



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.814

(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 1996

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.



Documents

Document Sharing Hub

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

		<i>Page</i>
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	3
3.3	Security frameworks overview definitions	3
3.4	Additional definitions	3
4	Abbreviations	4
5	General discussion of confidentiality	4
5.1	Basic concepts	4
5.1.1	Protection of information	4
5.1.2	Hide and reveal operations	5
5.2	Classes of confidentiality services	5
5.3	Types of confidentiality mechanisms	6
5.4	Threats to confidentiality	6
5.4.1	Threats when confidentiality is provided through access prevention	6
5.4.2	Threats when confidentiality is provided through information hiding	7
5.5	Types of confidentiality attacks	7
6	Confidentiality policies	7
6.1	Policy expression	8
6.1.1	Information characterization	8
6.1.2	Entity characterization	8
7	Confidentiality information and facilities	8
7.1	Confidentiality information	8
7.1.1	Hiding confidentiality information	8
7.1.2	Revealing confidentiality information	9
7.2	Confidentiality facilities	9
7.2.1	Operation related facilities	9
7.2.1.1	Hide	9
7.2.1.2	Reveal	9
7.2.2	Management related facilities	9
8	Confidentiality mechanisms	10
8.1	Confidentiality provision through access prevention	10
8.1.1	Confidentiality protection through physical media protection	10
8.1.2	Confidentiality protection through routing control	10
8.2	Confidentiality provision through encipherment	10
8.2.1	Confidentiality provision through data padding	10
8.2.2	Confidentiality provision through dummy events	11
8.2.3	Confidentiality provision through PDU header protection	11
8.2.4	Confidentiality provision through time varying fields	11
8.3	Confidentiality provision through contextual location	11
9	Interactions with other security services and mechanisms	12
9.1	Access Control	12

	<i>Page</i>
Annex A – Confidentiality in the OSI Reference Model	13
Annex B – Example of a sequence of movements through different confidentiality protected environments	15
Annex C – Representation of Information	16
Annex D – Covert Channels.....	17
Annex E – Confidentiality Facilities Outline	18

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.

Page blanche

page iv

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.