INTERNATIONAL STANDARD

ISO/IEC 11577

First edition
1995-05-15

Information technology — Open Systems Interconnection — Network layer security protocol

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



Reference number
ISO/IEC 11577:1995(E)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

CONTENTS

		Page
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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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).

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

this ITU-T Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and Standards listed below. Members of IEC and ISO maintain a registry of currently valid International Standards. The Telecommunications Standardization Bureau of ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

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

2.2 Paired Recommendations | International Standards equivalent in technical content

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

  ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model.*
- CCITT Recommendation X.209 (1988), *Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1).*

  ISO/IEC 8825:1990, *Information technology – Open Systems Interconnection – Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1).*
- ITU-T Recommendation X.210 (1993), *Information technology – Open Systems Interconnection – Conventions for the definition of OSI services.*

  ISO/IEC 10731:1994, *Information technology – Open Systems Interconnection – Basic Reference Model – Conventions for the definition of OSI services.*
- CCITT Recommendation X.223 (1988), *Use of X.25 to provide the OSI connection-mode network service.*

  ISO/IEC 8878:1992, *Information technology – Telecommunications and information exchange between systems – Use of X.25 to provide the OSI connection-mode network service.*
- CCITT Recommendation X.290 (1992), *OSI conformance testing methodology and framework for protocol Recommendations for CCITT applications – General concepts.*

  ISO/IEC 9646-1:1994, *Information technology – Open Systems Interconnection – Conformation testing methodology and framework – Part 1: General concepts.*
- CCITT Recommendation X.291 (1992), *OSI conformance testing methodology and framework for protocol Recommendations for CCITT applications – Abstract test suite specification.*

  ISO/IEC 9646-2:1994, *Information technology – Open Systems Interconnection – Conformance testing methodology and framework – Part 2: Abstract test suite specification.*
- CCITT Recommendation X.509 (1988), *Information technology – Open Systems Interconnection – The Directory: Authentication framework.*

  ISO/IEC 9594-8:1990, *Information technology – Open Systems Interconnection – The Directory – Part 8: Authentication framework.*
- CCITT Recommendation X.800 (1991), *Security architecture for Open Systems Interconnection for CCITT applications.*

  ISO 7498-2:1989, *Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture.*

---

[1] To be published.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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;

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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)

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

b) *Protection of NLSP Userdata*

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

This mode is selected by SA Attribute Param_Prot being FALSE.

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

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

2) NLSP Userdata in NLSP DATA is protected.

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

c) *No Protection*

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

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

5.5.2 Quality of Protection

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

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

5.5.3 Data Protection Functions

5.5.3.1 SDT PDU Based

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

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

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

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

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

- traffic flow confidentiality;
- integrity and data origin authentication;
- confidentiality,

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

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

5.5.3.2 No Header (NLSP-CO only)

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

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

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:

a) establish mechanism specific security attributes for use in protecting the connection (for example, keys, integrity sequence numbers);

b) perform peer entity authentication.

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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 ** 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 ** 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).

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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:

Primitives		*Parameters*
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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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:

Primitives		*Parameters*
UN-UNITDATA	Request	UN Called Address
	Indication	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:

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

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:

Primitives		*Parameters*
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 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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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) a definition of the UN service primitives and parameters (see below);

b) 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:

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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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:

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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

1 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.

2 It is assumed that the same limits apply to the length of NLSP Userdata as for UN Userdata.

3 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.

4 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

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

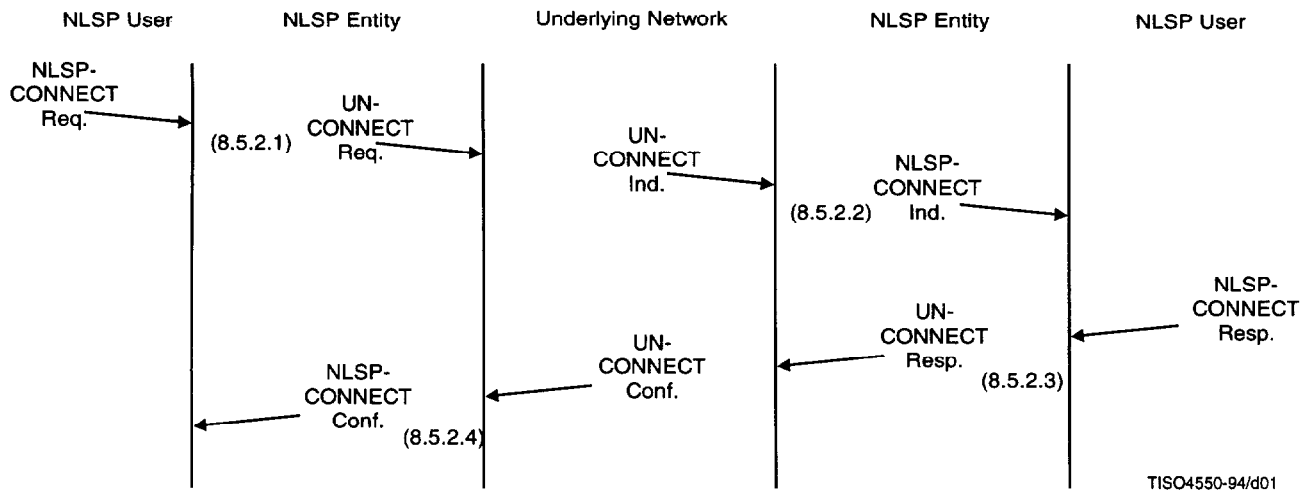


Figure 8-1 – Service Primitive Time Sequence Diagram for NLSP-CONNECT in UN-CONNECT

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:

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 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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

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.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

