



TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(10/2003)

Security

Security architecture for systems providing end-to-end communications

ITU-T Recommendation X.805

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

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
Satellite data transmission systems	X.350–X.369
IP-based networks	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.629
Efficiency	X.630–X.639
Quality of service	X.640–X.649
Naming, Addressing and Registration	X.650–X.679
Abstract Syntax Notation One (ASN.1)	X.680–X.699
OSI MANAGEMENT	
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 and ODMA functions	X.730–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

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

ITU-T Recommendation X.805

Security architecture for systems providing end-to-end communications

Summary

This Recommendation defines the general security-related architectural elements that, when appropriately applied, can provide end-to-end network security.

...

Source

ITU-T Recommendation X.805 was approved by ITU-T Study Group 17 (2001-2004) under the ITU-T Recommendation A.8 procedure on 29 October 2003.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications. The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. 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 Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

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.

NOTE

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

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure e.g. interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementors are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database.

© ITU 2004

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

CONTENTS

Page

1	Scope	1
2	References.....	1
3	Terms and definitions	1
4	Abbreviations and acronyms	1
5	Security architecture	2
6	Security dimensions.....	3
6.1	Access control security dimension	3
6.2	Authentication security dimension	3
6.3	Non-repudiation security dimension	3
6.4	Data confidentiality security dimension.....	3
6.5	Communication security dimension	3
6.6	Data integrity security dimension.....	4
6.7	Availability security dimension.....	4
6.8	Privacy security dimension.....	4
7	Security layers	4
7.1	The infrastructure security layer.....	5
7.2	The services security layer	5
7.3	The applications security layer	5
8	Security planes.....	5
8.1	The management security plane	6
8.2	The control security plane	6
8.3	The end-user security plane	7
9	Security threats	7
10	Description of the objectives achieved by application of security dimensions to security layers	9
10.1	Securing the infrastructure layer	11
10.2	Securing the services layer	14
10.3	Securing the applications layer.....	17

Introduction

The telecommunications and information technology industries are seeking cost-effective comprehensive security solutions. A secure network should be protected against malicious and inadvertent attacks and should have high availability, appropriate response time, reliability, integrity, scalability, and provide accurate billing information. Security capabilities in products are crucial to the overall network security (including applications and services). However, as more products are combined to provide total solutions, the interoperability, or the lack thereof, will define the success of the solution. Security must not only be a thread of concern for each product or service, but must be developed in a manner that promotes the interweaving of security capabilities in the overall end-to-end security solution. To achieve such a solution in a multi-vendor environment, network security should be designed around a standard security architecture.

ITU-T Recommendation X.805

Security architecture for systems providing end-to-end communications

1 Scope

This Recommendation defines a network security architecture for providing end-to-end network security. The architecture can be applied to various kinds of networks where the end-to-end security is a concern and independently of the network's underlying technology. This Recommendation defines the general security-related architectural elements that are necessary for providing end-to-end security. The objective of this Recommendation is to serve as a foundation for developing the detailed recommendations for the end-to-end network security.

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- ITU-T Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications*.

3 Terms and definitions

This Recommendation uses the following terms from ITU-T Rec. X.800:

- access control;
- availability;
- authentication;
- confidentiality;
- data integrity;
- non-repudiation;
- privacy.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations:

AAA	Authentication, Authorization and Accounting
ASP	Application Service Provider
ATM	Asynchronous Transfer Mode
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Service
DoS	Denial of Service
DS-3	Digital Signal level 3
FTP	File Transfer Protocol

IP	Internet Protocol
IPSec	IP Security Protocol
OAM&P	Operations, Administration, Maintenance & Provisioning
OSI	Open Systems Interconnection
PSTN	Public Switched Telephone Network
PVC	Permanent Virtual Circuit
QoS	Quality of Service
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SONET	Synchronous Optical Network
SS7	Signalling System No. 7
SSL	Secure Socket Layer (Encryption and authentication protocol)
VoIP	Voice over IP
VPN	Virtual Private Network

5 Security architecture

The security architecture was created to address the global security challenges of service providers, enterprises, and consumers and is applicable to wireless, optical and wire-line voice, data and converged networks. This security architecture addresses security concerns for the management, control, and use of network infrastructure, services and applications. The security architecture provides a comprehensive, top-down, end-to-end perspective of network security and can be applied to network elements, services, and applications in order to detect, predict, and correct security vulnerabilities.

The security architecture logically divides a complex set of end-to-end network security-related features into separate architectural components. This separation allows for a systematic approach to end-to-end security that can be used for planning of new security solutions as well as for assessing the security of the existing networks.

The security architecture addresses three essential questions with regard to the end-to-end security:

- 1) What kind of protection is needed and against what threats?
- 2) What are the distinct types of network equipment and facility groupings that need to be protected?
- 3) What are the distinct types of network activities that need to be protected?

These questions are addressed by three architectural components: security dimensions, security layers and security planes.

The principles described by the security architecture can be applied to a wide variety of networks independently of the network's technology or location in the protocol stack.

The following clauses describe in detail the architectural elements and their functions with respect to the major security threats.

6 Security dimensions

A security dimension is a set of security measures designed to address a particular aspect of the network security. This Recommendation identifies eight such sets that protect against all major security threats. These dimensions are not limited to the network, but extend to applications and end user information as well. In addition, the security dimensions apply to service providers or enterprises offering security services to their customers. The security dimensions are:

- 1) Access control;
- 2) Authentication;
- 3) Non-repudiation;
- 4) Data confidentiality;
- 5) Communication security;
- 6) Data integrity;
- 7) Availability; and
- 8) Privacy.

Properly designed and implemented security dimensions support security policy that is defined for a particular network and facilitate the rules set by the security management.

6.1 Access control security dimension

The access control security dimension protects against unauthorized use of network resources. Access control ensures that only authorized personnel or devices are allowed access to network elements, stored information, information flows, services and applications. In addition, Role-Based Access Control (RBAC) provides different access levels to guarantee that individuals and devices can only gain access to, and perform operations on, network elements, stored information, and information flows that they are authorized for.

6.2 Authentication security dimension

The authentication security dimension serves to confirm the identities of communicating entities. Authentication ensures the validity of the claimed identities of the entities participating in communication (e.g., person, device, service or application) and provides assurance that an entity is not attempting a masquerade or unauthorized replay of a previous communication.

6.3 Non-repudiation security dimension

The non-repudiation security dimension provides means for preventing an individual or entity from denying having performed a particular action related to data by making available proof of various network-related actions (such as proof of obligation, intent, or commitment; proof of data origin, proof of ownership, proof of resource use). It ensures the availability of evidence that can be presented to a third party and used to prove that some kind of event or action has taken place.

6.4 Data confidentiality security dimension

The data confidentiality security dimension protects data from unauthorized disclosure. Data confidentiality ensures that the data content cannot be understood by unauthorized entities. Encryption, access control lists and file permissions are methods often used to provide data confidentiality.

6.5 Communication security dimension

The communication security dimension ensures that information flows only between the authorized end points (the information is not diverted or intercepted as it flows between these end points).