlapped protected environments are used in this framework. Data within protected environments are protected by the application of a particular security mechanism (or mechanisms). All data within a protected environment are thus similarly protected. When two or more environments overlap, the data in the overlap are multiply protected. It may be deduced that the continuous protection of data that are moved from one environment into another must involve overlapped protected environments.

5.1.1 Protection of information

Communication or storage of information is realized by representing the information as data items. Confidentiality mechanisms protect against the disclosure of information by protecting some or all of the items listed in 5.1 above.

Ways to achieve confidentiality include:

1) prevention of the knowledge of the existence of data or of characteristics of data (such as data size or data creation date);
2) prevention of read-access to data; and
3) prevention of the knowledge of the semantics of data.

Confidentiality mechanisms protect against the disclosure of information by either:

1) protecting the representation of the information item from disclosure; or by

2) protecting the representation rules from disclosure.

In the second case, protection against disclosure of the existence or other attributes of a data item can be achieved by combining several data items into a composite data item and by protecting the representation rules of the composite object from disclosure.

5.1.2 Hide and reveal operations

The **hide** operation can be modeled as a movement of information from an environment A to the overlap (B) of A with another environment C. The reveal operation can be seen as the inverse of a hide operation. This is depicted in Annex B.

When information is moved from an environment protected by one confidentiality mechanism to an environment protected by another confidentiality mechanism:

1) if the **hide** operation of the second mechanism precedes the **reveal** operation of the first, the information is continually protected; and

2) if the **reveal** operation of the first mechanism precedes the **hide** operation of the second mechanism, the information is not continually protected.

For 1) above to be possible, some form of commutativity must exist between the **reveal** of the old mechanism and the **hide** of the new. An example in which **hide** and **reveal** operate with commutative properties occurs when one environment is protected through Access Control or physical means and the other is protected through cryptographic transformations.

Confidentiality impacts information retrieval, transfer, and management as follows:

1) confidentiality in information transfer using OSI is provided when the **hide** operation, transfer using an (N-1)-facility, and the **reveal** operation are combined to form the transmission part of an (N)-service;

2) confidentiality in data storage retrieval is provided when the **hide** operation, storage and retrieval, and the **reveal** operation are combined to form a higher level storage and retrieval service;

3) other forms of confidentiality may be provided by combining **hide** and **reveal** with other operations (e.g. those used for the purposes of data management).

With some confidentiality mechanisms, the **hide** facility makes part of the confidentiality-protected data available to the service user before the facility has completed the processing of all of the data. Similarly, with some mechanisms the **reveal** facility is able to start work on processing part of a confidentiality-protected data item before all of it is available. Thus, a data item may consist simultaneously of parts that are not yet **hidden**, parts that are **hidden**, and parts that have been **revealed**.

5.2 Classes of confidentiality services

Confidentiality services may be classified by the type of information protection they support. The types of information protection are:

1) protection of data semantics;

2) protection of data semantics and of associated attributes;

3) protection of data semantics, of their attributes, and of any information that may be derived from the data in question.

In addition, the service may be classified by the type of threats that exist in the environment in which it operates and against which the information is protected. By this criterion, services can be classified as follows:

1) *Protection against external threats*

   Such services assume that those with legitimate access to the information will not divulge it to those unauthorized. Such services do not protect the information divulged to authorized parties and do not constrain the behaviour of such parties while they possess information previously protected.

   Example: Sensitive files in A are protected through encryption. But processes that possess the required decryption keys may read the protected files and subsequently write to unprotected files.

2) *Protection against internal threats*

Such services assume that those authorized to have access to critical information and data may, willingly or not, carry out activities that eventually compromise the confidentiality of the information to be protected.

Example: Security labels and clearances are attached to the resources that are protected and to the entities that can access them. Accesses are restricted according to a well defined and understood flow control model.

