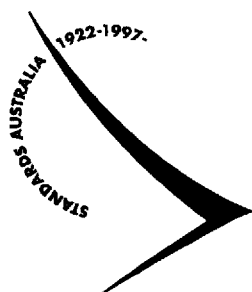


AS/NZS 4471:1997
ISO/IEC 11577:1995

Australian/New Zealand Standard[®]

**Information technology—
Open Systems Interconnection—
Network layer security protocol**



**LEADING AUSTRALIA
INTO THE FUTURE**



Documents

Document Sharing Hub

AS/NZS 4471:1997

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT/1, Information Systems—Interconnection. It was approved on behalf of the Council of Standards Australia on 24 February 1997 and on behalf of the Council of Standards New Zealand on 21 February 1997. It was published on 5 June 1997.

The following interests are represented on Committee IT/1:

Australian Bankers Association
 Australian Bureau of Statistics
 Australian Computer Society
 Australian Computer Users Association
 Australian Information Industry Association
 Australian Vice-Chancellors Committee
 Department of Defence, Australia
 Department of Industry, Science and Tourism, Australia
 Government Computing Service, New Zealand
 Information Exchange Steering Committee, Australia
 Institute of Information and Communication Technologies, CSIRO, Australia
 Telstra Corporation, Australia
 Telecom New Zealand

Review of Standards. To keep abreast of progress in industry, Joint Australian/New Zealand Standards are subject to periodic review and are kept up to date by the issue of amendments or new editions as necessary. It is important therefore that Standards users ensure that they are in possession of the latest edition, and any amendments thereto.

Full details of all Joint Standards and related publications will be found in the Standards Australia and Standards New Zealand Catalogue of Publications; this information is supplemented each month by the magazines 'The Australian Standard' and 'Standards New Zealand', which subscribing members receive, and which give details of new publications, new editions and amendments, and of withdrawn Standards.

Suggestions for improvements to Joint Standards, addressed to the head office of either Standards Australia or Standards New Zealand, are welcomed. Notification of any inaccuracy or ambiguity found in a Joint Australian/New Zealand Standard should be made without delay in order that the matter may be investigated and appropriate action taken.

AS/NZS 4471:1997

Australian/New Zealand Standard[®]

**Information technology—
Open Systems Interconnection—
Network layer security protocol**

First published as AS/NZS 4471:1997.

PUBLISHED JOINTLY BY:

STANDARDS AUSTRALIA
1 The Crescent,
Homebush NSW 2140 Australia

STANDARDS NEW ZEALAND
Level 10, Standards House,
155 The Terrace,
Wellington 6001 New Zealand

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT/1, Information Systems—Interconnection. It is identical with and has been reproduced from ISO/IEC 11577:1995, *Information technology—Open Systems Interconnection—Network layer security protocol*.

The objective of this Standard is to provide users of computer networks with a specification of a protocol to be used by end systems and intermediate systems in order to provide security services in the network layer of the OSI 7-layer model.

Users of this Standard are advised by Standards Australia and Standards New Zealand, under arrangements made with ISO and IEC, as well as certain other Standards organizations, that the number of this Standard is not reproduced on each page; its identity is shown only on the cover and title pages.

For the purpose of this Standard, the source text should be modified as follows:

- (a) *Terminology* The words ‘this Australian/New Zealand Standard’ should replace the words ‘this International Standard’ wherever they appear.
- (b) *Decimal marker* Substitute a full point for a comma where it appears as a decimal marker.
- (c) *References* The references to international Standards should be replaced by references, where appropriate, to the following Australian or Joint Australian/New Zealand Standards:

<i>Reference to International Standard or other publication</i>		<i>Australian or Joint Australian/New Zealand Standard</i>	
ISO		AS	
8648	Information processing systems— Open Systems Interconnection— Internal organization of the Network Layer	3622	Information processing systems— Open Systems Interconnection— Internal organization of the network layer
ISO/IEC		AS/NZS	
7498	Information technology— Open Systems Interconnection— Basic Reference Model	2777	Information processing systems— Open Systems Interconnection— Basic reference model
7498-1	Part 1: The Basic Model	2777.1	Part 1: The basic model
ISO		AS	
7498-2	Part 2: Security Architecture	2777.2	Part 2: Security architecture
ISO/IEC		AS/NZS	
8208	Information technology— Data communications—X.25 Packet Layer Protocol for Data Terminal Equipment	3621	Information technology— Data communications—X.25 packet layer protocol for data terminal equipment
8348	Information technology— Open Systems Interconnection— Network Service Definition	2994	Information technology— Open Systems Interconnection— Network service definition
8473	Information technology— Protocol for providing the connectionless-mode network service		
8473-1	Part 1: Protocol specification	—	

iii

ISO/IEC		AS	
8825	Information technology— Open Systems Interconnection— Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1)	3626	Information technology— Open Systems Interconnection— Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1)
		AS/NZS	
8878	Information technology— Telecommunications and information exchange between systems— Use of X.25 to provide the OSI connection-mode network service	3604	Information technology— Telecommunications and information exchange between systems— Use of X.25 to provide the OSI connection-mode network service
		AS	
9594	Information technology— Open Systems Interconnection— The Directory	4019	Information technology— Open Systems Interconnection— The Directory
9594-8	Part 8: Authentication framework	4019.8	Part 8: Authentication framework
9646	Information technology— Open Systems Interconnection— Conformation testing methodology and framework		
9646-1	Part 1: General concepts	—	
9646-2	Part 2: Abstract test suite specification	—	
		AS/NZS	
9834	Information technology— Open Systems Interconnection— Procedures for operation of OSI Registration Authorities	4153	Information technology— Open Systems Interconnection— Procedures for the operation of OSI registration authorities
9834-1	Part 1: General procedures	4153.1	Part 1: General procedures
9834-3	Part 3: Registration of object identifier component values for joint ISO/CCITT use	4153.3	Part 3: Registration of object identifier components values for joint ISO-CCITT use
9979	Data cryptographic techniques— Procedures for the registration of cryptographic algorithms	—	
10731	Information technology— Open Systems Interconnection— Basic Reference Model— Conventions for the definition of OSI services	—	
10745	Information technology— Open Systems Interconnection— Upper layers security model	—	
TR 13594	Information technology— Open Systems Interconnection— Lower layers security model	—	

CCITT

X.25

Interface between Data Terminal
Equipment (DTE) and Data
Circuit-Terminating Equipment
(DEC) for terminals operating in
Packet Mode and connected to
public data networks by dedicated
circuits

AS

—

© Copyright – STANDARDS AUSTRALIA/STANDARDS NEW ZEALAND

Users of Standards are reminded that copyright subsists in all Standards Australia and Standards New Zealand publications and software. Except where the Copyright Act allows and except where provided for below no publications or software produced by Standards Australia or Standards New Zealand may be reproduced, stored in a retrieval system in any form or transmitted by any means without prior permission in writing from Standards Australia or Standards New Zealand. Permission may be conditional on an appropriate royalty payment. Australian requests for permission and information on commercial software royalties should be directed to the head office of Standards Australia. New Zealand requests should be directed to Standards New Zealand.

Up to 10 percent of the technical content pages of a Standard may be copied for use exclusively in-house by purchasers of the Standard without payment of a royalty or advice to Standards Australia or Standards New Zealand.

Inclusion of copyright material in computer software programs is also permitted without royalty payment provided such programs are used exclusively in-house by the creators of the programs.

Care should be taken to ensure that material used is from the current edition of the Standard and that it is updated whenever the Standard is amended or revised. The number and date of the Standard should therefore be clearly identified.