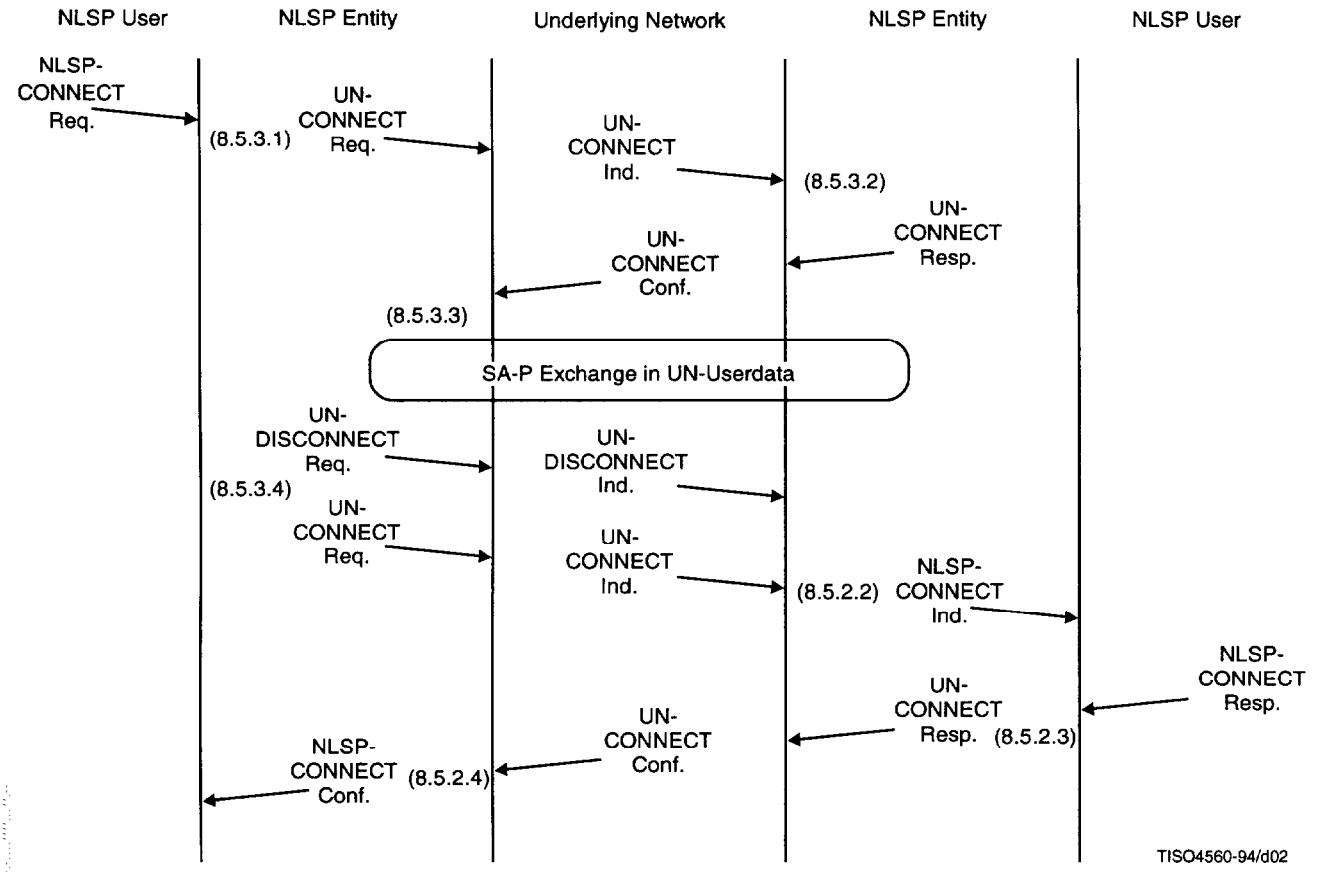


Figure 8-2 – Service Primitive Time Sequence Diagram for NLSP-CONNECT in UN-CONNECT with SA-P

8.5.3.2 UN-CONNECT Indication – UNC-UND clear and SA-P set

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

a) The NLSP shall prepare a CSC PDU with:

   1) UNC-UND flag clear;

   2) the SA-P flag set;

   4) the CSC content empty.

b) The NLSPE shall then respond with a UN-CONNECT response with:

   1) UN Responding address set to the local UN-Address;

   2) UN Receipt Confirmation Selection and Expedited Data Selection set to values determined locally from the parameters in the UN-CONNECT indication;

   3) UN QOS parameter set to a value determined locally from the UN QOS parameter in the UN-CONNECT indication;

   4) UN-Userdata empty;

   5) UN Authentication set to the CSC PDU.

The Called NLSPE shall await a SA-P exchange or a UN-DISCONNECT indication as described in 8.10. Any error in the SA-P shall be treated as an error as described in 8.4.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.5.3.3 UN-CONNECT Confirm – UNC-UND clear and SA-P set

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

a) the in-band SA-P shall be carried out;

b) the calling NLSPE awaits SA-P completion as described in 8.5.3.4 or a UN-DISCONNECT as described in 8.10.

8.5.3.4 SA-P Completion

On completion of the SA-P as described in 8.5.3.3, the Calling NLSPE shall carry out the following procedures:

a) A UN-DISCONNECT request shall be sent by the calling NLSPE with reason set to "disconnect-normal-condition", followed by a UN-CONNECT request with the service parameters set as follows.

b) 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.

c) 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.

d) 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.

e) If Protect_Connect_Params is FALSE, then the NLSP Userdata is placed in UN-Userdata.

f) 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.

g) 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 NLSP entity 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.

h) 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.

On completion of the SA-P the NLSP awaits a UN-DISCONNECT with reason set to "disconnect-normal-condition". On this UN-DISCONNECT indication, the called NLSPE then awaits a UN-CONNECT indication as described in 8.5.2.2.

The calling and called NLSPE shall then process subsequent NLSP and UN-CONNECT primitives as described in 8.5.2.2 to 8.5.2.4.

8.5.4 NLSP-CONNECT in UN-Data

The expected sequence of events is illustrated in Figure 8-3.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

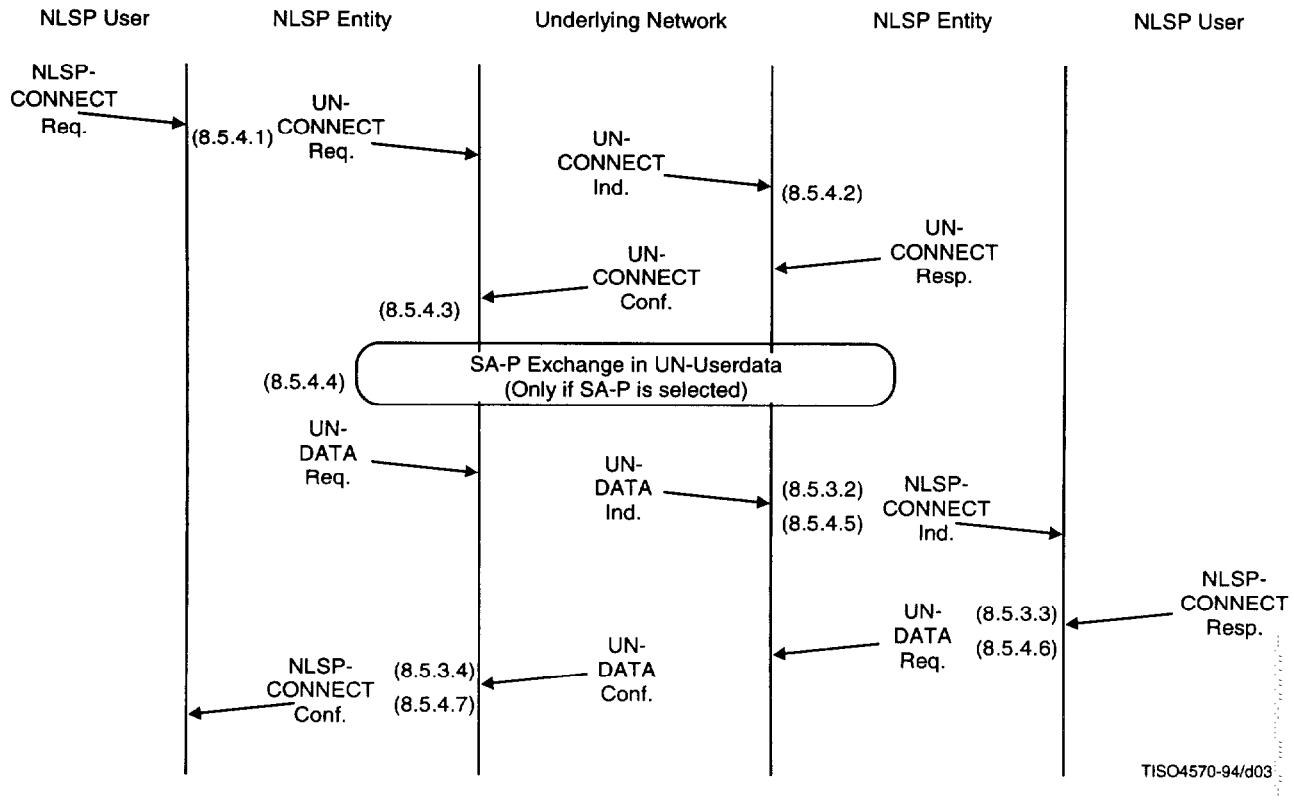


Figure 8-3 – Service Primitive Time Sequence Diagram for NLSP-CONNECT in UN-DATA

8.5.4.1 NLSP-CONNECT Request

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

a) A CSC PDU shall be prepared with:

1) UNC-UND flag set;

2) if in-band SA-P is selected, then the SA-P flag is set and SA-ID, Content Length and CSC PDU content fields are not present;

3) if in-band SA-P is not selected, then SA-P flag is clear, the SA-ID is set to Your_SA-ID and the CSC PDU content is set to the CSC first exchange as required for the mechanism specific procedures such as described in 10.3.

