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

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.*

3 Definitions

3.1 Reference Model definitions

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

a) End System;
b) Network Entity;
c) Network Layer;
d) Network Protocol;
e) Network Protocol Data Unit;
f) Network Relay;
g) Network Service;
h) Network Service Access Point;
i) Network Service Access Point Address;
j) Network Service Data Unit;
k) Protocol Data Unit;
l) Routing;
m) Service;
n) Service Data Unit.

3.2 Security Architecture definitions

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

a) Access Control;
b) Confidentiality;
c) Connection Integrity Without Recovery;
d) Connectionless Confidentiality;
e) Connectionless Integrity;
f) Data Origin Authentication;
g) Decipherment;

h) Digital Signature;

i) Encipherment;

j) Peer Entity Authentication;

k) Security Label;

l) Security Service;

m) Traffic Flow Confidentiality.

3.3 Service Convention definitions

This Recommendation | International Standard makes use of the following terms as defined in ITU-T Recommendation X.210 | ISO/IEC 10731:

a) Service Provider;

b) Service User.

3.4 Network Service definitions

This Recommendation | International Standard makes use of the following terms as defined in CCITT Recommendation X.213 | ISO 8348:

– subnetwork point of attachment.

3.5 Internal Organization of the Network Layer definitions

This Recommendation | International Standard makes use of the following terms as defined in ISO 8648:

a) Intermediate System;

b) Relay System;

c) Subnetwork;

d) Subnetwork Access Protocol;

e) Subnetwork Dependent Convergence Protocol;

f) Subnetwork Independent Convergence Protocol.

3.6 Connectionless Network Protocol definitions

This Recommendation | International Standard makes use of the following terms as defined in ITU-T Recommendation X.233 | ISO/IEC 8473-1:

a) Initial PDU;

b) Local Matter;

c) Reassembly;

d) Segment.

3.7 Upper Layer Security Model definitions

This Recommendation | International Standard makes use of the following terms as defined in ITU-T Recommendation X.803 | ISO/IEC 10745:

a) Secure Interaction Policy;

b) Security Relationship.

3.8 Conformance Testing definitions

This Recommendation | International Standard makes use of the following terms as defined in CCITT Recommendation X.290 | ISO/IEC 9646-1:

a) PICS proforma;

b) Protocol Implementation Conformance Statement;

c) Static Conformance Overview.

3.9 Additional definitions

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

3.9.1 Frozen SA-ID: An SA-ID that is not available for assignment to a Security Association because of requirements to prevent re-use.

3.9.2 Pairwise Key: A pair of related (public key) or identical (secret key) key values for use between two particular parties.

3.9.3 Security Control Information: Protocol Control Information (PCI) exchanged by a security protocol for the purpose of establishing or maintaining a security association.

3.9.4 SA-Attributes: The collection of information required to control the security of communications between an entity and its remote peer(s).

3.9.5 Security Association: A security relationship between communicating lower layer entities for which there exists corresponding SA-Attributes.

3.9.6 Data Unit Integrity: A form of connection integrity in which the integrity of individual SDUs is protected but errors in the sequence of SDUs are not detected.

3.9.7 In-band: Performed by protocol mechanisms using the SA PDU as defined in this ITU-T Recommendation | International Standard.

3.9.8 Out-of-band: Performed by means other than the use of the SA PDU.

3.9.9 Security Rules: Local information which, given security services selected, specify the security mechanisms to be used including all parameters needed for the operation of the mechanisms.

NOTE – This information may form a part of a Security Interaction Rules as defined in CCITT Recommendation X.803 | ISO/IEC 10745.

