

# Information technology — Open Systems Interconnection — Security frameworks for open systems: Confidentiality framework —

(ITU-T Rec. X.814 (1995) |  
ISO/IEC 10181-5:1996)

ICS 35.100.01

NO COPYING WITHOUT BSI PERMISSION EXCEPT AS PERMITTED BY COPYRIGHT LAW



Document Sharing Hub

# National foreword

This British Standard reproduces verbatim ISO/IEC 10181-5:1996 and implements it as the UK national standard.

The UK participation in its preparation was entrusted to Technical Committee IST/21, Open Systems Interconnection, Data Management and Open Distribution Processing, which has the responsibility to:

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

A list of organizations represented on this committee can be obtained on request.

### Cross-references

The British Standards which implement international or European publications referred to in this document may be found in the BSI Standards Catalogue under the section entitled “International Standards Correspondence Index”, or using the “Find” facility of the BSI Standards Electronic Catalogue.

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

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

### Summary of pages

This document comprises a front cover, an inside front cover, the ISO/IEC title page, pages ii to iv, pages 1 to 14 and a back cover.

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

This British Standard, having been prepared under the direction of the DISC Board, was published under the authority of the Standards Board and comes into effect on 15 February 1997

© BSI 11-1998

ISBN 0 580 26507 2

### Amendments issued since publication

| Amd. No. | Date | Comments |
|----------|------|----------|
|          |      |          |
|          |      |          |
|          |      |          |
|          |      |          |

INTERNATIONAL  
STANDARD

**ISO/IEC  
10181-5**

First edition  
1996-09-15

---

---

**Information technology — Open Systems  
Interconnection — Security frameworks for  
open systems: Confidentiality framework**

*Technologies de l'information — Interconnexion de systèmes  
ouverts (OSI) — Cadres généraux pour la sécurité des systèmes ouverts:  
Cadre général de confidentialité*



Reference number  
ISO/IEC 10181-5:1996(E)

**Contents**

|                                                                                      | Page |
|--------------------------------------------------------------------------------------|------|
| Foreword                                                                             | iv   |
| Introduction                                                                         | 1    |
| 1 Scope                                                                              | 1    |
| 2 Normative references                                                               | 2    |
| 2.1 Identical Recommendations   International Standards                              | 2    |
| 2.2 Paired Recommendations   International Standards equivalent in technical content | 2    |
| 3 Definitions                                                                        | 2    |
| 3.1 Basic Reference Model definitions                                                | 2    |
| 3.2 Security architecture definitions                                                | 2    |
| 3.3 Security frameworks overview definitions                                         | 2    |
| 3.4 Additional definitions                                                           | 3    |
| 4 Abbreviations                                                                      | 3    |
| 5 General discussion of confidentiality                                              | 3    |
| 5.1 Basic concepts                                                                   | 3    |
| 5.1.1 Protection of information                                                      | 4    |
| 5.1.2 Hide and reveal operations                                                     | 4    |
| 5.2 Classes of confidentiality services                                              | 4    |
| 5.3 Types of confidentiality mechanisms                                              | 5    |
| 5.4 Threats to confidentiality                                                       | 5    |
| 5.4.1 Threats when confidentiality is provided through access prevention             | 5    |
| 5.4.2 Threats when confidentiality is provided through information hiding            | 6    |
| 5.5 Types of confidentiality attacks                                                 | 6    |
| 6 Confidentiality policies                                                           | 6    |
| 6.1 Policy expression                                                                | 6    |
| 6.1.1 Information characterization                                                   | 6    |
| 6.1.2 Entity characterization                                                        | 7    |
| 7 Confidentiality information and facilities                                         | 7    |
| 7.1 Confidentiality information                                                      | 7    |
| 7.1.1 Hiding confidentiality information                                             | 7    |
| 7.1.2 Revealing confidentiality information                                          | 7    |
| 7.2 Confidentiality facilities                                                       | 7    |
| 7.2.1 Operation related facilities                                                   | 7    |
| 7.2.1.1 Hide                                                                         | 7    |
| 7.2.1.2 Reveal                                                                       | 7    |
| 7.2.2 Management related facilities                                                  | 7    |
| 8 Confidentiality mechanisms                                                         | 7    |
| 8.1 Confidentiality provision through access prevention                              | 8    |
| 8.1.1 Confidentiality protection through physical media protection                   | 8    |
| 8.1.2 Confidentiality protection through routing control                             | 8    |
| 8.2 Confidentiality provision through encipherment                                   | 8    |
| 8.2.1 Confidentiality provision through data padding                                 | 8    |
| 8.2.2 Confidentiality provision through dummy events                                 | 8    |
| 8.2.3 Confidentiality provision through PDU header protection                        | 9    |
| 8.2.4 Confidentiality provision through time varying fields                          | 9    |
| 8.3 Confidentiality provision through contextual location                            | 9    |
| 9 Interactions with other security services and mechanisms                           | 9    |
| 9.1 Access Control                                                                   | 9    |

|                                                                                                     | Page |
|-----------------------------------------------------------------------------------------------------|------|
| Annex A Confidentiality in the OSI Reference Model                                                  | 10   |
| Annex B Example of a sequence of movements through different confidentiality protected environments | 11   |
| Annex C Representation of Information                                                               | 12   |
| Annex D Covert Channels                                                                             | 12   |
| Annex E Confidentiality Facilities Outline                                                          | 14   |
| Figure B.1 — Illustration of protected regions                                                      | 11   |

**Descriptors:** Data processing, information interchange, network interconnection, open systems interconnection, communication procedure, protection of information, security techniques.

## Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 10181-5 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 21, *Open Systems Interconnection, data management and open distributed processing*, in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.814.

ISO/IEC 10181 consists of the following parts, under the general title *Information technology — Open Systems Interconnection — Security frameworks for open systems*:

- *Part 1: Overview;*
- *Part 2: Authentication framework;*
- *Part 3: Access control framework;*
- *Part 4: Non-repudiation framework;*
- *Part 5: Confidentiality framework;*
- *Part 6: Integrity framework;*
- *Part 7: Security audit framework.*

Annexes A to E of this part of ISO/IEC 10181 are for information only.

## 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.

## 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 cryptographic 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.