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 is set to a value determined locally from the NLSP Receipt Confirmation;

4) UN Expedited Data Selection is set to a value determined locally from the NLSP Expedited Data Selection;

5) UN QOS parameter set to value determined locally from the NLSP QOS;

6) UN-Userdata empty;

7) UN Authentication to the CSC PDU.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

c) The Calling NLSPE shall await a UN-CONNECT confirm as described in 8.5.4.3 or a UN-DISCONNECT indication as described in 8.10.

8.5.4.2 UN-CONNECT Indication – UNC-UND set

On receipt of a UN-CONNECT indication with UN Authentication containing a CSC PDU with the UNC-UND flag set:

a) if the SA-P flag is clear, then:

1) 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;

2) the CSC PDU content shall be checked as required for the mechanism specific procedures such as those described in 10.3.

If the SA-P flag is set or clear, the following procedures in this subclause are carried out.

b) The NLSPE shall then prepare a CSC PDU with:

1) UNC-UND flag set;

2) if in-band SA-P is selected then the SA-ID field shall be absent, else it shall be set to the SA-ID received in the CSC PDU;

3) if in-band SA-P is selected, then SA-P flag is set, else it is cleared;

4) if in-band SA-P is selected the CSC PDU content and Content length fields are not present, else the CSC PDU content is set to the CSC exchange as returned from the mechanism specific procedures such those defined 10.3.

NOTE – The current procedures do not cater for CSC exchange mechanisms requiring more than a two-way exchange of CSC PDUs optionally followed by an SDT-PDU.

c) The NLSPE shall then respond with a UN-CONNECT response with:

1) UN Responding address set to the local UN-Address;

2) UN Receipt Confirmation Selection and Expedited Data Selection set to values determined locally from the parameters in the UN-CONNECT indication;

3) UN QOS parameter set to a value determined locally from the UN QOS parameter in the UN-CONNECT indication;

4) UN-Userdata empty;

5) UN Authentication set to the CSC PDU.

d) The Called NLSPE shall await a SA-P exchange or UN-DATA indication containing an SDT PDU as described in 8.5.4.5 or a UN-DISCONNECT indication as described in 8.10 or a UN-RESET as described in 8.9.

8.5.4.3 UN-CONNECT Confirm – UNC-UND set

On receipt of a UN-CONNECT confirm with UN-Authentication containing a response CSC PDU with the UNC-UND flag set:

a) The SA-P flag in the CSC PDU is checked to match the selection of in-band SA-P.

b) If SA-P is not selected:

1) the CSC PDU content is checked using the mechanism specific procedures such as those described in 10.3;

2) the procedures continue as described in 8.5.4.4, c).

NOTE – If SA-P is not selected and the CSC exchange mechanism requires the exchange of more than two CSC-PDUs, then these are exchanged in UN-DATA before continuing with connection establishment procedures.

c) The in-band SA-P is selected:

1) the SA-P exchange shall be carried out;

2) the calling NLSPE awaits SA-P completion as described in 8.5.4.4 or a UN-DISCONNECT indication as described in 8.10 or a UN-RESET indication as described in 8.9. Any error in the SA-P shall be treated as an error as described in 8.4.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.5.4.4 SA-P Completion/No SA-P

On completion of the SA-P:

a) If the SA-P is successful, the established SA is subsequently used for completion of NLSP connection establishment and secure communications as described in the following subclauses.

b) If the SA-P is unsuccessful, the calling or called NLSPE shall invoke a UN-DISCONNECT and the NLSP connection establishment procedures shall be aborted.

On completion of the SA-P or following a UN-CONNECT confirm without SA-P as described in 8.5.4.3, b):

c) The following NLSP-CONNECT parameters, as passed to the Calling NLSP in the event described in 8.5.4.1, shall then be placed in a SDT PDU as described in 6.4.1.1 with Data Type "NLSP-CONNECT req/ind":

- NLSP Calling Address;
- NLSP Called Address;
- NLSP Userdata.

NOTE 1 – The NLSP address parameters are carried in a protected form even if Param_Prot is FALSE.

d) The SDT PDU shall be passed to the UN service provider in UN-Userdata of a UN-DATA request.

NOTE 2 – This can provide the third part of the peer entity authentication exchange.

e) The calling NLSPE awaits UN-DATA indication containing an SDT PDU as described in 8.5.4.7 or a UN-DISCONNECT indication as described in 8.10 or a UN-RESET indication as described in 8.9.

On completion of the SA-P the called NLSPE shall await a UN-DATA indication containing a SDT-PDU as described in 8.5.4.5 or a UN-DISCONNECT indication as described in 8.10 or a UN-RESET indication as described in 8.9.

8.5.4.5 UN-DATA containing an SDT PDU at Called NLSPE

On receipt of a UN-DATA indication containing a Secure Data Transfer PDU at the Called NLSPE this shall be checked as described in 6.4.2.2.

NOTE – This can provide the third part of the peer entity authentication exchange.

The Data Type field in the SDT PDU shall be checked to be NLSP-CONNECT req/ind.

The NLSP Called Address shall be checked to be an NLSP Address served by this NLSP entity as determined locally.

The NLSP Calling Address shall be checked to be an NLSP Address contained in SA Attribute Adr_Served.

If any security label is established for the connection this is checked against the set of labels authorized in SA Attribute Label_Set.

The NLSP-CONNECT indication shall be passed to the called NLSP user with the parameters set as follows:

a) NLSP Calling Address, NLSP Called Address, NLSP Userdata set as in Content Fields of the received SDT PDU;

b) NLSP Receipt Confirmation Selection and NLSP Expedited Data Selection set to the setting of the equivalent UN parameters in the UN-CONNECT response sent under the procedures in 8.5.4.2;

c) NLSP QOS "available" set to the UN QOS "selected" by the called NLSPE in the UN-CONNECT response sent under the procedures in 8.5.4.2 and with "target" and "lowest acceptable" unspecified.

The called NLSPE shall await an NLSP-CONNECT response as described in 8.5.4.6 or a NLSP-DISCONNECT request as described in 8.10 or a UN-DISCONNECT indication as described in 8.10 or a UN-RESET indication as described in 8.9.