Services that provide confidentiality protection against internal threats must either disallow covert channels (see Annex D) or restrict their information transfer rate within acceptable levels. In addition, they must disallow unauthorized inferences that may come about from the unexpected usage of legitimate information channels [such as inferences based on carefully constructed database queries – each of which is individually legitimate – or inferences based on the (in)ability of a system utility to carry out a command].

5.3 Types of confidentiality mechanisms

The objective of confidentiality mechanisms is to prevent unauthorized information disclosure. To this end, a confidentiality mechanism may:

1) Prevent access to the data (such as physical protection of a channel).

Access Control mechanisms (as described in ITU-T Rec. X.812 | ISO/IEC 10181-3) may be used to enable only authorized entities to have access to the data.

Techniques for physical protection are outside the scope of this Recommendation | International Standard. They are nevertheless included in other standards such as ISO 10202 (Security Architecture of Integrated Circuit Cards) and ANSI X9.17 / ISO 8734 (Financial Institution Key Management – Wholesale).

2) Use mapping techniques that render the information to be protected relatively inaccessible to all but those who possess some critical information about the mapping technique. Such techniques include:

a) encipherment;

b) data padding;

c) spread spectrum.

Confidentiality mechanisms of either type can be used in conjunction with other mechanisms of the same or of different types.

Confidentiality mechanisms can achieve different kinds of protection:

– protection of data semantics;

– protection of data attributes (including the existence of data); or

– protection against inferences.

Examples of these classes of mechanisms include:

1) Encipherment to conceal the data.

2) Encipherment in conjunction with segmenting and padding to conceal the length of PDUs (see 8.2).

3) Spread-spectrum techniques to conceal the existence of a communications channel.

5.4 Threats to confidentiality

There is a single, generic threat to confidentiality-protected information, namely, disclosure of the protected information. There are several threats to confidentiality-protected data, corresponding to the different ways in which confidentiality-protected information can be derived from the data. The following subclauses describe some of the threats to confidentiality-protected data in different environments.

5.4.1 Threats when confidentiality is provided through access prevention

Such threats include:

1) Penetration of the Access prevention mechanism, such as:

a) Exploiting weaknesses in physically protected channels.

b) Masquerading or using certificates inappropriately.

c) Exploiting weaknesses in the implementation of the prevention mechanism (e.g. a user might be able to request access to a file A, be granted access to A, and then modify the file name submitted so as to gain access to another file, B).

d) Embedding Trojan horses within trusted software.

2) Penetration of the services the prevention mechanism relies upon (e.g. masquerading when access is based on identity authentication, improper use of certificates, or penetration of the integrity mechanism used to protect certificates).

3) Exploitation of system utilities that may disclose, directly or indirectly, information about the system.

4) Covert channels.

5.4.2 Threats when confidentiality is provided through information hiding

Such threats include:

1) penetration of the cryptographic mechanism (be it through cryptanalysis, through purloined keys, chosen plaintext attacks, or through other means);

2) traffic analysis;

3) analysis of PDU headers;

4) covert channels.

5.5 Types of confidentiality attacks

To each of the threats enumerated above correspond one or more attacks, i.e. instantiations of the threat in question.

It is possible to distinguish between active and passive attacks, i.e. confidentiality attacks that result in system change and attacks that do not result in system change.

NOTE – Whether an attack is passive or active may be determined both by the characteristics of system under attack and by the actions carried out by the attacker.

Examples of passive attacks are:

1) eavesdropping and wiretapping;

2) traffic analysis;

3) analysis of PDU headers for purposes that are not legitimate;

4) copying of PDU data to systems other than the intended destinations.

5) cryptanalysis.

Examples of active attacks are:

1) Trojan horses (code whose undocumented features facilitate security breaches);

2) covert channels;

3) penetration of the mechanisms that support confidentiality; such as penetration of the authentication mechanism (e.g. successfully masquerading as an authorized entity), penetration of the Access Control Mechanism, and key interception;

4) spurious invocations of the cryptographic mechanisms, such as chosen plaintext attacks.