The use of material in print form or in computer software programs to be used commercially, with or without payment, or in commercial contracts is subject to the payment of a royalty. This policy may be varied by Standards Australia or Standards New Zealand at any time.

CONTENTS

	<i>Page</i>
Scope.....	1
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
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
Abbreviations	5
4.1 Data Units	5
4.2 Protocol Data Unit Fields.....	5
4.3 Parameters.....	5
4.4 Miscellaneous	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
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
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

	<i>Page</i>
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
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

	<i>Page</i>
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

AUSTRALIAN/NEW ZEALAND STANDARD

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 – Conformance 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.



Documents

Document Sharing Hub

COPYRIGHT

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 be 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.

5.5.4 Connection Security Control (NLSP-CO only)

When establishing a connection, Connection Security Control PDUs are exchanged to flag the mode of NLSP connection establishment (whether with in-band SA-P, and whether NLSP CONNECT primitives are mapped to UN-CONNECT or UN-DATA primitives). In addition, the CSC PDU can support peer entity authentication and establish values for dynamic SA Attributes such as keys and integrity sequence numbers. This is to allow re-use of a previously established SA without incurring the overhead of the SA-P. It can also be used at any time during the lifetime of a connection to re-authenticate (prove shared knowledge of) the SA or update dynamic attributes.

The CSC PDU is only used in connection mode NLSP. Clause 8 defined the general, mechanism independent, procedures for use of the CSC PDU. Clause 10 defines support for one class of mechanism for authentication and key management. Other, privately defined, procedures for support of other classes of mechanism may be used with the CSC PDU.

NOTE – When using alternative mechanisms for authentication if the ISN mechanism defined in clause 11 is being used, then the alternative mechanism should establish an initial value for the ISN.

5.5.5 PDUs Used by NLSP

The following PDUs are used by NLSP:

- a) *Secure Data Transfer PDU* – To protect NLSP service primitive parameters and other data through encapsulation as outlined in 5.5.3.1. The structure of this PDU is defined in 13.3.
- b) *Connection Security Control PDU* – To control the mode of NLSP-CO connection establishment and optionally provide peer entity authentication as well as modify dynamic SA Attributes as outlined in 5.5.4. The structure of this PDU is defined in 13.5.

NOTE – The CSC PDU is only applicable to NLSP-CO.

- c) *SA PDU* – A PDU which allows the in-band exchange of security control information for the purposes of SA management as outlined in 5.4.1. The structure of this PDU is defined in 13.4.

In addition, with NLSP-CO, data can optionally be protected without the addition of any extra protocol control information (i.e. not using the SDT PDU) as outlined in 5.5.3.2 instead of using the SDT PDU.

5.6 Overview of Protocol – NLSP-CL

5.6.1 Clauses defining NLSP-CL

The procedures for NLSP-CL are defined in clauses 6 and 7 with the optional mechanism specific procedures for encapsulation in clause 11. These procedures use the SDT PDU as defined in 13.3 and optionally the SA PDU as defined in 13.4.

The following subclauses only provide an overview of the operation of NLSP-CL; the specific clauses identified above define the operation of NLSP-CL.

5.6.2 NLSP-CL Functions

NLSP supports the ability to transfer protected or unprotected connectionless data between peer NLSP users if so allowed by access control rules in the ASSR. The NLSPE determines locally (using security services selected, destination NLSP address and other management information) whether protection is needed or not. Protected data transfer can be with protection of all NLSP service parameters or just NLSP Userdata as determined by SA Attribute Param_Prot.

On receipt of an NLSP-UNITDATA request:

- The NLSP entity checks the SA and determines if unprotected communication is permitted with the destination address and if so whether protection is required.
- If no protection is required, the NLSP entity will copy all NLSP primitives and parameters to the corresponding UN primitives and parameters without change.
- If protection is required, the NLSP entity encapsulates the service parameters, forms an SDT PDU and transfers it as the UN Userdata of a UN-UNITDATA request along with UN Source Address, UN Destination Address and UN QOS parameters. This can protect just NLSP Userdata or all NLSP service parameters.

On receipt of a UN-UNITDATA indication, the NLSP entity:

- Uses the UN source address and local information to determine if communication is permitted with the destination address and if so whether protection is required.
- If protection is not required, the UN service parameters are copied to the NLSP parameters without change.
- If protection is required, the NLSP entity checks the SDT PDU and extracts the NLSP Userdata, and optionally other NLSP service parameters, using the decapsulation function. The Userdata, Source Address, Destination Address and QOS parameters are passed to the NLSP-user in the NLSP-UNITDATA indication.

NOTE – On transmit NLSP can operate after (before on receipt) ITU-T Recommendation X.233 | ISO/IEC 8473-1 (CLNP) protocol functionality protecting CLNP PDUs. Also, on transmit NLSP can operate before (after on receipt) CLNP protocol functionality with NLSP PDUs carried in CLNP PDU data fields. See Annex E for further discussion on the use of NLSP and CLNP.

Since some of the CLNP parameters may have security relevance, the selection of such parameters, after NLSP on transmit, must be considered with the local security policy. Some of the optional parameters to consider are the recording of route, partial and complete source routing, and hop count. Any of these parameters could give information about one's network that should not be available to the observer of network.

In order to determine that a NLSP-CL PDU had been carried within a CLNP PDU, on receipt, the receiver should either check the selector of the destination address for all zeroes or that the NLSP protocol identifier within the data field of the CLNP PDU is as defined in 13.3. Either check can be used to indicate that this PDU is for processing by the network layer versus sending it directly to the transport layer.

5.7 Overview of Protocol – NLSP-CO

5.7.1 Clauses Defining NLSP-CO

The procedures for NLSP-CO based on No_Header are defined in clauses 6 and 8 with the optional mechanism specific procedures in clause 12 for encapsulation and 10 for connection security control. These procedures use the CSC PDU as defined in 13.5 and optionally the SA PDU as defined in 13.4.

The procedures for NLSP-CO based on use of the SDT PDU are defined in clauses 6 and 8 with the optional mechanism specific procedures in clause 11 for encapsulation and 10 for connection security control. These procedures use the SDT PDU as defined in 13.3, the CSC PDU as defined in 13.5 and optionally the SA PDU as defined in 13.4.

The following subclauses only provide an overview of the operation of NLSP-CO; the specific clauses identified above define the operation of NLSP-CO.

5.7.2 NLSP-CO Unprotected Connections

If unprotected communications is permitted between the calling and called addresses, all NLSP/UN service parameters are copied directly to/from the NLSP service interface from/to the UN service interface.

5.7.3 NLSP-CONNECT

On receipt of an NLSP-CONNECT request, the NLSPE checks whether an SA currently exists with the required characteristics. If so, this may be used to protect the connection. Otherwise, a new SA is established in-band as part of the NLSP-CONNECT functions or out-of-band within a given timeout. If neither of these can be carried out, a NLSP-DISCONNECT is returned.

Two basic modes of establishment of an NLSP connection are supported. In one the NLSP CONNECT parameters are carried in the UN-CONNECT service primitives. In the other NLSP CONNECT parameters are carried, after being encapsulated in an SDT PDU, in UN-DATA after the UN connection has been established. There are variations of both modes of NLSP connection establishment, one for use with in-band SA-P exchanges (using either the SA PDU and/or SDT PDU with SA-P content Data Type) carried in UN-DATA, the other for use with an SA that has been established out-of-band.

The Connection Security Control (CSC) PDU is used to signal the mode of connection establishment and if in-band SA-P is not being carried, the exchange of CSC PDUs is also used to:

- establish mechanism specific security attributes for use in protecting the connection (for example, keys, integrity sequence numbers);
- perform peer entity authentication.

Clause 10 defines optional support for mechanisms for simple challenge-response based authentication and key management.

