



INTERNATIONAL TELECOMMUNICATION UNION

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

X.810

(11/95)

DATA NETWORKS AND OPEN SYSTEM COMMUNICATIONS SECURITY

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – SECURITY FRAMEWORKS FOR OPEN SYSTEMS: OVERVIEW

ITU-T Recommendation X.810

(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.810 was approved on 21st of November 1995. The identical text is also published as ISO/IEC International Standard 10181-1.

NOTE

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

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	1
2.1 Identical Recommendations International Standards	1
2.2 Paired Recommendations International Standards equivalent in technical content	1
3 Definitions	2
3.1 Basic Reference Model definitions	2
3.2 Security architecture definitions	2
3.3 Additional definitions	2
4 Abbreviations	4
5 Notation	4
6 Organization	4
6.1 Part 1 – Overview	4
6.2 Part 2 – Authentication	4
6.3 Part 3 – Access control	5
6.4 Part 4 – Non-repudiation	5
6.5 Part 5 – Confidentiality	5
6.6 Part 6 – Integrity	6
6.7 Part 7 – Security audit and alarms	6
6.8 Key management	6
7 Common concepts	6
7.1 Security information	7
7.2 Security domain	7
7.2.1 Security policy and security policy rules	7
7.2.2 Security domain authority	8
7.2.3 Inter-relationships among security domains	8
7.2.4 Establishment of secure interaction rules	9
7.2.5 Inter-domain security information transfer	9
7.3 Security policy considerations for specific security services	9
7.4 Trusted entities	9
7.5 Trust	10
7.6 Trusted third parties	10
8 Generic security information	10
8.1 Security labels	10
8.2 Cryptographic checkvalues	11
8.3 Security certificates	11
8.3.1 Introduction to security certificates	11
8.3.2 Verification and chaining of security certificates	12
8.3.3 Revocation of security certificates	12
8.3.4 Re-use of security certificates	12
8.3.5 Security certificate structure	12
8.4 Security tokens	13
9 Generic security facilities	13
9.1 Management related facilities	13
9.1.1 Install SI	13
9.1.2 Deinstall SI	13
9.1.3 Change SI	13



	<i>Page</i>
9.1.4 Validate SI	14
9.1.5 Invalidate SI.....	14
9.1.6 Disable/Re-enable security service	14
9.1.7 Enrol	14
9.1.8 Un-enrol	14
9.1.9 Distribute SI.....	14
9.1.10 List SI	14
9.2 Operational related facilities	14
9.2.1 Identify trusted security authorities.....	14
9.2.2 Identify secure interaction rules	14
9.2.3 Acquire SI.....	14
9.2.4 Generate SI.....	14
9.2.5 Verify SI	15
10 Interactions between security mechanisms	15
11 Denial of service and availability	15
12 Other requirements	16
Annex A – Some examples of protection mechanisms for security certificates.....	17
A.1 Protection using an OSI communications security service	17
A.2 Protection using a parameter within the security certificate	17
A.2.1 The authentication method.....	17
A.2.2 The secret key method	17
A.2.3 The public key method.....	18
A.2.4 The one-way function method	18
A.3 Protection of the internal and external parameters while in transit.....	18
A.3.1 Transfer of internal parameters to the issuing security authority	18
A.3.2 Transfer of external parameters among entities	18
A.4 Use of security certificates by single entities or by groups of entities	19
A.5 Linking a security certificate with accesses	19
Annex B – Bibliography.....	20

Summary

This Recommendation | International Standard defines the framework within which security services for open systems are specified. This part of the Security Frameworks describes the organization of the security framework, defines security concepts which are required in more than one part of the security framework, and describes the interrelationship of the services and mechanisms identified in other parts of the framework.

Introduction

Many applications have requirements for security to protect against threats to the communication of information. Some commonly known threats, together with the security services and mechanisms that can be used to protect against them are described in CCITT Rec. X.800 | ISO 7498-2.

This Recommendation | International Standard defines the framework within which security services for open systems are specified.

Page 312/313

p 12

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – SECURITY FRAMEWORKS FOR OPEN SYSTEMS: OVERVIEW

1 Scope

The security frameworks address the application of security services in an Open Systems environment, where the term *Open Systems* is taken to include areas such as Database, Distributed Applications, ODP 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 are 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.

The security frameworks provide the basis for further standardization, providing consistent terminology and definitions of generic abstract service interfaces for specific security requirements. They also categorize the mechanisms that can be used to achieve those requirements.

One security service frequently depends on other security services, making it difficult to isolate one part of security from the others. The security frameworks address particular security services, describe the range of mechanisms that can be used to provide the security services, and identify interdependancies between the services and the mechanisms. The description of these mechanisms may involve a reliance on a different security service, and it is in this way that the security frameworks describe the reliance of one security service on another.

This part of the security frameworks:

- describes the organization of the security frameworks;
- defines security concepts which are required in more than one part of the security frameworks;
- describes the inter-relationship of the services and mechanisms identified in other parts of the frameworks.

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 indicated 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 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*.

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*.



ISO/IEC 10181-1 : 1996 (E)

3 Definitions

The following definitions are used either in the overview or are common to two or more of the subsequent parts of the security frameworks.

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

3.1 Basic Reference Model definitions

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

- (N)-layer;
- (N)-entity;
- (N)-protocol-data-unit;
- application process;
- real open system;
- real system.

3.2 Security architecture definitions

This Recommendation | International Standard makes use of the following terms defined in CCITT Rec. X.800 | ISO 7498-2:

- access control;
- availability;
- ciphertext;
- cryptographic checkvalue;
- decipherment;
- denial of service;
- digital signature;
- encipherment;
- insider threat;
- key;
- key management;
- plaintext;
- outsider threat;
- security audit;
- security label;
- security policy;
- sensitivity;
- threat.

3.3 Additional definitions

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

3.3.1 asymmetric cryptographic algorithm: An algorithm for performing encipherment or the corresponding decipherment in which the keys used for encipherment and decipherment differ.

NOTE – With some asymmetric cryptographic algorithms, decipherment of ciphertext or the generation of a digital signature requires the use of more than one private key.

3.3.2 certification authority: An entity that is trusted (in the context of a security policy) to create security certificates containing one or more classes of security-relevant data.

3.3.3 conditionally trusted entity: An entity that is trusted in the context of a security policy, but which cannot violate the security policy without being detected.