3.9.10 Label: See "Security Label" (CCITT Recommendation X.800 | ISO 7498-2).

4 Abbreviations

4.1 Data Units

NPDU	Network Protocol Data Unit
NSDU	Network Service Data Unit
PDU	Protocol Data Unit
SDU	Service Data Unit

4.2 Protocol Data Unit Fields

LI	Length Indicator

4.3 Parameters

QOS	Quality of Service

4.4 Miscellaneous

ASSR	Agreed Set of Security Rules
CL	Connectionless mode
CLNP	Connectionless mode Network Protocol
CLNS	Connectionless mode Network Service
CO	Connection mode
CSC PDU	Connection Security Control PDU
DU	Data Unit
EKE	Exponential Key Exchange (see Annex H)

ES	End System
ICV	Integrity Check Value
IS	Intermediate System
ISN	Integrity Sequence Number
KEK	Key Enciphering Key
NLSP	Network Layer Security Protocol
NLSP CO	NLSP for Connection mode
NLSP CL	NLSP for Connectionless mode
NLSPE	NLSP Entity
NS	Network Service
NSAP	Network Service Access Point
PCI	Protocol Control Information
PDU	Protocol Data Unit
SA	Security Association
SA-ID	Security Association Identifier
SA-P	Security Association Protocol
SA-PDU	Security Association PDU
SCI	Security Control Information
SDT PDU	Secure Data Transfer PDU
SN	Subnetwork
SNAcP	Subnetwork Access Protocol
SNICP	Subnetwork Independent Convergence Protocol
SNPA	Subnetwork Point of Attachment
UN	Underlying Network

5 Overview of the Protocol

5.1 Introduction

There are two basic modes of operation of the NLSP protocol which are:

a) NLSP-CL – For use in providing a secure connectionless network service.

b) NLSP-CO – For use in providing a secure connection oriented network service.

Both modes of NLSP operate as a sub-layer of the Network layer. The service provided to the entity above is called the NLSP service and the service assumed to be provided to NLSP is called the Underlying Network (UN) service. Primitives and parameters are prefixed with NLSP or UN to clearly distinguish the service being referenced. The UN and NLSP services are "notional interfaces", i.e. described as if they were a layer service but potentially residing entirely within the Network layer, depending on the location of the NLSP sub-layer (see Annex E).

Both modes of NLSP can be implemented in end systems and in intermediate systems. Both modes allow for the source and destination NLSP address and other NLSP CONNECT parameters to be optionally protected. NLSP-CO can be operated anywhere within the Network layer. NLSP-CL can be operated anywhere within the Network layer above the Subnetwork Dependent Convergence Protocol (see ISO 8648).

The protocol is designed so that it can be optimized to meet a range of requirements from environments where the main concern is high security to environments where the main concern is optimized performance. In particular, a "no-header" option is provided in NLSP-CO in which minimal impact on communications efficiency is achieved, although potentially with reduced security.

The NLSP protocol makes use of the concept of a Security Association (SA) which may exist outside of a specific connectionless UNITDATA or connection. A set of attributes defining parameters for security (e.g. algorithm, keys, etc.) are defined for the SA.

The protocol provides the same mode of service (CO or CL) at its upper and lower boundaries.

This protocol supports the use of a wide range of specific security mechanisms (both standardized and non-standardized). Users and implementors should choose the security mechanisms for use with this protocol appropriate to enforce their security service and level of protection required. Clauses 9 to 12 and Annex C define support for a set of specific mechanisms for all the security services required for NLSP.

The security protection which NLSP attempts to provide is derived from security service requirements established by the security domain administration.

NOTE – Use of the NLSP service Protection QOS parameter is a local matter and outside the scope of this ITU-T Recommendation | International Standard.

5.2 Overview of Services Provided

NLSP provides those security services defined in CCITT Recommendation X.800 | ISO 7498-2 to be appropriate to the Network layer, together with the OSI Network layer services as defined in CCITT Recommendation X.213 | ISO/IEC 8348.

NLSP-CL supports the following security services if selected:

a) Data Origin Authentication.

b) Access Control.

c) Connectionless Confidentiality – This protection optionally includes all NLSP service parameters depending on security services selected.

d) Traffic Flow Confidentiality.

e) Connectionless Integrity – This protection optionally includes all NLSP service parameters depending on security services selected.