In the case of NLSP-CONNECT being carried in UN-CONNECT with in-band SA-P, a UN connection is established to carry the SA-P and then released, before carrying out the UN-CONNECT exchange carrying the NLSP CONNECT parameters. The CSC PDUs are used on the second UN-CONNECT exchange to re-authenticate the peer NLSP entities.

The SA establishment is achieved through the exchange of SA PDUs or SDT PDUs which carry the information needed to set up the required SA Attributes. Annex C defines an SA Protocol for this purpose.

If NLSP-CONNECT parameters are required to be protected they will be encapsulated before transfer.

5.7.3 NLSP-DATA

On receipt of an NLSP-DATA request:

- a) If SDT PDU based protection is selected, the NLSP entity encapsulates the appropriate service parameters forms an SDT PDU and transfers it as the UN Userdata of a UN-DATA request.
- b) If No_Header based protection is selected, the NLSP Userdata is enciphered and transferred in the UN Userdata of a UN-DATA request.

On receipt of a UN-DATA indication:

- a) If SDT PDU based protection is selected, the NLSP entity checks the PDU and extracts the NLSP Userdata, and possibly a NLSP Confirmation Request, using the decapsulation function.
- b) If No_Header based protection is selected, the UN Userdata is deciphered to obtain the NLSP Userdata.
- c) The NLSP service parameters is passed to the NLSP user in the NLSP-DATA indication.

5.7.4 NLSP-EXPEDITED-DATA

This is processed in a similar manner to an NLSP-DATA Request.

NOTE – When using the SDT PDU the encapsulation function may expand the size of the data. Thus, the restricted size of the Userdata field may require the protected expedited data to be further segmented and reassembled when crossing the Underlying Network.

5.7.5 NLSP-RESET

This is passed directly to the Underlying Network by NLSP. The secure connection is re-authenticated and mechanism specific attributes are re-established using CSC PDUs carried in UN-DATA.

NOTE – It may also be necessary to re-initialize some security mechanisms since data may have been lost. In particular, integrity sequencing mechanisms must be able to prevent replay attacks even after data loss.

5.7.6 NLSP-DATA-ACKNOWLEDGE

If all NLSP service parameters are to be protected (i.e. Param_Prot is TRUE) this is encapsulated, placed in an SDT PDU and passed to the UN sub-layer by NLSP. Otherwise this service primitive is mapped directly to UN-DATA-ACKNOWLEDGE.

5.7.7 NLSP-DISCONNECT

On receipt of an NLSP-DISCONNECT request, if protection of the service parameters is required by the mode of protection selected (see 5.5.1), the NLSP entity constructs a Secure Data Transfer PDU containing the NLSP-DISCONNECT request NLSP Userdata and optionally the other parameters. This PDU is either carried in UN-DATA before the UN connection is released or, if it fits, the SDT PDU can be carried in the UN Userdata parameter of a UN-DISCONNECT.

If protection of NLSP-DISCONNECT request parameters is not required, then these are sent in a UN-DISCONNECT request.

5.7.8 Other Functions

NLSP also supports the following functions which are initiated on timeout or other external events:

- a) CSC PDU exchange to modify dynamic SA Attributes such as keys.
- b) Security Test Exchange to check that the cryptographic aspects of the SA are correctly set up.
- c) Transmission of SDT PDUs containing only a traffic padding field for Traffic Flow Confidentiality.

6 Protocol Functions Common to NLSP-CL and NLSP-CO

6.1 Introduction

This clause describes protocol functions common to the connection and connectionless mode NLSP. These are used as called up in clauses 7 and 8.

6.2 Common SA Attributes

The following SA Attributes control the operation of connection mode and connectionless mode NLSP. Their description includes mnemonics used to refer to these attributes in this Specification.

NOTE – Where an SA Attribute is “constrained by ASSR”, this constraint may define a single value or a set of values. Where the ASSR defines a range of values, the attribute value may be established by OSI systems management, an SA-P exchange or by other means outside the scope of this Specification.

a) *SA Identification:*

My_SA-ID: Integer of range

0 to $(256 \times \text{maxlength}) - 1$

The local identifier of the SA. The value of this attribute shall be set up on SA establishment.

Your_SA-ID: Integer of range

0 to $(256 \times \text{maxlength}) - 1$

The remote identifier of the SA. The value of this attribute shall be set up on SA establishment.

maxlength is an integer of range 2 to 126.

NOTE 1 – It is a serious error for there to be more than one SA with the same local identifier.

b) *Indicator of whether the NLSPE initiated or responded to the SA establishment:*

Initiator: Boolean

This attribute indicates how the initiator to responder flag should be set to detect reflected PDUs.

The value of this attribute shall be set up on SA establishment.

c) *UN Address of peer NLSP entity:*

Peer_Adr: Octet string to format defined in CCITT Recommendation X.213 | ISO/IEC 8348

The value of this attribute shall be set up on SA establishment.

d) *NLSP Address of entities served through the remote peer:*

Adr_Served: Set of octet strings to format defined in CCITT Recommendation X.213 | ISO/IEC 8348

The value of this attribute shall be set up on SA establishment or pre-established.

e) *Security services selected for the SA:*

AC: Integer of range constrained by ASSR

TF_Conf: Integer of range constrained by ASSR

f) *Parameter Protection:*

Param_Prot: Boolean

Protect all NLSP service parameters other than those which may be modified by the underlying network (i.e. QOS, Receipt Confirmation Selection and Expedited Data Selection).

g) *Label mechanism attributes:*

Label: Boolean

Explicit labelling of connections/connectionless PDUs.

Label_Set: Set of

{Label_Ref: Integer

Label_Auth: Object Identifier

Label_Content: To format defined by
Label_Auth}

The value of these attributes are set up on SA establishment or pre-established.

NOTE 2 – It is expected that these labels will be registered according to procedures defined by ISO/IEC and ITU-T.

6.3 Common Functions on a Request for an Instance of Communication**6.3.1 Initial Checks**

An NLSPE receiving a request for an instance of communication (i.e. an NLSP-CONNECT or UNITDATA request) shall check that:

- a) The NLSP Calling or Source Address is an NLSP address served by this NLSPE.
- b) The required security services can be provided by this NLSPE.

6.3.2 Identification of the Security Association

An NLSPE receiving a request for an instance of communication (that is, an NLSP-CONNECT or UNITDATA request) identifies among the SAs available to it an SA whose attributes satisfy the following conditions:

- a) any locally derived security service requirements match the security services selected for the SA;
- b) the NLSP Called or Destination Address is contained within the set of NLSP addresses in Adr_Served;
- c) no NLSP connection is currently using this SA (NLSP-CO only).

The procedure to be followed if more than one SA satisfies these conditions is a local matter. If no such SA exists and if in-band SA establishment is supported, then the SA-P (SA protocol) option may be selected as defined in clauses 7 and 8. Otherwise, out-of-band SA establishment procedures may be followed. If neither of these procedures can be completed successfully within a locally defined timeout, then error recovery procedures appropriate to the mode of communications, as defined in 7.4 and 8.4, will be carried out.

6.4 Secure Data Transfer Protocol Functions**6.4.1 Generate****6.4.1.1 SDT PDU Based**

The following shall be performed as utilized in clauses 7 and 8:

- a) The Data Type Field bit 8 shall be set to the value of SA Attribute Initiator.
- b) If these procedures are invoked from 8.6 (NLSP-DATA), the Data Type Field bit 7 shall be set according to those procedures, otherwise this bit is set to a value indicating "last".
- c) The Data Type Field bits 1-6 shall be set to a value defined in 13.3.4.2 as appropriate to the procedures in clauses 7 and 8.
- d) Data relating to NLSP service parameters or other protocol exchanges (e.g. test data) are placed in the appropriate Content Fields (see 13.3.4.3) as required according to the procedures in clauses 7 and 8.
- e) If (Label is TRUE), and in the case of NLSP-CO this is the first SDT PDU sent on the current connection, then either:
 - 1) a security label, including the Defining Authority, shall be placed in a Label Content Field and included in the PDU; or

- 2) a security label reference shall be placed in a Label Reference Content Field and included in the PDU.