8.5.4.6 NLSP-CONNECT Response

On receipt of a NLSP-CONNECT response the NLSP Responding Address, NLSP Userdata parameters shall be placed in an SDT PDU as described in 6.4.1.1 with Data Type "NLSP-CONNECT res/conf".

This SDT PDU shall be passed to the UN service provider in UN-Userdata of a UN-DATA request.

The called NLSPE has now completed its NLSP connection establishment procedures.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.5.4.7 UN-DATA containing SDT PDU at Calling NLSPE

On receipt of a UN-DATA indication containing a SDT PDU this shall be checked as described in 6.4.2.1. The Data Type field shall be checked to be NLSP-CONNECT res/conf.

The NLSP Responding Address shall be checked to an NLSP Address contained in SA Attribute Adr_Served.

An NLSP-CONNECT confirm is sent to the NLSP user with parameters set as follows:

a) NLSP Responding Address, NLSP Userdata, if present, set as in Content Fields of the received SDT PDU;

b) NLSP Receipt Confirmation Selection and NLSP Expedited Data Selection set to the setting of the equivalent UN parameters in the UN-CONNECT confirm sent under the procedures in 8.5 4.3;

c) NLSP QOS set to the UN QOS received in the UN-CONNECT confirm received under the procedures in 8.5.3.

The calling NLSPE has now completed its NLSP connection establishment procedures.

8.6 NLSP-DATA Functions

8.6.1 NLSP-DATA Request

On receipt of an NLSP-DATA request if No_Header is TRUE then the NLSP Userdata shall be encapsulated as described in 6.4.1.2. This is placed in UN-Userdata of a UN-DATA request and the NLSP Confirmation request Parameter copied to the equivalent UN-DATA parameter. The UN-DATA shall then be passed to the UN service provider.

On receipt of an NLSP-DATA request if No_Header is FALSE then:

a) As a local matter the NLSPE shall segment the NLSP Userdata (if required by the SA).

b) For each segment an SDT PDU shall be generated as described in 6.4.1.1 with Data Type "NLSP-DATA req/ind" containing:

   1) the NLSP Userdata segment;

   2) the Last/Not last flag set to 0 for the last segment and 1 for all preceding segments;

   3) the NLSP Confirmation Request Content Field if:

      i) NLSP Confirmation Request is present indicating "confirmation of receipt requested" in the NLSP-DATA request; and

      ii) this is the last segment; and

      ii) Param_Prot is TRUE.

c) The SDT PDU for each segment shall be placed in the UN-Userdata parameter of a UN-DATA request.

d) The UN Confirm Request parameter of the UN-DATA shall present indicating "confirmation of receipt requested" if:

   1) NLSP Confirm Request is indicated in the NLSP-DATA request; and

   2) this is the last segment; and

   3) Param_Prot is FALSE

   else, the UN-Confirm request parameter shall indicate "confirmation of receipt not requested".

e) The UN-DATA request primitive for each segment shall be passed to the UN service provider.

8.6.2 Protected Data in UN-DATA indication Following Connection Establishment

On receipt of a UN-DATA indication if No_Header is TRUE then the UN Userdata shall be decapsulated as described in 6.4.2.2. This is placed in NLSP-Userdata of an NLSP-DATA indication and the UN Confirmation request Parameter copied to the equivalent NLSP-DATA indication parameter. The NLSP-DATA indication shall then be passed to the NLSP service user.

On receipt of a UN-DATA indication if No_Header is FALSE then:

a) The SDT PDU in the UN Userdata shall be checked as described in 6.4.2.1.

b) If the Data Type field is "unrelated to any NLSP service primitive" then the SDT PDU shall be processed as in 8.11 and not as described below.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

c) If the Data Type field is NLSP-DATA-ACKNOWLEDGE req/ind the SDT PDU shall be processed as in 8.9.2 and not as described below.

d) If the Data Type field is NLSP-DISCONNECT req/ind the SDT PDU shall be processed as in 8.10.2 and not as described below.

e) Otherwise the Data Type field shall be checked to NLSP-DATA and processed as follows.

f) If the Last/Not Last flag in the SDT PDU is set to 1 (Not last) then the NLSP Userdata Content field in the SDT PDU is appended to any previous NLSP Userdata which is part of the same NLSP-DATA request/indication and retained by the NLSPE for later use.

g) If the Last/Not Last flag in the SDT PDU is set to 0 (Last) then:

1) the NLSP Userdata Content field in the SDT PDU is appended to any previous NLSP Userdata which is part of the same NLSP-DATA request/indication and placed in NLSP Userdata parameter of an NLSP-DATA indication;

2) if Param_Prot is TRUE then the NLSP Confirm Request in the NLSP-DATA indication shall indicate "confirmation of receipt requested" if the Confirm Request Content Field is present in the SDT PDU;

3) if Param_Prot is FALSE then the UN Confirm Request in the received UN-DATA indication is copied to the equivalent parameter in the NLSP-DATA indication;

4) the NLSP-DATA indication is passed to the NLSP user.

8.7 NLSP-EXPEDITED-DATA Functions

8.7.1 NLSP-EXPEDITED-DATA Request

On receipt of an NLSP-EXPEDITED DATA request if No_Header is TRUE then the NLSP Userdata shall be encapsulated as described in 6.4.1.2. This is placed in UN-Userdata of a UN-EXPEDITED-DATA request. The UN-EXPEDITED-DATA request shall then be passed to the UN service provider.

On receipt of an NLSP-EXPEDITED DATA request if No_Header is FALSE then:

a) As a local matter the NLSPE shall segment the NLSP Userdata (if required by the SA).

b) For each segment an SDT PDU shall be generated as described in 6.4.1.1 with Data Type "NLSP-EXPEDITED-DATA req/ind" containing:

1) the NLSP Userdata segment;

2) the Last/Not last flag set to 0 for the last segment and 1 for all preceding segments;

3) the SDT PDU for each segment shall be placed in the UN-Userdata parameter of a UN-EXPEDITED-DATA.

c) The UN-EXPEDITED-DATA request primitive for each segment shall be passed to the UN service provider.

NOTE – When using the SDT PDU because 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 when crossing the Underlying Network.

8.7.2 UN-EXPEDITED DATA Indication

On receipt of a UN-EXPEDITED DATA indication if No_Header is TRUE then the UN Userdata shall be decapsulated as described in 6.4.2.2. This is placed in NLSP-Userdata of an NLSP-EXPEDITED-DATA indication. The NLSP-EXPEDITED-DATA indication shall then be passed to the NLSP service provider.

On receipt of a UN-EXPEDITED DATA indication if No_Header is FALSE then:

NOTE – When using the SDT PDU because the encapsulation function may expand the size of the data. Thus, the restricted size of the Userdata field may require the SDT PDU to be reassembled from several NLSP-EXPEDITED-DATA requests before being fully processed.

a) The SDT PDU in the UN Userdata shall be checked as described in 6.4.2.1. The Data Type in the SDT PDU shall be checked to be NLSP-EXPEDITED DATA req/ind.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

b) If the Last/Not Last flag in the SDT PDU is set to 1 (Not last) then the NLSP Userdata Content field in the SDT PDU is appended to any previous NLSP Userdata which is part of the same NLSP-EXPEDITED-DATA request/indication and retained by the NLSPE for later use.

c) If the Last/Not Last flag in the SDT PDU is set to 0 (Last) then:

1) the NLSP Userdata Content field in the SDT PDU is appended to any previous NLSP Userdata which is part of the same NLSP-EXPEDITED-DATA request/indication and placed in NLSP Userdata parameter of an NLSP-EXPEDITED-DATA indication;

2) the NLSP-EXPEDITED-DATA indication service primitive is passed to the NLSP user.