NLSP-CO supports the following security services if selected:

a) Peer Entity Authentication.

b) Access Control.

c) Connection Confidentiality – This protection optionally includes all NLSP connection parameters depending on security services selected.

d) Traffic Flow Confidentiality.

e) Connection Integrity without Recovery – This protection optionally includes all NLSP connection parameters depending on security services selected. This protection also optionally includes integrity of a sequence of SDUs.

5.3 Overview of Services Assumed

The services assumed below NLSP are referred to as the Underlying Network (UN) service. The underlying services assumed by NLSP-CL use the same primitives as those defined in the Connectionless Network Service (CCITT Recommendation X.213 | ISO/IEC 8348).

For NLSP-CO, the UN-Interface is modelled in two parts:

a) A service using the same primitives as CCITT Recommendation X.213 | ISO/IEC 8348 with the addition of a parameter called the UN Authentication parameter.

b) The mapping of this service either onto the standard Network service or directly onto CCITT Recommendation X.25 | ISO/IEC 8208.

The Network address carried in the NLSP primitives is termed the NLSP-address. This service parameter identifies the NLSP user entity, which may or may not be a Transport entity depending on whether other Network layer protocols are used above NLSP and whether the NLSPE is located in an ES or an IS. The Network address passed to the Underlying Network is termed the UN address. This UN parameter is equivalent to the SNPA address if and only if there is no protocol operating between the NLSP-entity and the subnetwork access entity.

5.4 Security Associations and Security Rules

5.4.1 Security Associations

The operation of NLSP is controlled by a collection of security management information (e.g. security services selection information, security algorithm identifier, cryptographic keys) called Security Association Attributes (SA Attributes). The existence of the collection of security association attributes required to govern the provision security services between communicating entities is termed a Security Association.

Security Associations are described further in ITU-T Recommendation X.802 | ISO/IEC TR 13594 (Lower Layers Security Model).

The SA Attributes required for both NLSP-CL and NLSP-CO are defined in 6.2. The SA Attributes required for NLSP-CL are defined in 7.4. The attributes required for NLSP-CO are defined in 8.4. Further mechanism specific attributes are defined in 10.2, 11.2 and 12.2.

In order to protect an instance of communication (a connectionless SDU or a connection) an existing suitable SA is used, or if no suitable SA exists one needs to be established between the communicating parties.

The Security Association may be established out-of-band or using the NLSP in-band SA-P. The NLSP SA-P exchanges Security Control Information (SCI) through use of SA PDUs and/or SDT PDUs with content Data Type SA-P. SA-PDUs shall be used if the SCI is to be carried in the clear. Either the SA-PDU or the SDT PDU shall be used if the SCI is to be protected. This SCI is used to complete the SA Attributes building on any pre-established SA Attributes and Security Rules.

NLSP-CO also supports the exchange of information to update "dynamic" SA Attributes (for example, working keys, see Annex G) during connection establishment and within a connection. An update to the dynamic SA Attributes shall not change the security services provided.

Use of an in-band SA-P in conjunction with NLSP-CL is defined in 7.5. Use of an in-band SA-P with NLSP-CO is defined in 8.5 (during connection establishment) and 8.11.1 (during data transfer). A protocol for realizing the in-band SA-P is defined in Annex C of this Specification. An example of a mechanism to establish a key for use with this protocol is given in Annex H.

5.4.2 Security Rules

The setting of a number of SA Attributes will be constrained by security policy. This part of the security policy is termed the Set of Security Rules for the Protocol Entity. The Set of Security Rules for a protocol entity may constrain such SA Attributes as field lengths, the encipherment algorithms, etc., to be a single value or a set of values to be further constrained by other means (e.g. OSI systems management or using a SA-P exchange).

Where alternative protection levels are offered, the Set of Security Rules will define alternative constraints to meet the differing qualities of protection required.

When used for operation between NLSPEs a unique identifier for such Sets of Security Rules needs to be established and is known as an Agreed Set of Security Rules (ASSR). The ASSR identifier may be exchanged as part of Security Association establishment.