6 Confidentiality policies

A confidentiality policy is the part of a security policy which deals with the provision and use of the confidentiality service.

Data representing information whose confidentiality is protected is subject to control over which entities may read it. A confidentiality policy must therefore identify the information that is subject to controls and indicate which entities are intended to be allowed to read it.

Depending on the relative importance of the confidentiality of different types of information, a confidentiality policy may also indicate the type and strength of mechanisms that are to be used to provide the confidentiality services for each of the different types of information.

The management of a confidentiality security policy is not addressed in this Recommendation | International Standard.

6.1 Policy expression

In expressing a confidentiality policy means are required for identifying the information involved and the entities involved.

A security policy can be thought of as a set of rules. Each rule in a confidentiality policy can associate a data characterization and an entity characterization. In some policies these rules are not expressed explicitly but can be derived from the policy.

The following subclauses describe a number of ways in which confidentiality policies may be expressed. Note that, although some confidentiality mechanisms will have a parallel in specific kinds of policy expression, the way in which the policy is expressed does not directly imply the use of a specific mechanism to implement the policy.

6.1.1 Information characterization

A policy may identify information in a variety of ways. For example:

1) by identifying the entity that creates it;

2) by identifying the group of entities any of which may read it;

3) by its location; or

4) by identifying the context in which the data is presented (e.g. its intended function).

6.1.2 Entity characterization

There are many ways to characterize the entities involved in a confidentiality policy rule. Two commonly encountered ways are by individually and uniquely identifying the entities or by associating attributes with each entity. These two forms of entity characterization give rise to two kinds of policies: identity based and rule based policies respectively. These policies are discussed fully in the Access Control framework (see ITU-T Rec. X.812 | ISO/IEC 10181-3).

7 Confidentiality information and facilities

7.1 Confidentiality information

In 5.1.2 the operations of **hide** and **reveal** are discussed. Annex B shows by means of Figure B.1 the passage of data from one confidentiality protected environment to another using these operations.

With some confidentiality mechanisms the **hide** and **reveal** operations make use of auxiliary information. This auxiliary information is called **Hiding** Confidentiality Information (HCI) and **Revealing** Confidentiality Information (RCI) respectively.

7.1.1 Hiding confidentiality information

Hiding Confidentiality Information (HCI) is information used by the **hide** operation.

Examples include:

1) public keys;

2) symmetric keys;

3) the location where the data is to be stored; and

4) segmenting rules.

7.1.2 Revealing confidentiality information

Revealing Confidentiality Information (RCI) is information used by the **reveal** operation.

Examples include:

1) private keys;
2) symmetric keys;
3) the location where the data was stored; and
4) segmenting rules.

7.2 Confidentiality facilities

A number of confidentiality facilities have been identified and are enumerated in Annex E. The confidentiality facilities can be distinguished into those that relate to operational aspects and those that relate to management aspects.

7.2.1 Operation related facilities

7.2.1.1 Hide

This facility applies confidentiality protection to data. Candidate inputs to this facility include:

1) data (possibly confidentiality protected);
2) HCI;
3) mechanism specific identifiers such as those mentioned in Annex E.

Candidate outputs include:

1) confidentiality protected data;
2) other results of the **hide** operation performed;
3) the distinguishing identifier of the confidentiality protected environment in which the confidentiality protected data have been placed.

7.2.1.2 Reveal

This facility removes the protection a previous **hide** operation afforded to the data. Candidate inputs to this facility include:

1) confidentiality protected data;
2) RCI;
3) mechanism specific identifiers such as those mentioned in Annex E.

Candidate outputs include:

1) data (possibly confidentiality protected);
2) other results of the **reveal** operation performed;
3) the distinguishing identifier of the environment in which the output data have been placed.

7.2.2 Management related facilities

The confidentiality management facilities allow a user to obtain, modify, and remove HCI and RCI information (such as keys) which is necessary to the provision of confidentiality. In broad terms these facilities are:

1) install management information;
2) modify management information;
3) delete management information;
4) list management information.