8.8 RESET Functions

Any of the NLSP or UN-RESET related events listed below pre-empts any CSC PDU exchange, SA-P exchange or Test Exchange that is in progress.

8.8.1 NLSP-RESET Request

On receipt of an NLSP-RESET request a UN-RESET request shall be issued with the same parameter values.

Any segmented NLSP-Userdata retained under the procedures described in 8.6 or 8.7 shall be discarded.

The NLSPE shall await a UN-RESET confirm as described in 8.8.2 or an NLSP-DISCONNECT request or a UN DISCONNECT indication as described in 8.10. The NLSPE discard all UN-DATA and UN-DATA-ACKNOWLEDGE primitives until a UN-RESET confirm or DISCONNECT is received.

8.8.2 UN-RESET Confirm following NLSP-RESET Request

On receipt of a UN-RESET confirm, following a NLSP-RESET Request as described in 8.8.1, an NLSP-RESET confirm shall be issued with the same parameter values.

NOTE – It may 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. This may be achieved using the CSC PDU exchange described below.

If SA Attribute Initiator is TRUE then the NLSPE shall initiate a CSC exchange as described in 8.12.1. Otherwise the NLSPE shall await UN-DATA containing a CSC-PDU as described in 8.12.2.

8.8.3 UN-RESET Indication

On receipt of a UN-RESET indication during NLSP connection establishment procedures as described in 8.5 a UN-DISCONNECT request and NLSP-DISCONNECT indication shall be issued in compliance with the OSI network service and the connection establishment procedures aborted.

On receipt of a UN-RESET indication follow completion of NLSP connection establishment:

a) An NLSP-RESET indication shall be issued with the same parameter values.

b) Any segmented NLSP-Userdata retained under the procedures described in 8.6 or 8.7 shall be discarded.

c) The NLSPE shall await an NLSP-RESET response as described in 8.8.4 or an NLSP-DISCONNECT request or a UN DISCONNECT indication as described in 8.10. The NLSPE discard all UN-DATA and UN-DATA-ACKNOWLEDGE primitives until an NLSP-RESET response or DISCONNECT is received.

8.8.4 NLSP-RESET Response following UN-RESET Indication

On receipt of an NLSP-RESET response following a UN-RESET indication as described in 8.8.3 a UN-RESET response shall be issued.

NOTE – It may 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. This may be achieved using the CSC PDU exchange described below.

If SA Attribute Initiator is TRUE then the NLSPE shall initiate a CSC exchange as described in 8.12.1. Otherwise the NLSP shall await UN-DATA containing a CSC-PDU as described in 8.12.2.

8.8.5 NLSP initiated Reset

On a reset initiated due to a event relating to the NLSP protocol (e.g. a check failure as described in 8.4):

a) Any segmented NLSP-Userdata retained under the procedures described in 8.6 or 8.7 shall be discarded.

b) An NLSP-RESET indication shall be passed to the NLSP service user with NLSP Originator and NLSP Reason set to a locally determined value.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

c) A UN-RESET request shall be passed to the UN service provider with UN Reason set to a locally determined value.

d) The NLSPE shall await an NLSP-RESET response as described in 8.8.6 and a UN-RESET confirm as described in 8.8.7. An NLSP-DISCONNECT request or a UN DISCONNECT indication as described in 8.10 may also be received.

e) The NLSPE shall discard all UN-DATA and UN-DATA-ACKNOWLEDGE primitives until a UN-RESET confirm or any DISCONNECT is received.

f) The NLSPE shall discard all NLSP-DATA and NLSP-DATA-ACKNOWLEDGE primitives until an NLSP-RESET response or any DISCONNECT is received.

8.8.6 NLSP-RESET Response following an NLSP initiated Reset

No further action is required on an NLSP-RESET following an NLSP initiated Reset.

8.8.7 UN-RESET Confirm following an NLSP initiated Reset

NOTE – It may 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. This may be achieved using the CSC PDU exchange described below.

On a UN-RESET Confirm following an NLSP initiated Reset, if SA Attribute Initiator is TRUE, then the NLSPE shall initiate a CSC exchange as described in 8.12.1. Otherwise the NLSPE shall await UN-DATA containing a CSC-PDU as described in 8.12.2.

8.9 NLSP-DATA ACKNOWLEDGE

8.9.1 NLSP-DATA-ACKNOWLEDGE Request

On receipt of an NLSP-DATA-ACKNOWLEDGE request, if No_Header is TRUE or Param_Prot is FALSE, then a UN-DATA-ACKNOWLEDGE request is passed to the UN service provider.

On receipt of an NLSP-DATA-ACKNOWLEDGE, if No_Header is FALSE and Param_Prot is TRUE then:

a) an SDT PDU shall be generated as described in 6.4.1.1 with Data Type "NLSP-DATA-ACKNOWLEDGE req/ind" containing no additional Content Fields;

b) the SDT PDU shall be passed to the UN service provider as UN-Userdata in a UN-DATA request primitive.

8.9.2 Protected NLSP-DATA-ACKNOWLEDGE in UN-DATA indication

If an SDT PDU is received in UN-DATA indication with the Data Type set to NLSP-DATA-ACKNOWLEDGE, as described in 8.6.2, item c), then:

a) the SDT PDU shall be checked that it contains no Content Fields related to NLSP service parameters;

b) an NLSP-DATA-ACKNOWLEDGE indication shall be passed to the NLSP user.

8.9.3 UN-DATA-ACKNOWLEDGEMENT indication

On receipt of a UN DATA-ACKNOWLEDGEMENT:

a) the NLSPE shall check that No_Header is TRUE or Param_Prot is FALSE;