Security rules are described further in ISO/IEC TR 13594 (Lower Layers Security Model).

5.5 Overview of Protocol – Protection Functions

5.5.1 Scope of Protection

Both NLSP-CO and NLSP-CL have three different modes of operation which support three basic degrees of protection:

a) *Protection of all NLSP service parameters*

In this mode all NLSP service parameters including addresses and all user data, excluding those that are negotiated with the service provider (QOS, Receipt Confirmation Selection, Expedited Data Selection), are protected.

This mode is selected by SA Attribute Param_Prot (see 6.2) being TRUE.

b) *Protection of NLSP Userdata*

In this mode user data is protected but other NLSP service parameters are not.

This mode is selected by SA Attribute Param_Prot being FALSE.

For NLSP-CO there are further sub-modes of protection of NLSP Userdata, either:

1) All NLSP Userdata is protected (including NLSP Userdata in the NLSP-CONNECT, NLSP-DATA and NLSP-DISCONNECT service primitives).

2) NLSP Userdata in NLSP DATA is protected.

The sub-modes for NLSP are further selected by a SA Attribute Protect_Connect_Params (see 8.3). If Protect_Connect_Params is TRUE then all NLSP Userdata is protected, else only NLSP Userdata in NLSP-DATA is protected. Protect_Connect_Params shall be forced to TRUE (i.e. all NLSP Userdata is protected) if Param_Prot is TRUE.

c) *No Protection*

In this mode all NLSP service parameters are directly copied onto the equivalent UN service parameters. All the procedures of NLSP are bypassed.

This mode is selected locally based on the addresses of the communicating peers and local security service requirements.

5.5.2 Quality of Protection

The realization of security (protection) QOS in the OSI lower layers is accomplished by implementations selecting security services to be applied via locally controlled security policy. Any in-band indication of security services selected is conveyed in a security association protocol which is independent of an instance of communication, implicitly by use of a security label or explicitly by other means. Hence, any exchange relating to selection of security services are independent of conveyance of QOS parameter across service interface boundaries.

NOTE – It is possible that there may also be a requirement to indicate the security services to higher layers. However, no immediate requirement for definition of specific protect QOS requirements has been established to date.

5.5.3 Data Protection Functions

5.5.3.1 SDT PDU Based

Both NLSP-CO and NLSP-CL can protect NLSP service parameters through use of a Secure Data Transfer PDU (SDT PDU). NLSP CO also has an alternative approach to protection of NLSP Userdata which is selected by the SA Attribute No_Header (see 8.3) being TRUE.

Use of the SDT PDU based procedures protect NLSP service parameters by:

a) encoding NLSP service parameters as an Octet-String-Before-Encapsulation;

b) if explicit security labelling is selected (SA Attribute Label is TRUE), then placing a security label in the Octet-String-Before-Encapsulation;

c) applying an encapsulation (and decapsulation) function which supports mechanisms for:

– traffic flow confidentiality;

– integrity and data origin authentication;

– confidentiality,

as appropriate to the security services selected. This function provides a protected octet string.

Subclauses 6.4.1.1 and 6.4.2.1 define generic, mechanism independent procedures for the use of the SDT PDU to protect data. Clause 11 defines support for one class of mechanism for SDT PDU based encapsulation. Other, privately defined, procedures for encapsulation may be used with the SDT PDU.

5.5.3.2 No Header (NLSP-CO only)

The NLSP CO No_Header mode protects NLSP Userdata by an encapsulation function which does not alter the length of the protected data. NLSP does not add any protocol control information to the protected data. The security services supported will depend on the mechanisms used but the encapsulation function shall at least provide confidentiality. The No_Header mode can only be used to protect a single service parameter (NLSP Userdata) and hence can only used if Param_Prot is FALSE.

Subclauses 6.4.1.2 and 6.4.2.2 define generic, mechanism independent procedures for the use of the No_Header mode to protect data. Clause 12 defines support for one class of mechanism for No_Header encapsulation. Other, privately defined, procedures for encapsulation may be used with the No_Header mode.