8 Confidentiality mechanisms

The confidentiality of data may depend on the medium in which the data reside or transit. Therefore:

1) the confidentiality of stored data can be assured by using mechanisms that hide the semantics (such as encipherment) or that fragment the data;

2) the confidentiality of data in transit can be assured by using mechanisms that bar access (such as physically protected channels or routing control), via mechanisms that hide the semantics of the data (such as encipherment), or via mechanisms that scatter the data (such as frequency hopping).

These types of mechanism can be used alone or in combination.

The classification above shows that the confidentiality mechanisms can be grouped as follows:

1) mechanisms that prevent unauthorized access to the data;

2) encipherment mechanisms that hide the data but leave it accessible; and

3) contextual mechanisms that make the data only partially accessible, such that the data cannot be completely recreated from the limited amount of collected data.

8.1 Confidentiality provision through access prevention

Confidentiality through access prevention can be achieved through Access Control as described in ITU-T Rec. 812 | ISO/IEC 10181-3, through physical media protection, and through routing control as described below.

8.1.1 Confidentiality protection through physical media protection

Physical measures may be taken to ensure that data in a medium can be inspected only through the use of a specific, limited set of mechanisms. Data confidentiality is achieved by ensuring that only authorized entities can avail themselves of such mechanisms.

8.1.2 Confidentiality protection through routing control

The purpose of this mechanism is to prevent unauthorized disclosure of the information represented by transferred data items. The mechanism supports confidentiality by using only trusted and secure facilities to route the data.

8.2 Confidentiality provision through encipherment

The purpose of these mechanisms is to prevent disclosure of the semantics of data, either in transit or in storage. These mechanisms can be regarded as operating between two sets of entities:

– any entity in the first set may initially hold the data (with access to the semantics); and

– any entity in the second set is an authorized recipient of the information the data represent.

There are different classes of confidentiality mechanism to be considered:

1) confidentiality mechanisms based on symmetric encipherment in which the same key is used to encipher (**hide** operation) and to decipher (**reveal** operation) the data; and,

2) confidentiality mechanisms based on asymmetric encipherment in which a public key is used to encipher (**hide** operation) the data and the corresponding private key is used to decipher them (**reveal** operation).

The chief distinction between these two basic classes of mechanism is that, in 1), those capable of performing the **hide** operation are those capable of performing the **reveal** operation and vice versa, whereas in 2) all, or nearly all, can perform the **hide** operation while only those with access to the private key can perform the **reveal** operation.

8.2.1 Confidentiality provision through data padding

The purpose of this mechanism is to prevent knowledge of the information represented by the size of a data item. This mechanism increases the size of data items so that the size of a padded data item bears little relation to its original size. One way to do this is to add random data to the beginning or the end of the data item. This must be done in a way that the padding is recognizable as such by authorized entities but is indistinguishable from the data by unauthorized entities. In order to achieve this, data padding can be used in conjunction with cryptographic transformations.

This mechanism can be used in conjunction with data segmenting at the network layer as described in ITU-T Rec. X.273 | ISO/IEC 11577.

Data padding can be used to prevent the size of data items being used as a covert channel.

8.2.2 Confidentiality provision through dummy events

The purpose of this mechanism is to prevent inferencing based on the rate that a given event occurs. An instance of this mechanism can be found in network layer security protocols that seek to hide the volume of traffic exchanged over untrusted links.

This mechanism produces pseudo-events (e.g. bogus PDUs) that only authorized parties can identify as such. This mechanism can be used to counter covert channel attacks that perform signaling based on variations in the rate of an activity.

NOTE – Data and traffic padding are examples of this mechanism. In both instances the mechanism conceals the attributes of an object by embedding it in a bigger one and cryptographically protecting the whole.

8.2.3 Confidentiality provision through PDU header protection

The purpose of this mechanism is to prevent inferencing based on PDU headers during communication.