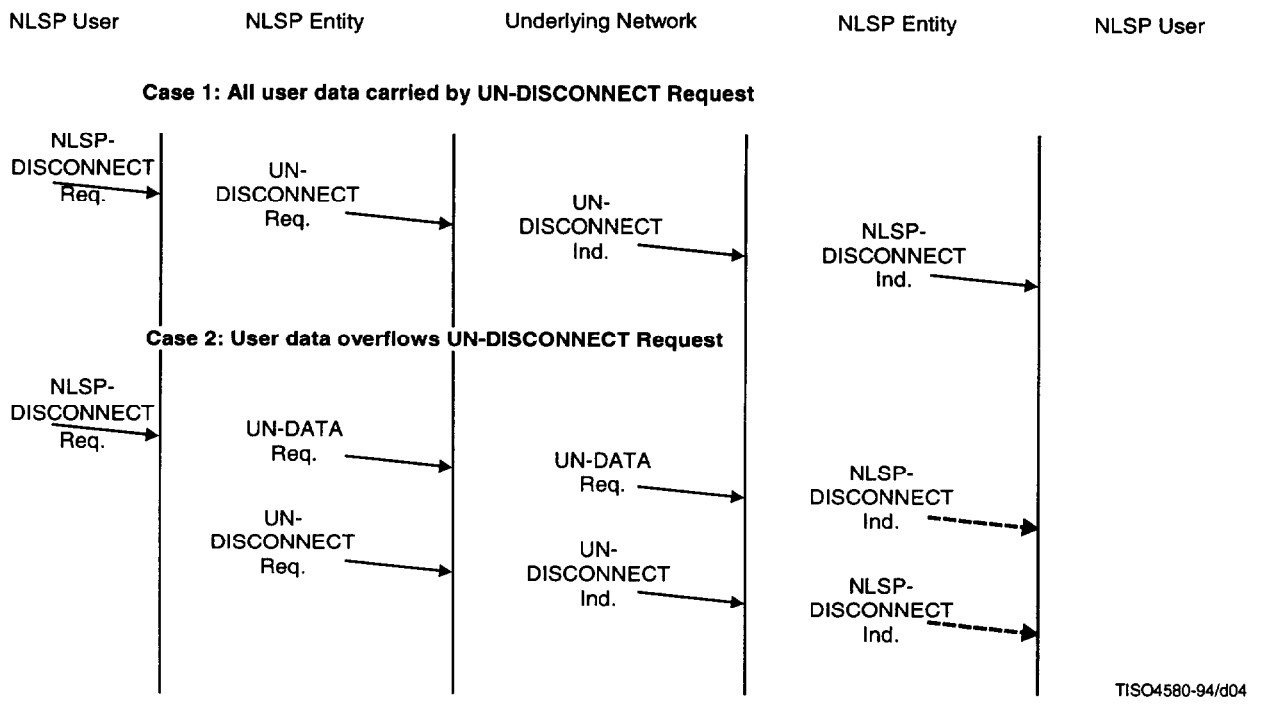
b) an NLSP-DATA-ACKNOWLEDGEMENT indication shall be passed to the NLSP user.

8.10 NLSP-DISCONNECT

Any of the NLSP or UN-DISCONNECT related events listed below pre-empts any CSC-PDU exchange, SA-P exchange or Test Exchange that is in progress.

The procedures for NLSP user initiated disconnect are illustrated in Figure 8-4.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale



NOTE – NLSP DISCONNECT may occur at either of the points indicated.

Figure 8-4 – Service Primitive Time Sequence Diagram for NLSP-DISCONNECT

8.10.1 NLSP-DISCONNECT Request

On receipt of an NLSP-DISCONNECT request during NLSP connection establishment procedures as described in 8.5 a UN-DISCONNECT request shall be issued in compliance with the OSI network service (i.e. if the establishment of a UN connection has started) and the connection establishment procedures aborted. If Protect_Connect_Params is TRUE the parameters of any UN-DISCONNECT request shall be determined locally else the NLSP-DISCONNECT request parameters shall be copied across the equivalent UN-DISCONNECT request parameters.

NOTE – If an NLSP-DISCONNECT request occurs during connection establishment and Protect_Connect_Params is selected the NLSP-DISCONNECT request parameters will be discarded.

On receipt of an NLSP-DISCONNECT request following NLSP connection establishment:

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 of a UN-DISCONNECT request. Other NLSP-DISCONNECT request parameters are copied through to the equivalent UN-DISCONNECT request parameters.

b) If Protect_Connect_Params is TRUE, No_Header is FALSE and Param_Prot is TRUE then an SDT PDU is generated containing all the NLSP-DISCONNECT request parameters as described in 6.4.1.1 with Data Type "NLSP-DISCONNECT req/ind". This is placed in UN-Userdata. Other UN-DISCONNECT parameters are determined locally.

c) If NLSP Userdata is present, Protect_Connect_Params is TRUE, No_Header is FALSE and Param_Prot is FALSE then a SDT PDU is generated containing NLSP Userdata as described in 6.4.1.1 with Data Type "NLSP-DISCONNECT req/ind". This is placed in UN-Userdata. Other NLSP-DISCONNECT request parameters are copied through to the equivalent UN-DISCONNECT request parameters.

d) If Protect_Connect_Params is FALSE then all the NLSP-DISCONNECT parameters are copied through to the equivalent UN-DISCONNECT request parameters.

NOTE – It is assumed that the same limits to the length of NLSP Userdata applies as for UN Userdata.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

e) If following b) or c) above, the resulting UN-Userdata parameter is greater than the maximum length of the UN-Userdata of the UN-DISCONNECT request then this shall be sent instead in a UN-DATA request UN-Userdata parameter and passed to the UN service provider. The UN Userdata for the UN-DISCONNECT request shall be empty.

NOTE – An implementation should wait for this UN-DATA to traverse the underlying network before proceeding with the UN-DISCONNECT as described in the following paragraph. The duration of this wait is determined locally.

f) A UN-DISCONNECT request shall be sent with the parameters set as described above.

8.10.2 Protected NLSP-DISCONNECT in UN-DATA Indication

If an SDT PDU is received in UN-DATA indication with the Data Type set to NLSP-DISCONNECT, as described in 8.6.2 item d), then:

a) the NLSPE checks that Protect_Connect_Params is TRUE and No_Header is FALSE;

b) any content fields containing NLSP service parameters are copied to the equivalent NLSP DISCONNECT parameters and NLSP Originator is set to NS User;

c) the NLSPE retains the NLSP-DISCONNECT parameters set as above awaits a UN-DISCONNECT indication or issues an NLSP-DISCONNECT indication immediately. The choice is a local decision.

8.10.3 UN-DISCONNECT Indication

On Receipt of a UN-DISCONNECT indication during NLSP connection establishment procedures as described in 8.5 an NLSP-DISCONNECT indication shall be issued in compliance with the OSI network service and the connection establishment procedures aborted. The UN-DISCONNECT indication parameters shall be copied across the equivalent parameters of any NLSP-DISCONNECT indication or if Protect_Connect_Params is TRUE set as determined locally.

Otherwise, on a UN-DISCONNECT indication following NLSP connection establishment with UN Userdata not empty:

a) If Protect_Connect_Params is TRUE and No_Header is TRUE then the UN Userdata shall be decapsulated as described in 6.4.2.2. This is placed in NLSP Userdata of an NLSP-DISCONNECT indication. Other NLSP-DISCONNECT indication parameters shall be set to the equivalent parameters the UN-DISCONNECT indication.

b) If Protect_Connect_Params is TRUE, No_Header is FALSE and Param_Prot is TRUE then a SDT PDU in the UN Userdata shall be checked as described in 6.4.2.1. The Data Type shall be checked to be NLSP-DISCONNECT req/ind. Any Content Fields relating to the NLSP-DISCONNECT parameters are copied through to these parameters.

c) If Protect_Connect_Params is TRUE, No_Header is FALSE and Param_Prot is FALSE then a SDT PDU in UN Userdata is checked as described in 6.4.2.1. The Data Type shall be checked to be NLSP-DISCONNECT. The presence of the Userdata Content Field shall be checked and then copied through to the NLSP Userdata of an NLSP-DISCONNECT indication. Other UN-DISCONNECT indication parameters are copied through to the equivalent NLSP-DISCONNECT indication parameters.

d) If Protect_Connect_Params is FALSE then all the UN-DISCONNECT parameters are copied through to the equivalent NLSP-DISCONNECT indication parameters.

e) The NLSP-DISCONNECT indication shall be passed to the NLSP user.

