

STANDARD

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

	<i>Page</i>
1 Scope	1
2 Normative references	2
2.1 Identical Recommendations International Standards	2
2.2 Paired Recommendations International Standards equivalent in technical content	2
2.3 Additional References	3
3 Definitions	3
3.1 Reference Model definitions	3
3.2 Security Architecture definitions	3
3.3 Service Convention definitions	4
3.4 Network Service definitions	4
3.5 Internal Organisation of the Network Layer definitions	4
3.6 Connectionless Network Protocol definitions	4
3.7 Upper Layer Security Model definitions	4
3.8 Conformance Testing definitions	4
3.9 Additional definitions	5
4 Abbreviations	5
4.1 Data Units	5
4.2 Protocol Data Unit Fields	5
4.3 Parameters	5
4.4 Miscellaneous	5
5 Overview of the Protocol	6
5.1 Introduction	6
5.2 Overview of Services Provided	7
5.3 Overview of Services Assumed	7
5.4 Security Associations and Security Rules	8
5.5 Overview of Protocol – Protection Functions	8
5.6 Overview of Protocol – NLSP-CL	10
5.7 Overview of Protocol – NLSP-CO	11
6 Protocol Functions Common to NLSP-CL and NLSP-CO	13
6.1 Introduction	13
6.2 Common SA Attributes	13
6.3 Common Functions on a Request for an Instance of Communication	14
6.4 Secure Data Transfer Protocol Functions	14
6.5 Use of a Security Association Protocol	16

© ISO/IEC 1995

All rights reserved. Unless otherwise specified, 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 publisher.

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

Printed in Switzerland

This is a preview of "ISO/IEC 11577:1995". [Click here to purchase the full version from the ANSI store.](#)

7	Protocol Functions FOR NLSP-CL.....	16
	7.1 Services Provided by NLSP-CL	16
	7.2 Services Assumed	17
	7.3 Security Association Attributes	17
	7.4 Checks.....	17
	7.5 In-Band SA Establishment.....	17
	7.6 Processing NLSP-UNITDATA Request.....	17
	7.7 Processing UN-UNITDATA Indication	18
8	Protocol Functions for NLSP-CO	19
	8.1 Services Provided by NLSP-CO	19
	8.2 Services Assumed	20
	8.3 Security Association Attributes	21
	8.4 Checks and other Common Functions	21
	8.5 NLSP-Connect Functions	22
	8.6 NLSP-DATA Functions.....	33
	8.7 NLSP-EXPEDITED-DATA Functions	34
	8.8 RESET Functions.....	35
	8.9 NLSP-DATA ACKNOWLEDGE	36
	8.10 NLSP-DISCONNECT	36
	8.11 Other Functions.....	39
	8.12 Peer Entity Authentication.....	40
9	Overview of Mechanisms used	41
	9.1 Security Services and Mechanisms.....	41
	9.2 Functions Supported	42
10	Connection security control (NLSP-CO only).....	42
	10.1 Overview.....	42
	10.2 SA-Attributes	43
	10.3 Procedures.....	44
	10.4 CSC-PDU Fields used.....	45
11	SDT PDU Based encapsulation Function	45
	11.1 Overview.....	45
	11.2 SA Attributes	46
	11.3 Procedures.....	47
	11.4 PDU Fields used	49
12	No-Header Encapsulation Function (NLSP-CO only).....	49
	12.1 Overview.....	49
	12.2 SA Attributes	49
	12.3 Procedures.....	50
13	Structure and Encoding of PDUS	50
	13.1 Introduction.....	50
	13.2 Content Field Format	51

This is a preview of "ISO/IEC 11577:1995". [Click here to purchase the full version from the ANSI store.](#)

13.3	Protected Data.....	51
13.4	Security Association PDU	57
13.5	Connection Security Control PDU.....	57
14	Conformance.....	59
14.1	Static Conformance Requirements.....	59
14.2	Dynamic Conformance Requirements	61
14.3	Protocol Implementation Conformance Statement	61
Annex A	– Mapping UN primitives to CCITT Rec. X.213 ISO 8348	62
Annex B	– Mapping UN Primitives to CCITT Rec. X.25 ISO 8208	63
Annex C	– Security Association Protocol Using Key Token Exchange and Digital Signatures	64
C.1	Overview.....	64
C.2	Key Token Exchange (KTE)	65
C.3	SA-Protocol Authentication.....	65
C.4	SA Attribute Negotiation	66
C.5	SA Abort/Release.....	67
C.6	Mapping of SA-Protocol Functions to Protocol Exchanges	67
C.7	SA PDU – SA Contents	70
Annex D	– NLSP PICS Proforma	74
D.1	Introduction.....	74
D.2	Abbreviations and Special Symbols	74
D.3	Instructions for Completing the PICS Proforma.....	74
D.4	Identification.....	76
D.5	Features Common to NLSP-CO and NLSP-CL.....	77
D.6	Features Specific to NLSP-CL.....	81
D.7	Features Specific to NLSP-CO	83
Annex E	– Tutorial on some Basic Concepts of NLSP.....	87
E.1	Basis of Protection	87
E.2	Underlying vs NLSP Service	88
E.3	NLSP Addressing.....	88
E.4	Connection Mode NLSP	92
E.5	Connectionless Mode NLSP	94
E.6	Security Attributes and Associations	99
E.7	Dynamic Functional Relationship between NLSP and CLNP.....	99
E.8	Dynamic Functionality Related to Layered Model.....	101
Annex F	– Example of an Agreed Set of Security Rules	103
Annex G	– Security Associations and Attributes	105
Annex H	– Example Key Token Exchange – EKE Algorithm	107

This is a preview of "ISO/IEC 11577:1995". [Click here to purchase the full version from the ANSI store.](#)

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.

This is a preview of "ISO/IEC 11577:1995". [Click here to purchase the full version from the ANSI store.](#)

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).

This is a preview of "ISO/IEC 11577:1995". [Click here to purchase the full version from the ANSI store.](#)

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