One instance of this mechanism is address hiding as described in ITU-T Rec. X.273 | ISO/IEC 11577. An intermediate system X may receive a PDU, encipher it, and embed it in a new PDU whose origin appears to be X and whose destination appears to be Y, a peer system where the data are decrypted and the original PDU recovered. Since the original header (including the addresses) is encrypted, no inferencing based on header information is possible other than that implied by the fact that X and Y are exchanging encrypted PDUs.

Another instance is when for each *bona fide* PDU sent by a system A, n additional copies with varying destination addresses and header options are created (i.e. the system creates dummy broadcast traffic; this mechanism is also an instance of the mechanisms described in 8.2.2 above).

Address hiding at the network layer is described in ITU-T Rec. X.273 | ISO/IEC 11577. Address hiding can be carried out in other layers (e.g. ITU-T Rec. X.411 | ISO/IEC 10021-4, known as MHS, describes the use of address hiding at the application layer).

This mechanism embodies ideas similar to those in 8.3 below.

8.2.4 Confidentiality provision through time varying fields

This mechanism, used in conjunction with encipherment, protects against inferencing based on dynamic variations of data items. To this end, it combines the data to be protected with time varying fields in such a way that attackers cannot determine if changes in the representation are caused by changes in the data or by changes in the time varying fields. Ideally, this mechanism generates a different data representation for each meaningful potential observation of the protected data so that inferences based on the absence of dynamic variation are disallowed as well. Examples include:

1) *PDU transmission*

   A time varying field is placed in front of the protected part of each PDU; the resultant combined data are then enciphered using a cryptographic mechanisms with chaining (i.e. the varying field affects the encryption of the subsequent data).

2) *Storage*

   Where time varying fields are placed at the beginning of the stored files so as to conceal changes (or the lack thereof).

This mechanism can be used in conjunction with padding and segmenting so as to conceal variations of the size of the protected data.

8.3 Confidentiality provision through contextual location

A form of confidentiality-protection by preventing access to data can be provided when data may be found in any of a large number of different contexts. If it is infeasible (for reasons computational or physical) to examine all possible contexts in the time before the context used is changed, a level of confidentiality can be obtained.

Examples of such mechanisms include:

1) the provision of a large number of physical or virtual channels through which information is transmitted (e.g. the “spread spectrum” use of one out of a large number of radio frequencies);

2) the provision of a large number of locations for data storage (e.g. addresses on a magnetic disc);

3) the transmission of information through hidden secondary communications channels which are concealed within a primary communication channel (steganography).

This form of confidentiality assumes that unauthorized recipients cannot obtain the information needed to identify the currently correct context. This information must therefore itself be protected by a confidentiality service.

9 Interactions with other security services and mechanisms

This clause describes how other security services and mechanisms can be used to support confidentiality. The use of confidentiality to support other security services is not described here.

9.1 Access Control

Access Control, as described in ITU-T Rec. X.812 | ISO/IEC 10181-3 can be used to regulate access to the data.

Annex A

Confidentiality in the OSI Reference Model

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

The relationship of security services to the OSI Reference Model is defined in CCITT Rec. X.800 | ISO 7498-2. This annex summarizes what is relevant to confidentiality.

Different security services are considered:

- connection confidentiality;
- connectionless confidentiality;
- selective field confidentiality;
- traffic flow confidentiality.

A.1 Connection confidentiality

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

A.2 Connectionless confidentiality

Connectionless confidentiality provides for the confidentiality of selected fields within the (N)-user-data in a single connectionless (N)-SDU.

A.3 Selective field confidentiality

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

A.4 Traffic flow confidentiality

Traffic flow confidentiality provides for the protection of the information which might be derived from observation of traffic flows.

A.5 Use of confidentiality within OSI layers

The confidentiality services are relevant to the following OSI layers:

- Physical Layer (layer 1);
- Data Link Layer (layer 2);
- Network Layer (layer 3);
- Transport Layer (layer 4);
- Presentation Layer (layer 6);
- Application Layer (layer 7).