The label selected shall be one of the values in SA Attribute Label_Set.

NOTE 1 – In the case of NLSP CO if Protect_Connect_Params only the SDT PDU carrying NLSP CONNECT parameters will be labelled, else the first SDT PDU sent in either direction during the NLSP data transfer phase will be labelled.

- f) An Encapsulation function (for example, the one described in clause 11) shall be called with the following arguments being passed:
 - 1) SA-ID shall be set to My_SA-ID;
 - 2) unit-data-type shall be set to:
 - “expedited” if the data to be protected is from an NLSP-EXPEDITED-DATA primitive;
 - “normal”, otherwise;
 - 3) Octet-String-Before-Encapsulation shall be set to the constructed PDU fields.
- g) The Encapsulation function shall return either an error or an encapsulated-octet-string. Upon successful completion of the Encapsulate function, the unprotected header of the SDT PDU shall be created as defined in 13.3.2 with the encapsulated-octet-string appended to the header.

NOTE 2 – The SA-ID is not present in NLSP-CO.

6.4.1.2 No Header Present (NLSP-CO only)

The following shall be performed as utilised in clause 8:

- a) An Encapsulation function which does not alter the size of data (for example, the one described in clause 12) shall be called with the following arguments being passed:
 - 1) SA-ID shall be set to My_SA-ID;
 - 2) unit-data-type shall be set to:
 - “expedited” if the data to be protected is from an NLSP-EXPEDITED-DATA primitive;
 - “normal”, otherwise;
 - 3) Octet-String-Before-Encapsulation shall be set to the NLSP Userdata parameter.
- b) The Encapsulate function shall return either an error or an encapsulated-octet-string.

6.4.2 Check

6.4.2.1 SDT PDU Based

The following shall be performed as utilised in clauses 7 and 8:

- a) The Unprotected Header shall be discarded from the PDU.
- b) A Decapsulate function (for example, the one described in clause 11) shall be called with the following arguments being passed:
 - 1) SA-ID shall be set to My_SA-ID;
 - 2) unit-data-type shall be set to:
 - “expedited” if the data to be decapsulated is from an UN-EXPEDITED-DATA primitive;
 - “normal”, otherwise;
 - 3) encapsulated-octet-string shall be set to the remainder of the PDU.
- c) The Decapsulate function shall return either an error or an Octet-String-Before-Encapsulation. Upon successful completion of the Decapsulate function, the following processing shall be performed.
- d) The Data Type Field, bit 8 (Initiator to Responder) flag shall be checked to NOT equal the value of SA Attribute Initiator.
- e) The Data Type Field bit 1-6 and bit 7 will be checked to be a value appropriate for the procedures given in clauses 7 and 8.

- f) If (Label is TRUE), and in the case of NLSP-CO this is the first SDT PDU received on the current connection, then the PDU shall be checked to ensure that one and only one Label or Label Reference Content Field is present. If present, the value of the label shall be checked to ensure it is contained in the set Label_Set.
- g) Content Fields relating to NLSP service parameters or other protocol functions shall be checked to be present as required according to the procedures in clauses 7 and 8. The data is retrieved from these fields and handled according to the procedures in clauses 7 and 8.

6.4.2.2 No Header Present (NLSP-CO only)

The following shall be performed as utilised in clause 8:

- a) The Decapsulate function defined to be used for this SA (for example, the one described in clause 12) shall be called with the following arguments being passed:
 - 1) SA-ID shall be set to My_SA-ID;
 - 2) unit-data-type shall be set to:
 - “expedited” if the data to be decapsulated is from an UN-EXPEDITED-DATA primitive;
 - “normal”, otherwise;
 - 3) encapsulated-octet-string shall be set to the UN Userdata parameter.
- b) The Decapsulate function shall return either an error or an Octet-String-Before-Encapsulation.

6.5 Use of a Security Association Protocol

When two NLSPEs do not have an SA established, they may establish an SA by using a Security Association Protocol (SA-P) or some other method. An SA-P exchanges SA PDUs, or SDT PDU with content Data Type set to SA-P, between NLSPEs to establish, modify, or terminate an SA.

NLSP clauses 7 and 8 define how use of the SA-P might be invoked but no SA-P procedures. The procedures for the SA-P, and the PCI contained in the SA PDU/SDT PDU, depend on the specific mechanism used to provide the SA-P (a suitable protocol mechanism is defined in Annex C). Any SA-P shall provide the following features:

- a) derivation of all SA attributes required for the selected form of protection;
- b) keys that have come from an authenticated source;
- c) establishment of initial information for the purpose of authentication and integrity, if required.

An NLSPE shall discard SA PDUs if the specific SA-P is not supported.

An SA-P may be based on either symmetric or asymmetric algorithms. It is recommended that an asymmetric algorithm be used. Annex C contains an example of such a mechanism.

7 Protocol Functions for NLSP-CL

7.1 Services Provided by NLSP-CL

The services provided by NLSP will be referred to with the prefix “NLSP”. The primitives are:

<i>Primitives</i>	<i>Parameters</i>
NLSP-UNITDATA Request	NLSP Destination Address
Indication	NLSP Source Address
	NLSP Quality of Service
	NLSP Userdata

The service primitives and parameters are directly equivalent to those defined in CCITT Recommendation X.213 | ISO/IEC 8348.

7.2 Services Assumed

The service assumed by NLSP on its lower boundary will be referred to with the prefix "UN" (for "Underlying Network"). The primitives are:

<i>Primitives</i>	<i>Parameters</i>
UN-UNITDATA	Request
	Indication
	UN Called Address
	UN Calling Address
	UN Quality of Service
	UN Userdata

The service primitives and parameters assumed are the equivalent to those defined in the CLNS (see CCITT Recommendation X.213 | ISO 8348/AD1).

7.3 Security Association Attributes

The following attributes control the operation of NLSP-CL. Their description includes the mnemonics used to refer to these attributes in this Specification:

NOTE – Where an SA Attribute is "constrained by ASSR", this constraint may define a single value or a set of values. Where the ASSR defines a range of values, the attribute value may be established by OSI systems management, an SA-P exchange or by other means outside the scope of this Specification.

- Security services selected for the SA:

DOAuth: Integer of range constrained by ASSR Data Origin Authentication level.

The value of this attribute shall be pre-established or set up on SA establishment.

CLConf: Integer of range constrained by ASSR Connectionless confidentiality level.

The value of this attribute shall be pre-established or set up on SA establishment.

CLInt: Integer of range constrained by ASSR Connectionless integrity level.

The value of this attribute shall be pre-established or set up on SA establishment.

7.4 Checks

At many points in the following descriptions, the NLSP-CL entity checks that some condition is satisfied. Unless otherwise specified, whenever such a check fails, the NLSP-CL entity shall discard the data currently being processed. Optionally, the entity may also file an audit report. What failures are to be audited is considered to be a local matter.

7.5 In-Band SA Establishment

An SA may be established in band using a Security Association Protocol (SA-P). An SA-P is defined in Annex C of this Specification.

NOTE – Currently, the SA-P does not include any recovery procedures and therefore, care should be taken that the required reliability is provided when using this protocol with NLSP-CL.

