INTERNATIONAL STANDARD

ISO/IEC 11577

First edition
1995-05-15

Information technology — Open Systems Interconnection — Network layer security protocol

Technologies de l'information — Interconnexion de systèmes ouverts (OSI) — Protocole de sécurité de la couche de réseau

Reference number
ISO/IEC 11577:1995(E)

CONTENTS

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 11577 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*, in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.273.

NOTE — The publication dates of ISO/IEC 7498-1, ISO/IEC 9646-1, ISO/IEC 9646-2, ISO/IEC 10731, ISO/IEC 10745 and ISO/IEC TR 13594, referenced in this International Standard, differ from those referenced in the identical ITU Recommendation X.273 due to the publication of new editions during final preparation of this International Standard.

Annexes A to D form an integral part of this International Standard. Annexes E to H are for information only.

Introduction

The protocol defined by this ITU-T Recommendation | International Standard is used to provide security services in support of an instance of communication between lower layer entities. This protocol is positioned with respect to other Standards by the layered structure defined in CCITT Rec. X.200 | ISO/IEC 7498-1 and by the Network layer organization as defined in ISO 8648 and extended by ITU-T Rec. X.802 | ISO/IEC TR 13594 (Lower Layer Security Model). It provides security services in support of both connection-mode and connectionless-mode Network services. In particular, this protocol is located in the Network layer, and it has functional interfaces and clearly defined service interfaces at its upper and lower boundaries.

To evaluate conformance of a particular implementation, it is necessary to have a statement of which capabilities and options have been implemented for a given OSI protocol. Such a statement is called a Protocol Implementation Conformance Statement (PICS).

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – NETWORK LAYER SECURITY PROTOCOL

1 Scope

This ITU-T Recommendation | International Standard specifies a protocol to be used by End Systems and Intermediate Systems in order to provide security services in the Network layer, which is defined by CCITT Rec. X.213 | ISO/IEC 8348, and ISO 8648. The protocol defined in this ITU-T Recommendation | International Standard is called the Network Layer Security Protocol (NLSP).

This ITU-T Recommendation | International Standard specifies:

1) Support for the following security services defined in CCITT Rec. X.800 | ISO 7498-2:
   a) peer entity authentication;
   b) data origin authentication;
   c) access control;
   d) connection confidentiality;
   e) connectionless confidentiality;
   f) traffic flow confidentiality;
   g) connection integrity without recovery (including Data Unit Integrity, in which individual SDUs on a connection are integrity protected);
   h) connectionless integrity.
2) The functional requirements for implementations that claim conformance to this ITU-T Recommendation | International Standard.

The procedures of this protocol are defined in terms of:

a) requirements on the cryptographic techniques that can be used in an instance of this protocol;
b) requirements on the information carried in the security association used in an instance of communication.

Although the degree of protection afforded by some security mechanisms depends on the use of some specific cryptographic techniques, correct operation of this protocol is not dependent on the choice of any particular encipherment or decipherment algorithm. This is a local matter for the communicating systems.

Furthermore, neither the choice nor the implementation of a specific security policy are within the scope of this ITU-T Recommendation | International Standard. The choice of a specific security policy, and hence the degree of protection that will be achieved, is left as a local matter among the systems that are using a single instance of secure communications. This ITU-T Recommendation | International Standard does not require that multiple instances of secure communications involving a single open system must use the same security protocol.

Annex D provides the PICS proforma for the Network Layer Security Protocol in compliance with the relevant guidance given in ISO/IEC 9646-2.

2 Normative references

The following Recommendations and International Standards contain provisions which, though reference in this text, constitute provisions of this ITU-T Recommendation | International Standard. At time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this ITU-T 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 a registry of currently valid International Standards. The Telecommunications Standardization Bureau of ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

- CCITT Recommendation X.213 (1992) | ISO/IEC 8348:1993, *Information technology – Open Systems Interconnection – Network Service Definition.*
- ITU-T Recommendation X.233 (1993) | ISO/IEC 8473-1:1994, *Information technology – Protocol for providing the connectionless-mode network service: Protocol specification.*
- ITU-T Recommendation X.802 (1994) | ISO/IEC TR 13594:—[1] , *Information technology – Open Systems Interconnection – Lower layers security model.*
- ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:—[1], *Information technology – Open Systems Interconnection – Upper layers security model.*

2.2 Paired Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.200 (1988), *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model.*

  ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model.*

- 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).*

- ITU-T Recommendation X.210 (1993), *Information technology – Open Systems Interconnection – Conventions for the definition of OSI services.*

  ISO/IEC 10731:1994, *Information technology – Open Systems Interconnection – Basic Reference Model – Conventions for the definition of OSI services.*

- CCITT Recommendation X.223 (1988), *Use of X.25 to provide the OSI connection-mode network service.*

  ISO/IEC 8878:1992, *Information technology – Telecommunications and information exchange between systems – Use of X.25 to provide the OSI connection-mode network service.*

- CCITT Recommendation X.290 (1992), *OSI conformance testing methodology and framework for protocol Recommendations for CCITT applications – General concepts.*

  ISO/IEC 9646-1:1994, *Information technology – Open Systems Interconnection – Conformation testing methodology and framework – Part 1: General concepts.*

- CCITT Recommendation X.291 (1992), *OSI conformance testing methodology and framework for protocol Recommendations for CCITT applications – Abstract test suite specification.*

  ISO/IEC 9646-2:1994, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 2: Abstract test suite specification.*

- CCITT Recommendation X.509 (1988), *Information technology – Open Systems Interconnection – The Directory: Authentication framework.*

  ISO/IEC 9594-8:1990, *Information technology – Open Systems Interconnection – The Directory – Part 8: Authentication framework.*

- 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.*

[1] To be published.

2.3 Additional references

- ISO/IEC 8208:1990, *Information technology – Data communications – X.25 Packet Layer Protocol for Data Terminal Equipment.*
- ISO 8648:1988, *Information processing systems – Open Systems Interconnection – Internal organization of the Network Layer.*
- ISO/IEC 9834-1:1993, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities – Part 1: General procedures.*
- ISO/IEC 9834-3:1990, *Information technology – Open Systems Interconnection – Procedures for the operation of OSI Registration Authorities – Part 3: Registration of object identifier component values for joint ISO/CCITT use.*
- ISO/IEC 9979:1991, *Data cryptographic techniques – Procedures for the registration of cryptographic algorithms.*
- CCITT 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.*