



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.815

(11/95)

**DATA NETWORKS AND OPEN SYSTEM
COMMUNICATIONS SECURITY**

**INFORMATION TECHNOLOGY –
OPEN SYSTEMS INTERCONNECTION –
SECURITY FRAMEWORKS FOR OPEN
SYSTEMS: INTEGRITY FRAMEWORKS**

ITU-T Recommendation X.815

(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.815 was approved on 21st of November 1995. The identical text is also published as ISO/IEC International Standard 10181-6.

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
2.3 Additional References	2
3 Definitions	2
4 Abbreviations	4
5 General discussion of integrity	4
5.1 Basic concepts	5
5.2 Types of integrity services	5
5.3 Types of integrity mechanisms	5
5.4 Threats to integrity	6
5.5 Types of integrity attacks	6
6 Integrity policies	7
6.1 Policy expression	7
6.1.1 Data characterization	7
6.1.2 Entity characterization	7
6.1.2.1 Identity based policies	7
6.1.2.2 Rule based policies	7
7 Integrity information and facilities	7
7.1 Integrity information	7
7.1.1 Shield integrity information	8
7.1.2 Modification detection integrity information	8
7.1.3 Unshield integrity information	8
7.2 Integrity facilities	8
7.2.1 Operational related facilities	8
7.2.2 Management related facilities	9
8 Classification of integrity mechanisms	9
8.1 Integrity provision through cryptography	9
8.1.1 Integrity provision through sealing	9
8.1.2 Integrity provision through Digital Signatures	9
8.1.3 Integrity provision through encipherment of redundant data	10
8.2 Integrity provision through context	10
8.2.1 Data Replication	10
8.2.2 Pre-agreed context	11
8.3 Integrity provision through detection and acknowledgement	11
8.4 Integrity provision through prevention	11
9 Interactions with other security services and mechanisms	11
9.1 Access Control	11
9.2 Data origin authentication	12
9.3 Confidentiality	12
Annex A – Integrity in the OSI Basic Reference Model	13
Annex B – External Data Consistency	15
Annex C – Integrity Facilities Outline	17

Summary

This Recommendation | International Standard defines a general framework for the provision of integrity services. The property that data has not been altered or destroyed in an unauthorized manner is called integrity.

Introduction

Many open systems applications have security requirements which depend upon the integrity of data. Such requirements may include the protection of data used in the provision of other security services such as authentication, access control, confidentiality, audit and non-repudiation, that, if an attacker could modify them, could reduce or nullify the effectiveness of those services.

The property that data has not been altered or destroyed in an unauthorized manner is called integrity. This Recommendation | International Standard defines a general framework for the provision of integrity services.

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

**INFORMATION TECHNOLOGY – OPEN SYSTEMS
INTERCONNECTION – SECURITY FRAMEWORKS
FOR OPEN SYSTEMS: INTEGRITY FRAMEWORK****1 Scope**

The 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 integrity of data in information retrieval, transfer, and management:

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

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

- 1) standards that incorporate the concept of integrity;
- 2) standards that specify abstract services that include integrity;
- 3) standards that specify uses of an integrity service;
- 4) standards that specify means of providing integrity within an open system architecture; and
- 5) standards that specify integrity 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 identified in clause 7;
- standards of type 5) can be based upon the classes of mechanisms identified in clause 8.

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

The integrity addressed by this Recommendation | International Standard is that defined by the constancy of a data value. This notion (constancy of a data value) encompasses all instances in which different representations of a data value are deemed equivalent (such as different ASN.1 encodings of the same value). Other forms of invariance are excluded.

The usage of the term data in this Recommendation | International Standard includes all types of data structures (such as sets or collections of data, sequences of data, file-systems and databases).

ISO/IEC 10181-6 : 1996 (E)

This framework addresses the provision of integrity to data that are deemed to be write-accessible to potential attackers. Therefore, it focusses on the provision of integrity through mechanisms, both cryptographic and non-cryptographic that do not rely exclusively on regulating access.

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 – Basic Reference Model: The Basic Model*.
- 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.811 (1995) | ISO/IEC 10181-2:1996, *Information technology – Open Systems Interconnection – Security frameworks for open systems: Authentication framework*.
- 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

- ITU-T Recommendation X.224 (1993), *Protocol for providing the OSI connection-mode transport service*.
ISO/IEC 8073:1992, *Information technology – Telecommunications and information exchange between systems – Open Systems Interconnection – Protocol for providing the connection-mode transport service*.
- 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*.

2.3 Additional References

- ISO/IEC 9979:1991, *Data cryptographic techniques – Procedures for the registration of cryptographic algorithms*.

3 Definitions

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

3.1 This Recommendation | International Standard builds on concepts developed in ITU-T Recommendation X.200 | ISO/IEC 7498-1 and makes use of the following terms defined in it:

- a) (N)-connection;
- b) (N)-entity;
- c) (N)-facility;