7.6 Processing NLSP-UNITDATA Request

7.6.1 Initial Checks and Identification of SA

On receipt of an NLSP-UNITDATA request, the NLSPE checks if unprotected communications are allowed based on local security service requirements and the source/destination address pair. If unprotected communications are allowed, the NLSP service parameters are copied directly to the equivalent UN service parameters in a UN-UNITDATA request and no further action is taken by the NLSPE.

If protected communications are required the initial checks and identification of SA procedures as described in 6.3 shall be performed, followed by the procedures below:

7.6.2 Protection of NLSP-UNITDATA

The NLSPE shall perform the “generate SDT PDU functions” as defined in 6.4.1.1 with Data Type “NLSP-UNITDATA req/in” containing:

- a) if Param_Prot is TRUE, the source NLSP address;
- b) if Param_Prot is TRUE, the destination NLSP address;
- d) the NLSP Userdata parameter.

The Last/Not last flag shall be set to Last (i.e. bit 7 of the data type field = 0).

7.6.3 Network Request

The SDT PDU shall be passed to the next lower protocol as the UN Userdata parameter of a UN-UNITDATA Request.

If Param_Prot is TRUE the UN Source Address shall be the local NLSP entity UN-Address, else the NLSP Source Address shall be copied to the UN Source Address.

If Param_Prot is TRUE the UN Destination Address shall be Peer_Adr, else the NLSP Destination Address shall be copied to the UN Destination Address.

UN QOS shall be determined by local policy but may be copied from NLSP QOS.

NOTE – If record route and source route parameters are in NLSP QOS parameters and are not passed as UN QOS parameters, then the specified QOS may not be provided for the part of the route between source and destination NLSP-CL entities.

7.7 Processing UN-UNITDATA Indication

7.7.1 Initial Checks and Processing

If no SDT PDU is present the NLSPE checks if unprotected communications are allowed based on local security service requirements and the source/destination address pair. If unprotected communications are allowed, the UN service parameters are copied directly to the equivalent NLSP service parameters in a NLSP UNITDATA request and no further action is taken by the NLSPE. If unprotected communications are not allowed, then the procedures described in 7.4 are carried out. No further action is taken by the NLSPE.

If an SDT PDU is present the NLSPE shall identify among the SAs available to it an SA with My_SA-ID equal to the SA-ID Field in the received SDT-PDU. All further operations refer to this identified SA.

The NLSPE shall perform the common processing as defined in 6.4.2.1. In addition, the following checks shall be carried out:

- a) If the Data Type field is “not related to any NLSP service primitive” then the SDT PDU shall not be processed any further under these procedures. Otherwise the Data Type field shall be checked to be NLSP-UNITDATA.

NOTES

- 1 The value of the “Last/Not last flag” (i.e. bit 7 of the data type field) can be ignored.
- 2 Support for Traffic Padding or Test exchanges in Connectionless mode is outside the scope of NLSP.

- b) If Param_Prot is TRUE the SDT PDU shall be checked to ensure that the following fields are present:
 - 1) Destination Address;
 - 2) Source Address.

An NLSP UNITDATA indication shall be passed to the NLSP User with parameters set and address checked as defined in 7.7.2.

7.7.2 Parameters of the NLSP-CL Indication

7.7.2.1 Address Parameters

If Param_Prot is TRUE then the NLSPE shall set the NLSP service parameters to the values contained in the SDT PDU.

If Param_Prot is FALSE then the values shall be taken from the UN Indication parameters as follows:

- a) the NLSP Source Address = UN Source Address; and
- b) the NLSP Destination Address = UN Destination Address.

The NLSP Destination Address, set as described above, shall be checked to be an NLSP Address served by this NLSP entity as determined by the local security policy.

The NLSP Source Address, set as described above, shall be checked to be an NLSP Address contained in SA Attribute Adr_Served.

7.7.2.2 QOS

QOS parameters are copied from the UN service to the NLSP service.

7.7.2.3 Userdata

The data in the Userdata field from the Octet-String-Before-Encapsulation of the SDT PDU shall be passed to the NLSP user in the NLSP-Userdata parameter of the NLSP-UNITDATA indication.

8 Protocol Functions for NLSP-CO

8.1 Services Provided by NLSP-CO

The primitives of the services provide by NLSP-CO are:

<i>Primitives</i>		<i>Parameters</i>
NLSP-CONNECT	Request Indication	NLSP Called Address NLSP Calling Address NLSP Receipt Confirmation Selection NLSP Expedited Data Selection NLSP QOS Parameter Set NLSP Userdata
NLSP-CONNECT	Response Confirm	NLSP Responding Address NLSP Receipt Confirmation Selection NLSP Expedited Data Selection NLSP QOS Parameter Set NLSP Userdata
NLSP-DATA	Request Indication	NLSP Userdata NLSP Confirmation Request
NLSP-DATA-ACKNOWLEDGE	Request Indication	
NLSP-EXPEDITED DATA	Request Indication	NLSP Userdata
NLSP-RESET	Request Indication	NLSP Reason NLSP Originator NLSP Reason
NLSP-RESET	Response Confirmation	
NLSP-DISCONNECT	Request Indication	NLSP Originator NLSP Reason NLSP Userdata NLSP Responding Address

NOTE – Originator does not apply to Request.

The service primitives and parameters are directly equivalent to those defined in CCITT Recommendation X.213 | ISO 8348.

8.2 Services Assumed

The service assumed by NLSP on its lower boundary will be referred to with the prefix "UN" (for "Underlying Network"). This is a notional interface (see 5.1).

The UN Interface is modelled in two parts:

- a definition of the UN service primitives and parameters (see below);
- a mapping from the UN service (see 5.1) either onto a standard Network service or directly onto ISO/IEC 8208/CCITT Rec. X.25.

Annexes A and B define the mapping from the notional service interface to the Network service and to ISO/IEC 8208 or X.25.

The UN primitives assumed for NLSP-CO are:

<i>Primitives</i>		<i>Parameters</i>
UN-CONNECT	Request	UN Called Address
	Indication	UN Calling Address UN Receipt Confirmation Selection UN Expedited Data Selection UN QOS Parameter Set UN Userdata UN Authentication ¹⁾
UN-CONNECT	Response	UN Responding Address
	Confirm	UN Receipt Confirmation Selection UN Expedited Data Selection UN QOS Parameter Set UN Userdata UN Authentication ¹⁾
UN-DATA	Request	UN Userdata
	Indication	UN Confirmation Request
UN-DATA-ACKNOWLEDGE	Request	
	Indication	
UN-EXPEDITED-DATA	Request	UN Userdata
	Indication	
UN-RESET	Request	UN Reason
	Indication	UN Originator UN Reason
UN-RESET	Response	
	Confirm	
UN-DISCONNECT	Request	UN Reason UN Userdata UN Responding Address
	Indication	UN Originator UN Reason UN Userdata UN Responding Address

Annexes A and B define the mapping of UN Authentication onto CCITT Recommendation X.213 | ISO/IEC 8348 and onto ISO/IEC 8208 or X.25.

¹⁾ The UN Authentication parameter is used to convey the CSC PDU. This enables an efficient encoding when NLSP is used in conjunction with ISO/IEC 8208 or X.25 where the UN Authentication parameter can be conveyed by the DTE Protection Facility field (see Annex B).

NOTE – When NLSP is used closely coupled with ISO/IEC 8208 | CCITT Recommendation X.25 it may be able to use alternative encodings which take full advantage of the underlying protocol whereas the variant mapping onto CCITT Recommendation X.213 | ISO/IEC 8348 assumes only the use of an underlying Network service.