Otherwise, on a UN-DISCONNECT indication following NLSP connection establishment with NLSP Userdata empty:

a) If the NLSPE is awaiting an UN-DISCONNECT indication following a Protected NLSP-DISCONNECT in UN-DATA indication [see 8.10.2 c)] then the protected NLSP parameter fields shall be placed in the NLSP-DISCONNECT indication. Other NLSP-DISCONNECT indication parameters shall be set to the equivalent parameters the UN-DISCONNECT indication.

b) Else, the UN-DISCONNECT indication parameters shall be copied through to the equivalent NLSP-DISCONNECT indication parameters.

c) The NLSP-DISCONNECT indication shall be passed to the NLSP user unless one has already been issued.

The SA Attributes may be deleted locally following any UN-DISCONNECT if Retain_On_Disconnect is false.

8.10.4 NLSP Initiated Disconnect

On failure of an SA-P or any other check NLSP-DISCONNECT indications and UN-DISCONNECT requests are passed to the NLSP user and underlying network as defined in 8.4.

Figure 8-5 gives an illustrative example of an NLSP initiated disconnect due to an unsuccessful SA-P.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale

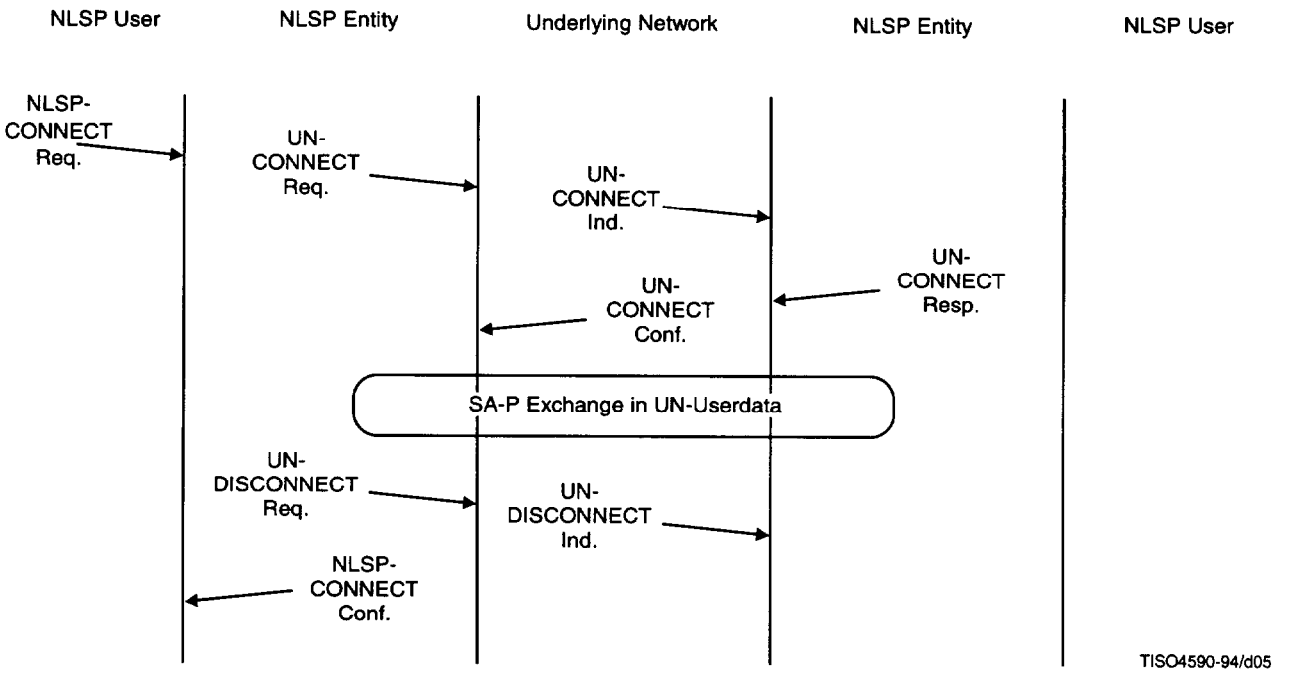


Figure 8-5 – NLSP initiated disconnect due to an unsuccessful SA-P

8.11 Other Functions

The following procedures are initiated on timed or other external events.

8.11.1 Modify Dynamic SA-Attributes

The NLSPE may modify dynamic SA attributes (see Annex G) at any time during the lifetime of a connection. Any change to dynamic SA attributes shall not modify the security services provided. This shall be achieved through an exchange of CSC PDUs or an SA-P exchange (using either SA-PDUs or SDT PDUs with content data type SA Protocol) in UN-DATA Userdata or by external means. This exchange is transparent to the NLSP user and no NLSP primitives are defined to invoke it.

NOTE – For example, this exchange could take place at regular intervals during a connection (for example, every hour or every 10 000 Secure Data PDUs) in order to exchange keys.

When data transfer is being performed with No_Header selected a UN-RESET shall be sent before the exchange of CSC PDUs as defined in 8.8.5.

The procedures for CSC-PDU exchange shall be as described in 8.12. An example SA-P which include procedures for modification of SA Attributes is given Annex C.

8.11.2 Security Test Exchange

These procedure shall be used to test the operation of the cryptographic aspects of a SA.

These procedures can only be invoked at states where NLSP-DATA primitives can be sent in UN-DATA (i.e. after NLSP connection establishment is complete, before any disconnect procedures and not during reset procedures).

A test exchange will be pre-empted by any DISCONNECT, RESET, CSC-PDU exchange or SA-P exchange.

NOTE – The use of this facility will be governed by locally. Possible modes of usage are:

a) not used;

b) following an exchange of keys;

c) periodically, at a locally determined time.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

8.11.2.1 Invocation of Test Exchange

On invocation of a test exchange:

a) a Test Data field shall be created with direction flag clear (set to 0) and test data set to random data;

b) a SDT PDU shall be generated as described in 6.4.1.1, with Data Type "not related to any NLSP service primitive", containing the Test Data field;

c) this PDU shall be sent in UN-DATA UN-Userdata with UN Receipt Confirmation indicating "receipt confirmation not required".

8.11.2.2 UN-Data with SDT PDU containing Test Data

On receipt of UN-DATA containing an SDT PDU with the Data Type set to 0 (unrelated to any NLSP service primitive) as described in 8.6.2, item b), if the SDT PDU contains Test Data it shall be processed as follows:

a) If the direction flag in the Test Data field is clear a new SDT PDU shall be generated as described in 6.4.1.1, with Data Type "not related to any NLSP service primitive" and containing a Test Data field with direction flag set and the data set to the random data received. This shall be returned in UN-DATA UN Userdata with UN Receipt Confirmation indicating "receipt confirmation not required".

b) If the direction flag in the Test Data is set then the received test data shall be checked to be identical to the test data sent earlier. If not the NLSPE shall perform error functions as defined in 8.4.

8.11.3 Traffic Padding

Additional UN-DATA primitives containing Secure Data Transfer PDUs with just Traffic Padding may be sent to hide the presence of user data.

All NLSP entities must be able to receive Secure Data Transfer PDUs with such Traffic Padding.

The use of this facility is at the discretion of the local NLSP entity and is transparent to the NLSP Service User.

8.11.3.1 Invocation of Traffic Padding

On invocation of traffic padding:

a) an SDT PDU shall be generated as described in 6.4.1.1, with Data Type "not related to any NLSP service primitive", containing no additional content fields other than those required by 6.4.1.1;

b) this PDU shall be sent in UN-DATA UN-Userdata with UN Receipt Confirmation indicating "confirmation receipt not required".