A.5.1 Use of confidentiality at the physical layer

Connection confidentiality and traffic flow confidentiality either singly or in combination are the only confidentiality services provided at the physical layer. The traffic flow confidentiality takes two forms: full traffic flow confidentiality which can only be provided on some types of transmission and limited traffic flow confidentiality which can always be provided.

A.5.2 Use of confidentiality at the data-link layer

Connection confidentiality and connectionless confidentiality are the only security services provided at the data-link layer. These services make use of encipherment mechanisms.

A.5.3 Use of confidentiality at the network layer

Connection confidentiality, connectionless confidentiality and traffic flow confidentiality are the only confidentiality services provided at the network layer. Connection confidentiality and connectionless confidentiality may be provided by an encipherment mechanism and/or routing control. Traffic flow confidentiality may be provided by a traffic padding mechanism, in conjunction with a confidentiality service at or below the network layer and/or routing control. These services allow confidentiality between network nodes, subnetwork nodes or relays.

A.5.4 Use of confidentiality at the transport layer

Connection confidentiality and connectionless confidentiality are the only confidentiality services provided at the transport layer. Connection confidentiality and connectionless confidentiality may be provided by an encipherment mechanism. These services allow confidentiality between end systems.

A.5.5 Use of confidentiality at the presentation layer

Connection confidentiality, connectionless confidentiality, and selective field confidentiality may be provided at the presentation layer. In the case of selective field confidentiality, the indication of which fields are to be confidentiality protected is provided by the application layer.

A.5.6 Use of confidentiality at the application layer

All the confidentiality services, namely, connection confidentiality, connectionless confidentiality, selective field confidentiality and traffic flow confidentiality may be provided at the application layer. Connection confidentiality and connectionless confidentiality can be supported using a lower layer encipherment mechanism. Selective field confidentiality can be supported using an encipherment mechanism at the presentation layer. A limited traffic 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.

Annex B

Example of a sequence of movements through different confidentiality protected environments

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

Figure B.1 is an example of a sequence of **hide/reveal** operations that preserve the confidentiality as data are moved from an initial environment A to an environment E. The example assumes that environments A and E support confidentiality through Access Control while environment C protects confidentiality through encipherment. Overlapped environments B (A and C) and D (C and E) protect the data through encipherment as well as Access Control.

The diagram illustrates the following operations:

1) a **hide** operation, t, which enciphers the data and thereby places them into overlapped environment B;

2) a **reveal** operation, u, which moves the data from B to C. This **reveal** operation removes the data from the access control protected environment but does not affect the confidentiality protection that was applied with the **hide** operation "t";

3) a **hide** operation, v, which again applies access control protection by moving the data into overlapped environment D where the data are protected through encipherment and E's Access Control;

4) a **reveal** operation, w, which deciphers the data and thereby moves them out of D and into E;