8.3 Security Association Attributes

The following attributes control the operation of NLSP-CO. Their description includes the mnemonics used to refer to these attributes in this Specification:

NOTE 1 – Where an SA Attribute is “constrained by ASSR”, this constraint may define a single value or a set of values. Where the ASSR defines a range of values, the attribute value may be established by OSI systems management, an SA-P exchange or by other means outside the scope of this Specification.

a) *Security services selected for the SA:*

PE Auth: Integer of range constrained by ASSR
Peer entity authentication level.

CO Conf: Integer of range constrained by ASSR
Connection confidentiality level.

CO Int: Integer of range constrained by ASSR
Connection integrity without recovery.

The values of these attributes shall be pre-established or set up on SA establishment.

b) *CO protocol related attributes:*

Retain_On_Disconnect: Boolean

Whether the SA Attributes are to be retained in disconnection.

The value of this attribute shall be set up on SA establishment or pre-established.

Protect_Connect_Params: Boolean

Protect NLSP Userdata in NLSP-CONNECT and NLSP-DISCONNECT, as well as other service parameters in NLSP-CONNECT and NLSP-DISCONNECT if Param_Prot is also TRUE.

The value of this attribute shall be constrained by the ASSR.

NOTE 2 – Param_Prot cannot be TRUE if Protect_Connect_Params is FALSE.

No_Header: Boolean

If true the No_Header based protection is to be used to protect data (e.g. using the procedures defined in clause 12).

The value of this attribute shall be constrained by the ASSR.

8.4 Checks and other Common Functions

At many points in the following descriptions, it is stated that some condition is satisfied. Unless otherwise specified, whenever such a check fails during the NLSP-Connect or NLSP-Disconnect procedures, UN-DISCONNECT request and NLSP-DISCONNECT indication shall be issued as appropriate. If this occurs following connection establishment the NLSPE shall discard the data currently being processed and, as a local decision, shall invoke either:

- an NLSP initiated UN-RESET procedures as defined in 8.8.5;
- a UN-DISCONNECT request and NLSP-DISCONNECT indication.

Optionally the entity may also file an audit report. It is a local matter to decide what audit information is to be recorded.

Similarly, an expected sequence of events is given in the procedures described below. If this sequence is not followed then an unexpected event shall be treated in the same way as a check failing.

Where the following descriptions refer to the generation or checking of CSC PDUs, or Secure Data Transfer PDUs, appropriate mechanism specific procedures, e.g. those described in clauses 9 to 12 of this Specification, shall be carried out.

8.5 NLSP-Connect Functions

8.5.1 Initial Procedures

8.5.1.1 Initial Checks – NLSP CONNECT Request

On receipt of an NLSP-CONNECT request, the NLSPE shall check if unprotected communications are allowed based on local security service requirements and the calling/called address pair. If unprotected communications are allowed, the NLSP and UN service parameters are copied directly to the equivalent UN and NLSP service parameters for all subsequent NLSP and UN service primitives until after receipt of a UN-DISCONNECT indication. No further action is taken by the NLSPE for the duration of the connection.

If protected communications are required, the NLSPE shall follow the procedures for initial checks and identification of the security association as described in 6.3.1 and 6.3.2, respectively. This is followed by the procedures defined in 8.5.2, 8.5.3 or 8.5.4. The appropriate procedures depend on the connection establishment mode selected as defined in 8.5.1.2. The same subclause is then used for subsequent UN-CONNECT and NLSP-CONNECT service primitive for that UN connection.

8.5.1.2 NLSP Connection Establishment Mode

If an SA currently exists with the required characteristics, then this may be used to protect the connection. Otherwise, a new SA shall be established, in-band as part of the NLSP-CONNECT functions or out-of-band within a given timeout. If neither of these can be carried out, an NLSP-DISCONNECT shall be returned.

There are two basic modes for the establishment of an NLSP connection with variations to support in band SA establishment as follows:

- a) **NLSP-CONNECT in UN-CONNECT**, in which the protocol exchanges to provide authentication and exchange NLSP-CONNECT parameters are carried in the UN-CONNECT parameters;
- b) **NLSP-CONNECT in UN-CONNECT with SA-P**, in which in-band SA establishment is carried in UN-DATA on a pre-connection before establishing a second UN connection with the authentication and NLSP-CONNECT parameters carried in the UN-CONNECT as in a) above;
- c) **NLSP-CONNECT in UN-DATA**, in which an authentication exchange is carried in the UN-CONNECT followed by exchange of NLSP-CONNECT parameters in UN-DATA;
- d) **NLSP-CONNECT in UN-DATA with SA-P**, in which a SA-P exchange is carried in UN-DATA followed by exchange of NLSP-CONNECT parameters in UN-DATA.

The selection of the most appropriate mode is a local decision made by the calling NLSPE based on the requirements (or expected requirements) for NLSP connection establishment and the profiling environment in which NLSP operates.

The selection of a SA-P is indicated by the SA-P flag in the CSC PDU. The selection of NLSP-CONNECT in UN-CONNECT or NLSP-CONNECT in UN-DATA is indicated to the remote NLSPE by the UNC-UND flag (see Table 8-2).

In the two latter modes (NLSP-CONNECT in UN-DATA with or without SA-P) the NLSP-CONNECT parameters are encoded in an SDT-PDU and hence these modes cannot be used in No_Header mode.

In the first two modes (NLSP-CONNECT in UN-CONNECT with or without SA-P) the NLSP-CONNECT parameters will be protected in an SDT PDU if No_Header is FALSE and Protect_Connect_Params is TRUE. However, these modes cannot be used if the resultant SDT PDU is greater than the space available in the UN-CONNECT UN Userdata.

Table 8-1 indicates the limitations on the various modes of connection establishment as defined above. This can be used to determine which procedures for call set up are appropriate for a given profile:

Table 8-1 – Table Giving Limitations for NLSP Connection Establishment Mode

SAP	No_Header	Protect_Connect_Params	SDT PDU Length Limits (See Notes)	Mode	Connection Set-up Procedures
TRUE	TRUE	EITHER		NLSP-CONNECT in UN-CONNECT with SA-P	8.5.3 followed by 8.5.2.2 to 8.5.2.4
	FALSE	TRUE	SDT <= max UN Userdata	NLSP-CONNECT in UN-CONNECT with SA-P	8.5.3 followed by 8.5.2.2 to 8.5.2.4
TRUE	FALSE	FALSE		NLSP-CONNECT in UN-CONNECT with SA-P	8.5.3 followed by 8.5.2.2 to 8.5.2.4
TRUE	FALSE	EITHER		NLSP-CONNECT in UN-DATA with SA-P	8.5.4
FALSE	TRUE	EITHER		NLSP-CONNECT in UN-CONNECT	8.5.2
FALSE	FALSE	TRUE	SDT <= max UN Userdata	NLSP-CONNECT in UN-CONNECT	8.5.2
FALSE	FALSE	FALSE		NLSP-CONNECT in UN-CONNECT	8.5.2
FALSE	FALSE	EITHER		NLSP-CONNECT in UN-DATA	8.5.4

EITHER Under Protect_Connect_Params is used to denote that this may be either TRUE or FALSE.

NOTES

- SDT refers to the maximum possible length of the SDT PDU that may be generated during connection establishment for the profile environment in which NLSP is operating.
- It is assumed that the same limits apply to the length of NLSP Userdata as for UN Userdata.
- For UN mapping to CCITT Recommendation X.213 | ISO 8348 "max UN Userdata" is the maximum Userdata that can be carried in the network service N-CONNECT service primitives (e.g. 128 for CCITT Recommendations X.223 | ISO 8878 and X.25 | ISO 8208) less the length of the CSC PDU.
- For UN mapping directly to ISO 8208 | X.25 "max UN Userdata" is 128.

