



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.802

(04/95)

**DATA NETWORKS AND OPEN SYSTEM
COMMUNICATIONS**

SECURITY

**INFORMATION TECHNOLOGY –
LOWER LAYERS SECURITY MODEL**

ITU-T Recommendation X.802

(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.802 was approved on 10th of April 1995. The identical text is also published as ISO/IEC International Standard 13594.

NOTE

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

© ITU 1995

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.

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

	Page
1 Scope.....	1
2 References	1
2.1 Identical Recommendations International Standards	1
2.2 Paired Recommendations International Standards equivalent in technical content	2
2.3 Additional references	2
3 Definitions	2
3.1 OSI Reference Model definitions	2
3.2 Open System Security Frameworks definitions	3
3.3 Internal Organization of the Network Layer definitions.....	3
3.4 Additional definitions	3
4 Abbreviations	3
5 Security associations	3
5.1 General overview	3
5.2 Establishing a security association for the lower layers.....	5
5.3 Security association close	6
5.4 Modification of attributes in a connection	6
6 Influence on existing protocols	6
6.1 General principle.....	6
6.2 Connectionless SDU size	6
6.3 Concatenation of PDUs.....	6
6.4 Algorithm and mechanism independence	6
7 Common security PDU structure	7
8 Determination of security services and mechanisms.....	7
9 Protection QOS	7
10 Security rules.....	7
11 Placement of security in the lower layers.....	7
12 Use of (N-1)-layer(s) to enhance (N)-layer security	13
13 Security labelling	13
14 Security domains	13
15 Security of routeing.....	13
16 Security Management.....	14
16.1 Security policy	14
16.2 Security association management	14
16.3 Key management	14
16.4 Security Audit.....	14
17 Traffic flow confidentiality	14
18 Guidelines for the definition of SA-Attributes.....	15
19 Error handling	15
Annex A – Illustrative example of an Agreed Set of Security Rules	16

Summary

This Recommendation | International Standard describes the cross layer aspects of the revision of security services in the lower layers of the OSI Reference Model (Transport, Network, Data Link, Physical). It describes the architectural concepts common to these layers, the basis for interactions relating to security between layers and the placement of security protocols in the lower layers.

Copyright © 1995 ITU-T. All rights reserved.

TECHNICAL REPORT

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – LOWER LAYERS SECURITY MODEL

1 Scope

This Recommendation | Technical Report describes the cross layer aspects of the provision of security services in the lower layers of the OSI Reference Model (Transport, Network, Data Link and Physical layers).

This Recommendation | Technical Report describes:

- a) architectural concepts common to the lower layers based on those defined in CCITT Rec. X.800 | ISO 7498-2;
- b) the basis for interactions relating to security between protocols in the lower layers;
- c) the basis for any interactions relating to security between the lower layers and upper layers of OSI;
- d) the placement of security protocols in relation to other lower layer security protocols and the relative role of such placements.

There should be no conflict between the security protocols for the lower layers and the model described in this Recommendation | Technical Report.

CCITT Rec. X.500 | ISO/IEC 9594-1 identifies the security services relevant to each of the lower layers of the OSI Reference Model.

2 References

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | Technical Report. At time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | Technical Report 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 OSI connectionless-mode Network service: Protocol specification*.
- ITU-T Recommendation X.234 (1994) | ISO/IEC 8602:1995, *Information technology – Protocol for providing the OSI connectionless-mode Transport service*.
- 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 – Open Systems Interconnection – Transport layer security protocol*.
- ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.

- ITU-T Recommendation X.810¹⁾ | ISO/IEC 10181-1...¹⁾, *Information technology – Open Systems Interconnection – Security frameworks in open systems: Security frameworks overview.*
- ITU-T Recommendation X.812¹⁾ | ISO/IEC 10181-3...¹⁾, *Information technology – Open Systems Interconnection – Security frameworks in 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.*
- 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.208 (1988), *Specification of Abstract Syntax Notation One (ASN.1).*
ISO/IEC 8824:1990, *Information technology – Open Systems Interconnection – Specification of Abstract Syntax Notation One (ASN.1).*
- CCITT Recommendation X.209 (1988), *Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*
ISO/IEC 8825:1990, *Information technology – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

2.3 Additional references

- ISO/IEC 8208:1995, *Information technology – Data communications – X.25 Packet Layer Protocol For Data Terminal Equipment.*
- ITU-T Recommendation X.25 (1993), *Interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for terminals operating in packet mode and connected to public data networks by dedicated circuits.*
- ISO 8648:1988, *Information processing systems – Open Systems Interconnection – Internal organization of the Network Layer.*
- ISO 9542:1988²⁾, *Information processing systems – Telecommunications and information exchange between systems – End system to intermediate system routing exchange protocol for use in conjunction with the Protocol routing for providing the connectionless-mode network service (ISO 8473).*
- ISO/IEC 10589:1992, *Information technology – Telecommunications and information exchange between systems – Intermediate system to intermediate system intra-domain-routing routine information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network service (ISO 8473).*
- ISO/IEC 10747:1994, *Information technology – Telecommunications and information exchange between systems – Protocol for exchange of inter-domain routing information among intermediate systems to support forwarding of ISO 8473 PDUs.*

3 Definitions

3.1 OSI Reference Model definitions

This Recommendation | Technical Report makes use of the following terms as defined in ITU-T Rec. X.200 | ISO/IEC 7498-1:

- Quality of Service

¹⁾ Presently at the stage of draft.

²⁾ Currently under revision.