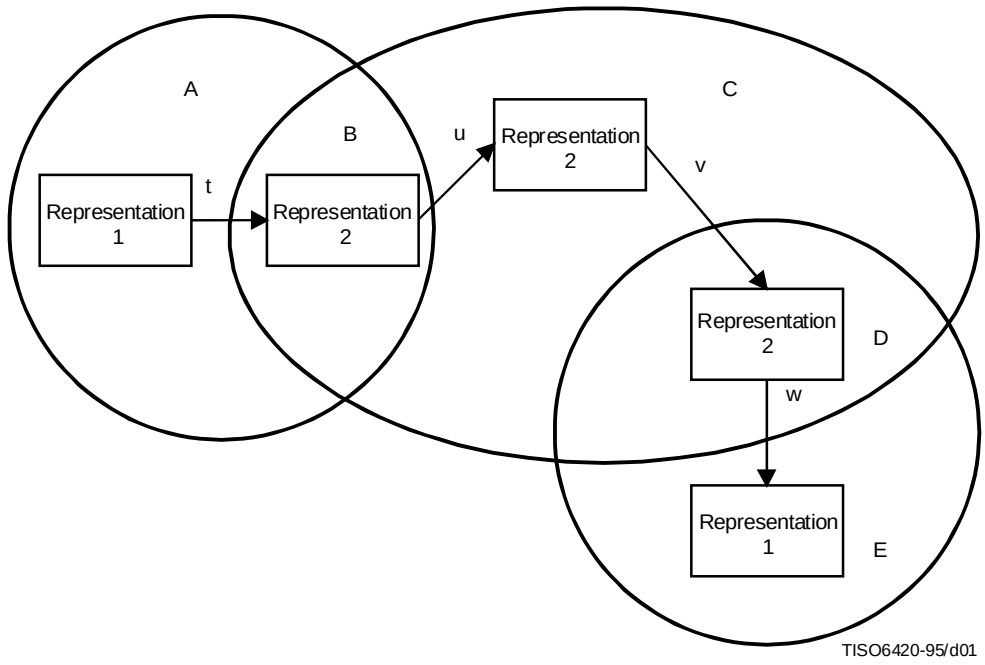

Figure B.1 – Illustration of protected regions

Annex C

Representation of Information

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

Communication or storage of an information item is realized using a *representation* of the information item [e.g. the number seventeen can be encoded as 17 decimal, 11 hexadecimal, the ninth odd integer, the seventh prime number, or 289 (17*17)]. Information can be either be obtained either from its representation or from the attributes of the representation. Thus, we can obtain information by:

1) inspecting a data value when the representation conventions and related information are known;

2) ascertaining whether or not a data item exists;

3) the size of a data item;

4) dynamic variations of representations.

For example, the information that “the King is dead” could be inferred as follows:

– by inspecting a Boolean whose value is true when the king is dead, false otherwise;

– by ascertaining the existence or non-existence of a file called “King’s death report” in a file directory;

– by inspecting a list of dead monarchs and finding out that its length has increased;

– by establishing that a counter, indicating the number of days the country has ever been in a monarch-less state, can be observed to be changing daily.

The mapping between an information item and some representation of it is defined by a set of *representation rules*. Representation rules describe:

– how the information is encoded into data;

– how the data can be made to yield the information encoded therein; and

– what explicit and implicit contextual changes must be made whenever information is encoded (e.g. the creation of a file may result in directory changes).

The confidentiality mechanisms addressed by this Framework protect an information item by either:

1) protecting a representation of the information item from disclosure, by ensuring it within an appropriate *environment*; or

2) protecting knowledge of the representation rules from disclosure.

Different environments can be considered to have differing strengths, depending upon the extent of protection against disclosure provided to representations in those environments. Also different sets of representation rules can be considered to have differing strengths, depending upon the difficulty of the representation rules becoming known to unauthorized entities.

As a basis of describing the characteristics of different types of confidentiality mechanisms, the concept of *confidentiality protection context* is used. A confidentiality protection context (for any information item) is a particular representation of that information item existing in a particular environment.

The behaviour of confidentiality mechanisms can be understood by recognizing that transfer of information potentially involves moving through a sequence of distinct confidentiality protection contexts.

A change of representation or a change of environment constitutes a movement from one confidentiality protection context to another. A change of representation will usually be either to a stronger (more protective) representation or to a weaker (less protective) representation. Similarly, a change of environment will usually be either to a stronger (more protective) environment or to a weaker (less protective) environment.

Annex B provides an example of movements through different confidentiality protection contexts.

Annex D

Covert Channels

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

The term covert channels refers to mechanisms which are not intended to be used for communication and which can be used to transfer information in ways that violate the security policy.

Covert channel attacks are attacks performed inside a system by the sender of some data. This attempt is not constrained to use particular means of information transfer, such as those usually provided specifically for the purpose. In a sufficiently complex environment there is usually one or more means to transfer information outside the mechanisms provided to communicate data and to store and retrieve it. Such means are called covert channels.