8.5.1.3 Initial Checks – UN-CONNECT Indication

On receipt of a UN-CONNECT indication with no CSC PDU present in the UN Authentication parameter, the NLSPE shall check if unprotected communications are allowed based on local security service requirements and the calling/called address pair. If unprotected communications are allowed, the NLSP and UN service parameters are copied directly to the equivalent UN and NLSP service parameters for all subsequent NLSP and UN service primitives until after a receipt of UN-DISCONNECT indication. No further action is taken by the NLSPE for the duration of the connection.

If unprotected communications are not allowed and no CSC PDU is present, then the procedures defined in 8.4 for check failure are carried out.

If a CSC PDU is present, then the procedures defined in 8.5.2, 8.5.3 or 8.5.4 are carried out depending on the value of the SA-P and UNC-UND flags in the PDU Type field as given in the Table 8-2. The SA-P flag indicates being set.

indicates that in band SA-P exchanges are to be carried by NLSP. The UNC-UND flag being set indicates that the NLSP-CONNECT is to be carried in UN-DATA instead of UN-CONNECT. The same subclause is then used for subsequent UN-CONNECT and NLSP-CONNECT service primitives for that UN connection.

Table 8-2 – CSC PDU Flags Identifying NLSP Connection Set Up Procedures

UNC-UND Flag	SA-P Flag	NLSP Connection Set Up Procedures
Set	Set	8.5.4 (NLSP-CONNECT in UN-DATA)
Set	Clear	8.5.4 (NLSP-CONNECT in UN-DATA)
Clear	Set	8.5.3 (NLSP-CONNECT in UN-CONNECT with SA-P)
Clear	Clear	8.5.2 (NLSP-CONNECT in UN-CONNECT)

8.5.2 NLSP-CONNECT in UN-CONNECT

The expected sequence of events for NLSP connection establishment with the NLSP-CONNECT parameters in UN-CONNECT is illustrated in Figure 8-1.

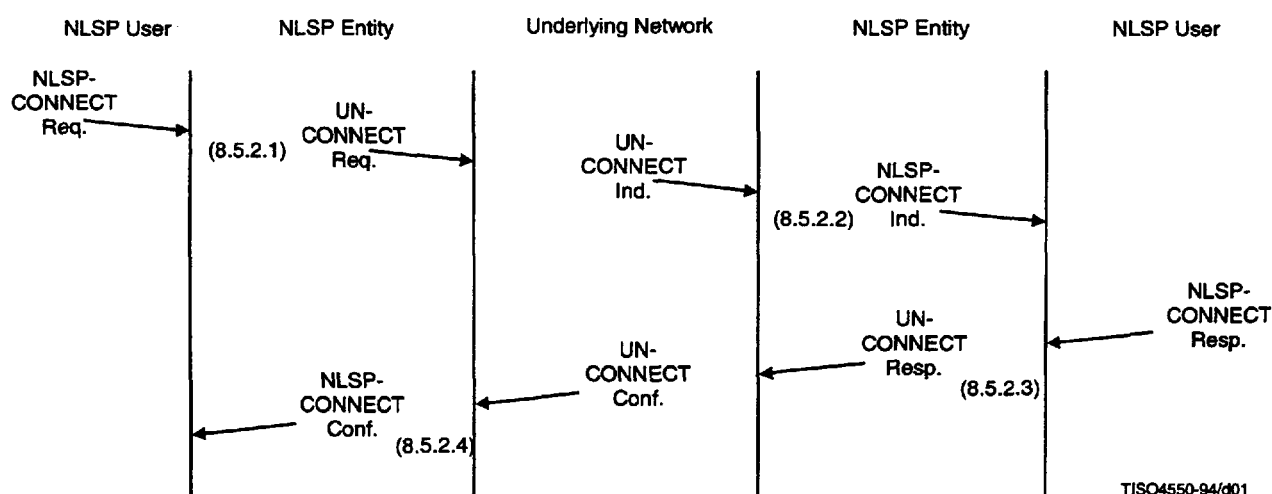


Figure 8-1 – Service Primitive Time Sequence Diagram for NLSP-CONNECT in UN-CONNECT

8.5.2.1 NLSP-CONNECT Request

On an NLSP-CONNECT request if the NLSP-CONNECT parameters are to be carried in UN-CONNECT, the following procedure shall be carried out:

- If Protect_Connect_Params is TRUE and No_Header is TRUE, then any NLSP Userdata shall be encapsulated as described in 6.4.1.2. This is placed in UN-Userdata.
- If Protect_Connect_Params is TRUE, No_Header is FALSE and Param_Prot is TRUE, then a SDT PDU is generated containing the NLSP Called Address, NLSP Calling Address, and NLSP Userdata as described in 6.4.1.1 with Data Type "NLSP-CONNECT req/ind". This is placed in UN-Userdata.

- c) If Protect_Connect_Params is TRUE, No_Header is FALSE and Param_Prot is FALSE, then a SDT PDU is generated containing NLSP Userdata, if any is present, as described in 6.4.1.1 with Data Type "NLSP-CONNECT req/ind". This is placed in UN-Userdata.
- d) If Protect_Connect_Params is FALSE, then the NLSP Userdata is placed in UN-Userdata.
- e) A CSC PDU is prepared with:
 - 1) UNC-UND flag clear;
 - 2) the SA-ID of the current SA is placed in the SA-ID field;
 - 3) the SA-P flag is cleared;
 - 4) the CSC content is set to the CSC first exchange as required for the mechanism specific procedures such as those described in 10.3.
- f) A UN-CONNECT request shall be invoked with:
 - 1) if Param_Prot the UN Called Address is set to Peer_Adr, else NLSP Called Address;
 - 2) if Param_Prot the UN Calling Address set to the local NLSPE UN-address, else NLSP Calling Address;
 - 3) UN Receipt Confirmation Selection and Expedited Data Selection set to the values determined locally from NLSP Receipt Confirmation Selection and Expedited Data Selection;
 - 4) UN QOS parameter set to a value determined locally from the NLSP QOS parameter;
 - 5) UN-Userdata set as described in a) to d) above;
 - 6) UN Authentication set to CSC PDU as described in e) above.
- g) The Calling NLSPE awaits a UN-CONNECT confirm as described in 8.5.2.4 or a UN-DISCONNECT indication as described in 8.10.

8.5.2.2 UN-CONNECT Indication – UNC-UND Clear and SA-P Clear

On receipt of a UN-CONNECT indication with UN Authentication containing an CSC PDU with the UNC-UND flag clear and the SA-P flag clear:

- a) The NLSPE shall identify among the SAs available to it an SA with My_SA-ID equal to the SA-ID field in the received CSC PDU. All further operations refer to this identified SA.
- b) The CSC PDU content shall be checked as required for the mechanism specific procedures such as those described in 10.3. The response CSC PDU content returned shall be held for use in processing the NLSP-CONNECT response as described in 8.5.2.3.
- c) If Protect_Connect_Params is TRUE and No_Header is TRUE, then any UN-Userdata shall be decapsulated as described in 6.4.2.2. This is placed in NLSP-Userdata. Other NLSP-CONNECT indication parameters are copied from the UN-CONNECT indication parameters.
- d) If Protect_Connect_Params is TRUE, No_Header is FALSE and Param_Prot is TRUE, then the SDT PDU in UN-Userdata is checked as in 6.4.2.1. The Data Type field shall be checked to be NLSP-CONNECT req/ind. The NLSP Called Address, NLSP Calling Address, and NLSP Userdata Content Fields in the SDT PDU shall be placed in the NLSP-CONNECT indication parameters. The UN Receipt Confirmation Selection and Expedited Data Selection, as well as the UN QOS parameter set shall be copied into the equivalent NLSP-CONNECT indication parameters.
- e) If Protect_Connect_Params is TRUE, No_Header is FALSE and Param_Prot is FALSE, then, if present, the SDT PDU in UN-Userdata is checked as in 6.4.2.1. The Data Type field shall be checked to be NLSP-CONNECT req/ind. The Userdata Content field in the SDT-PDU shall be placed in NLSP-Userdata. Other NLSP-CONNECT indication parameters shall be copied from the UN-CONNECT indication parameters.
- f) If Protect_Connect_Params is FALSE, then all the UN-CONNECT indication parameters are copied into the NLSP-CONNECT indication parameters.
- g) The NLSP Called Address, set as described above, shall be checked to be an NLSP Address served by this NLSP entity as determined locally.
- h) The NLSP Calling Address, set as described above, shall be checked to be an NLSP Address in SA Attribute Adr_Served.

