



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.800

Amendment 1
(10/96)

SERIES X: DATA NETWORKS AND OPEN SYSTEM
COMMUNICATION

Security

**Security architecture for Open Systems
Interconnection for CCITT applications**

**Amendment 1: Layer Two Security Service and
Mechanisms for LANs**

ITU-T Recommendation X.800 – Amendment 1

(Previously CCITT Recommendation)

ITU-T X-SERIES RECOMMENDATIONS
DATA NETWORKS AND OPEN SYSTEM COMMUNICATION

PUBLIC DATA NETWORKS	X.1–X.199
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 SYSTEM INTERCONNECTION	X.200–X.299
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	X.300–X.399
General	X.300–X.349
Satellite data transmission systems	X.350–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
Networking	X.600–X.629
Efficiency	X.630–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
Systems Management framework and architecture	X.700–X.709
Management Communication Service and Protocol	X.710–X.719
Structure of Management Information	X.720–X.729
Management functions	X.730–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
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

For further details, please refer to ITU-T List of Recommendations.

FOREWORD

The ITU-T (Telecommunication Standardization Sector) is a permanent organ of the International Telecommunication Union (ITU). The ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Conference (WTSC), which meets every four years, establishes the topics for study by the ITU-T Study Groups which, in their turn, produce Recommendations on these topics.

The approval of Recommendations by the Members of the ITU-T is covered by the procedure laid down in WTSC Resolution No. 1 (Helsinki, March 1-12, 1993).

Amendment 1 to ITU-T Recommendation X.800 was prepared by ITU-T Study Group 7 (1993-1996) and was approved under the WTSC Resolution No. 1 procedure on the 5th of October 1996.

NOTE

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

© ITU 1997

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.

CONTENTS

	<i>Page</i>
Annex D – Layer Two Security Service and Mechanisms for LANs	1
D.0 <i>Introduction</i>	1
D.1 <i>LAN security services</i>	1
D.2 <i>LAN security mechanisms</i>	1
D.3 <i>Table modifications for LAN security</i>	2

SUMMARY

Recommendation X.800 provides an overview of security services allocated to the seven layers of the OSI Reference Model. Amendment 1, which is to be published as Annex D, extends the security services of the Data Link Layer to accommodate LAN security.

SECURITY ARCHITECTURE FOR OPEN SYSTEMS INTERCONNECTION FOR CCITT APPLICATIONS

Annex D

Layer Two Security Service and Mechanisms for LANs

(Geneva, 1996)

D.0 *Introduction*

This annex covers Layer 2 Security Services and Mechanisms for Local Area Networks (LANs).

The illustration of the placement of security services in Table 2 of clause 7 suggests that only confidentiality services should be available at layer 2. However, it is recognized that in some environments that deploy LANs, additional layer 2 security services and mechanisms may be required. For example, an organization may not deploy full OSI functionality or incorporating layer 2 relays may require security services other than confidentiality.

D.1 *LAN security services*

The security services that may be provided, singly or in combination, in the data link layer for LANs are:

- a) peer entity authentication;
- b) data origin authentication;
- c) access control;
- d) connection confidentiality;
- e) connectionless confidentiality;
- f) connection integrity without recovery; and
- g) connectionless integrity.

D.2 *LAN security mechanisms*

The identified security services can be provided as follows:

- a) the peer entity authentication service can be provided by an appropriate combination of cryptographically-derived or protected authentication exchanges, protected password exchange and signature mechanisms;
- b) the data origin authentication service can be provided by encipherment or signature mechanisms;
- c) the access control service can be provided through the appropriate use of specific access control mechanisms;
- d) the connection confidentiality service can be provided by an encipherment mechanism;
- e) the connectionless confidentiality service can be provided by an encipherment mechanism;
- f) the connection integrity without recovery service can be provided by using a data integrity mechanism, sometimes in conjunction with an encipherment mechanism; and
- g) the connectionless integrity service can be provided by using a data integrity mechanism, sometimes in conjunction with an encipherment mechanism.

D.3 *Table modifications for LAN security*

Table 2/X.800 has not been modified but would reflect the legend Y for layer 2 (LANs) for the following security services:

- Peer Entity Authentication;
- Data Origin Authentication;
- Access Control Service;
- Connection Integrity without Recovery; and
- Connectionless Integrity.

ITU-T RECOMMENDATIONS SERIES

- Series A Organization of the work of the ITU-T
- Series B Means of expression
- Series C General telecommunication statistics
- Series D General tariff principles
- Series E Telephone network and ISDN
- Series F Non-telephone telecommunication services
- Series G Transmission systems and media
- Series H Transmission of non-telephone signals
- Series I Integrated services digital network
- Series J Transmission of sound-programme and television signals
- Series K Protection against interference
- Series L Construction, installation and protection of cables and other elements of outside plant
- Series M Maintenance: international transmission systems, telephone circuits, telegraphy, facsimile and leased circuits
- Series N Maintenance: international sound-programme and television transmission circuits
- Series O Specifications of measuring equipment
- Series P Telephone transmission quality
- Series Q Switching and signalling
- Series R Telegraph transmission
- Series S Telegraph services terminal equipment
- Series T Terminal equipments and protocols for telematic services
- Series U Telegraph switching
- Series V Data communication over the telephone network
- Series X Data networks and open system communication**
- Series Z Programming languages