Many covert channels involve the authorized modulation of states or events that is visible to entities unauthorized to receive information from the source of that modulation. Information is transferred through a common understanding between the source and recipient of the meaning to be ascribed to such modulation.

Example channels in data communication mechanisms include ascribing meaning to:

- the different available sizes of (N)-PDU;
- the different destination addresses able to be received or intercepted by the covert channel recipient on (N)-connections or (N)-connectionless-mode transmissions; and
- the different available durations between the transmission of (N)-PDUs on the same (N)-connection or from the same (N)-entity.

The latter is an example of a timing covert channel.

Example channels in data storage and retrieval mechanisms include ascribing meaning to:

- the name given to a storage area;
- the presence or absence of specifically named stored data;
- the amount of stored data;
- the ability to accept further data for storage; and
- the duration for which specifically named data is (or is not) stored.

Examples such as the first of these, in which data (a name) can be stored and then retrieved are referred to as “storage covert channels”.

System resources and communications protocols can be specified and modelled as abstract objects defined to provide a number of specific primitive operations. Hence, more generally, examples include ascribing meaning to:

- the choice of one out of the available operations;
- the order in which service primitives are used; and
- the duration between uses of an operation, when these are potentially visible to the covert channel recipient.

The confidentiality of information can only be guaranteed when all means of transferring information are identified (including covert channels) and each controlled through the use of suitable confidentiality mechanisms.

In many instances complete covert channel prevention is infeasible (for reasons technical, organizational, economic, or other). Nevertheless, it may be feasible to reduce the rate at which information can be conveyed through such channels to levels that are deemed acceptable.

Annex E

Confidentiality Facilities Outline

<table>
<tr><td colspan="3" rowspan="3">Security Facilities Outline</td><td rowspan="3">Element</td><td colspan="3">Entity: Initiator, Verifier, Confidentiality-TTP</td></tr>
<tr><td colspan="3">Function:</td></tr>
<tr><td colspan="3">Info. object: Confidentiality-protected data</td></tr>
<tr><td colspan="3">Goal of Service</td><td colspan="3">Information is not made available or disclosed to unauthorized individuals, entities, or processes</td></tr>
<tr><td rowspan="6">ACTIVITY</td><td colspan="2">Entity</td><td colspan="4">Security Domain Authority (SDA)</td></tr>
<tr><td colspan="2">Function</td><td colspan="4"></td></tr>
<tr><td colspan="2">Management related activity</td><td colspan="4">– Install management information
– Modify management information
– Delete management information
– List management information
– Disable management information
– Re-enable management information</td></tr>
<tr><td colspan="2">Entity</td><td>Initiator</td><td>Verifier</td><td>Confidentiality-TTP</td></tr>
<tr><td colspan="2">Function</td><td></td><td></td><td></td></tr>
<tr><td colspan="2">Operational related activity</td><td>– Hide data
– Security Label</td><td>– Reveal data
– Security Label</td><td>– Entity certificate</td></tr>
<tr><td rowspan="3">INFORMATION</td><td colspan="2">Input/Output Data element managed by SDA</td><td colspan="4">– Public keys
– Symmetric keys
– Security Label</td></tr>
<tr><td colspan="2">Information type used in operation</td><td colspan="4">– Hiding Confidentiality Information (HCI)
– Revealing Confidentiality Information (RCI)</td></tr>
<tr><td colspan="2">Control Information</td><td colspan="4">– confidentiality-protected mechanism type
– confidentiality-protected level</td></tr>
</table>

This annex makes use of the following concepts.

E.1 Confidentiality entities

Confidentiality in Open Systems involves the following entities:

E.1.1 Initiator

The entity that generates confidentiality-protected data either for transmission or for storage.

E.1.2 Verifier

The entity that retrieves information from confidentiality protected data.

E.1.3 Trusted Third Party (TTP) for confidentiality facilities

The entity which distributes either hiding-confidentiality-information or revealing-confidentiality-information to the entities exchanging confidentiality-protected-data.