- i) If any security label is established for the connection, this shall be checked against the set of labels authorized in SA Attribute Label_Set
- j) The NLSP-CONNECT indication shall be passed to the NLSP user.
NOTE – NLSP Receipt Confirmation Selection, Expedited Data Selection and NLSP QOS parameter set can be modified to a locally determined value before being passed to the NLSP user.
- k) The called NLSPE awaits an NLSP-CONNECT response as described in 8.5.2.3 or a NLSP-DISCONNECT request or UN-DISCONNECT indication as described in 8.10.

8.5.2.3 NLSP-CONNECT Response

On receipt of a NLSP-CONNECT response:

- a) If Protect_Connect_Params is TRUE and No_Header is TRUE, then any NLSP Userdata shall be encapsulated as described in 6.4.1.2. This is placed in UN-Userdata.
- b) If Protect_Connect_Params is TRUE, No_Header is FALSE and Param_Prot is TRUE, then a SDT PDU is generated containing NLSP Responding Address, and NLSP Userdata as described in 6.4.1.1 with Data Type "NLSP-CONNECT res/conf". This is placed in UN-Userdata.
- c) If Protect_Connect_Params is TRUE, No_Header is FALSE, Param_Prot is FALSE and NLSP Userdata is present, then a SDT PDU is generated containing NLSP Userdata as described in 6.4.1.1 with Data Type "NLSP-CONNECT res/conf". This is placed in UN-Userdata.
- d) If Protect_Connect_Params is FALSE, then the NLSP Userdata is placed in UN-Userdata.
- e) If it is not possible to fit the data generated in a) to d) above in the UN-Userdata, then these procedures shall be aborted as defined in 8.4.
- f) A CSC PDU shall be generated with:
 - 1) the SA-P and UNC-UND flags clear;
 - 2) the SA-ID to the SA-ID as in the CSC PDU received in the UN-CONNECT indication;
 - 3) the CSC content set to the value returned from the earlier invocation of the mechanism specific procedures in 8.5.2.2, b).
- g) A UN-CONNECT response shall be sent with:
 - 1) UN Responding Address if Param_Prot is TRUE set to the local NLSP entity UN-Address else to NLSP Responding Address parameter;
 - 2) UN Receipt Confirmation Selection and Expedited Data Selection set to the values determined locally from NLSP Receipt Confirmation Selection and Expedited Data Selection;
 - 3) UN QOS parameter set to the values determined locally from NLSP QOS parameter;
 - 4) UN-Userdata as described in a) to d) above;
 - 5) UN Authentication set to CSC PDU as described in g) above.
- h) If required under the mechanism specific procedures for authentication and CSC exchange (such as those described in 10.3), the called NLSPE may await an SDT PDU in UN-DATA before it completes establishment of the NLSP connection and processes NLSP-DATA primitives from the NLSP User. Otherwise, the Called NLSPE has now completed its NLSP connection establishment procedures and can enter the data transfer phase.

NOTE – If the CSC exchange mechanism requires the exchange of more than two CSC-PDUs, then these are exchanged in UN-DATA before the connection establishment is complete.

8.5.2.4 UN-CONNECT Confirm – UNC-UND Clear and SA-P Clear

On receipt of a UN-CONNECT confirmation with UN Authentication containing a CSC PDU with both the UNC-UND and SA-P flags clear:

- a) The CSC PDU content is checked using the mechanism specific procedures such as those described in 10.3.
- b) If Protect_Connect_Params is TRUE and No_Header is TRUE, then any UN-Userdata shall be decapsulated as described in 6.4.2.2. This is placed in NLSP-Userdata. Other NLSP-CONNECT confirm. parameters are copied from the UN-CONNECT confirm parameters.

- c) If Protect_Connect_Params is TRUE, No_Header is FALSE and Param_Prot is TRUE, then the SDT PDU in UN-Userdata is checked as in 6.4.2.1. The Data Type field shall be checked to be NLSP-CONNECT res/conf. The NLSP Responding Address, and NLSP Userdata content fields in the SDT PDU shall be placed in the NLSP-CONNECT confirm parameters. The UN Receipt Confirmation Selection and Expedited Data Selection parameters as well as UN QOS parameters set shall be copied to the NLSP-CONNECT confirm parameters.
- d) If Protect_Connect_Params is TRUE, No_Header is FALSE and Param_Prot is FALSE, then, if present, the SDT PDU in UN-Userdata is checked as in 6.4.2.1. The Data Type field shall be checked to be NLSP-CONNECT res/conf. The Userdata content field in the SDT-PDU shall be placed in NLSP-Userdata. Other NLSP-CONNECT confirm parameters shall be copied from the UN-CONNECT confirm parameters.
- e) If Protect_Connect_Params is FALSE, then all the UN-CONNECT confirm parameters shall be copied into the NLSP-CONNECT confirm parameters.
- f) If present the NLSP Responding Address shall be checked to an NLSP Address contained in SA Attribute Adr_Served.
- g) The NLSP Connect confirm shall be passed to the NLSP user.
- h) If required under the mechanism specific procedures for authentication and CSC exchange (such as those described in 10.3), a SDT PDU may be created as described in 6.4.1.1 with Data Type "not related to any NLSP service primitive" containing no Content fields other than those required under clause 6. This shall be sent in UN-Userdata of a UN-DATA primitive.

NOTE – If the CSC exchange mechanism requires the exchange of more than two CSC-PDUs, then these are exchanged in UN-DATA before the connection establishment is complete.

The NLSP connection establishment procedures are now complete.

8.5.3 NLSP-CONNECT in UN-CONNECT with SA-P

The expected sequence of events is illustrated in Figure 8-2.

8.5.3.1 NLSP-CONNECT Request

On an NLSP-CONNECT request if the NLSP-CONNECT is to be carried in UN-CONNECT and in-band SA establishment is selected, the following procedure shall be carried out:

- a) A CSC PDU shall be prepared with:
 - 1) UNC-UND flag clear;
 - 2) the SA-P flag is set and SA-ID, Content Length and CSC PDU content are not present.
- b) A UN-CONNECT request shall be sent with:
 - 1) UN Called Address set to Peer_Adr;
 - 2) UN Calling Address set to the local NLSP entity UN-Address;
 - 3) UN Receipt Confirmation Selection set to a value determined locally;
 - 4) UN Expedited Data Selection is set to a value determined locally;
 - 5) UN QOS parameter set to value a value determined locally;
 - 6) UN-Userdata empty;
 - 7) UN Authentication to the CSC PDU.
- c) The Calling NLSPE shall await a UN-CONNECT confirm as described in 8.5.3.3 or a UN-DISCONNECT indication as described in 8.10.