8.11.3.2 UN-Data with SDT PDU containing No Additional Content Fields

On receipt of UN-DATA containing an SDT PDU with the Data Type set to 0 (unrelated to any NLSP service primitive) as described in 8.6.2, item b), if the SDT PDU contains no content fields, other than those generally required in clause 6, the SDT PDU shall be ignored.

8.12 Peer Entity Authentication

The procedures defined in 8.12.1 and 8.12.2 may be invoked:

- following a UN-RESET or NLSP-RESET as described in 8.8;
- at time intervals decided locally,

in order to perform peer entity authentication or modify dynamic SA attributes.

The exchange of CSC-PDUs during connection establishment is described in 8.5.

NLSP-DATA or NLSP-EXPEDITED-DATA requests shall not be serviced until a CSC exchange is complete.

The CSC-Exchange will be pre-empted by any RESET or DISCONNECT primitive.

8.12.1 Invocation of CSC Exchange

On invocation of a CSC Exchange a CSC shall be created with:

a) UNC-UND and SA-P flags clear;

b) SA-ID set to Your_SA-ID;

c) content set to the CSC first exchange as required for the mechanism specific procedures such as those described in 10.3.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

This CSC-PDU shall be sent in UN Userdata of a UN DATA with "confirmation request not required".

The NLSPE invoking the CSC exchange shall await an a UN-DATA containing a CSC PDU. Alternatively the CSC exchange can be pre-empted either by a UN-RESET or NLSP-RESET as described in 8.8, or a UN-DISCONNECT or NLSP-DISCONNECT as described in 8.10.

8.12.2 UN-DATA containing a CSC-PDU

On receipt of UN-DATA containing a CSC PDU (at either the initiator or the responder to the CSC exchange) then the Content is checked as required for the mechanism specific procedures as described in 10.3.

Depending on the mechanism specific procedures the NLSPE may:

a) Return with a CSC-PDU content and indicate further CSC exchange is required

In which case the CSC PDU UNC-UND and SA-P flags shall be clear, SA-ID set to Your_SA-ID and the Content set as required for the mechanism specific procedures. The CSC PDU shall be sent in UN-DATA Userdata. The NLSPE shall await another UN-DATA containing a CSC PDU. Alternatively the CSC exchange can be pre-empted either by a UN-RESET or NLSP-RESET as described in 8.8, or a UN-DISCONNECT or NLSP-DISCONNECT as described in 8.10.

b) Return a CSC-PDU content and indicate SDT PDU required to complete exchange

In which case the CSC UNC-UND and SA-P flags shall be clear, SA-ID set to Your_SA-ID and the Content set as required for the mechanism specific procedures. The CSC PDU shall be send in UN-DATA Userdata. The NLSPE shall await another UN-DATA containing an SDT PDU which is processed as described in 8.6. Alternatively the CSC exchange can be pre-empted either by a UN-RESET or NLSP-RESET as described in 8.8, or a UN-DISCONNECT or NLSP-DISCONNECT as described in 8.10.

NOTE 1 – The authentication is not deemed to be complete, and hence NLSP-DATA (or NLSP EXPEDITED) requests shall not be processed at this NLSPE, until receipt of a SDT PDU. This SDT PDU may either contain a NLSP-DATA from the remote NLSP user or may be unrelated to any NLSP service primitive.

NOTE 2 – This option cannot be supported if No_Header is TRUE.

c) Return a CSC-PDU content and indicate exchange complete

In which case the CSC UNC-UND and SA-P flags shall be clear, SA-ID set to Your_SA-ID and the Content set as required for the mechanism specific procedures. The CSC PDU shall be send in UN-DATA Userdata.

d) Indicate that a SDT PDU is required to be sent completing the CSC exchange

In which case if NLSP-DATA (or NLSP-EXPEDITED-DATA) request is awaiting to be sent and No_Header is FALSE then this shall be processed as described in 8.6 or 8.7. Otherwise an SDT PDU shall 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 generally required in clause 6, and sent in UN Userdata of a UN-DATA primitive.

e) Indicate that the CSC exchange is complete

In which case no further action is required.

NOTE 3 – No general procedures are defined to resolve collisions between two CSC Exchanges initiated at the same time.

NOTE 4 – With the authentication mechanisms defined in clause 10, if use of the encapsulation/decapsulation functions, such as the one described in clause 11, does not include ISNs full peer entity authentication is not provided. In addition, full peer entity authentication is not provided if a No_Header encapsulation mechanism, such as the one described in clause 12, is used.

9 Overview of Mechanisms used

Clauses 9 to 12 define specific mechanisms for use with the generic protocol defined in clauses 1 to 8. These mechanisms are not the only mechanisms which can be used to provide security within the generic NLSP. Other mechanisms may be standardized in future and it is possible for private mechanisms to be used with NLSP.

9.1 Security Services and Mechanisms

NLSP-CL supports the following security services, if selected, with the mechanisms described:

a) *Data Origin Authentication* – The mechanism used to provide this service is ICVs in conjunction with key management.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

b) *Access Control* – The mechanisms used to provide this service are Security Labels and/or the control of keys and/or use of authenticated addresses.

c) *Connectionless Confidentiality* – The mechanism used to provide this service is encipherment. This protection optionally includes all NLSP service parameters depending on security services selected.

d) *Traffic Flow Confidentiality* – The mechanism used to provide this service is traffic padding and/or hiding the NLSP-address.

e) *Connectionless Integrity* – The mechanism used to provide this service is an ICV. This protection optionally includes all NLSP service parameters depending upon security services selected.

NLSP-CO supports the following security services, if selected, with the mechanisms described:

a) *Peer Entity Authentication* – The mechanism used to provide this service is an exchange of enciphered integrity sequence numbers in conjunction with key management.

b) *Access Control* – The mechanism used to provide this service is security labels and/or through the control of keys and/or authenticated addresses.

c) *Connection Confidentiality* – The mechanism used to provide this service is encipherment. This protection optionally includes all NLSP connection parameters depending upon security services selected.

d) *Traffic Flow Confidentiality* – The mechanism used to provide this service is traffic padding and/or address hiding.

e) *Connection Integrity without Recovery* – The mechanism used to provide this service is integrity check value and integrity sequence numbers. This protection optionally includes all NLSP connection parameters depending upon the security services selected.

9.2 Functions Supported

The essential feature of the mechanisms supported by NLSP are:

a) A connection authentication function which supports peer entity authentication and establishes initial values for "dynamic" SA Attributes supporting secure data transfer. This function is used by NLSP-CO only.

b) An encapsulation function based on the SDT PDU which supports secure data transfer by using the following mechanisms:

   1) Integrity Sequence Number;

   2) Padding for traffic flow confidentiality, block integrity algorithms, and block encipherment algorithms;

   3) Integrity Check Value;

   4) Encipherment.

c) An encapsulation function based on the No_Header form of protection which uses an encipherment mechanism which doesn't change the length of the data.

The mechanisms are carried out in the order given above.

10 Connection security control (NLSP-CO only)

10.1 Overview

The "Connection Security Control" procedure uses an exchange of Connection Security Control (CSC) PDUs to:

a) optionally, specify a new encipherment/integrity key;

b) perform peer entity authentication;

c) establish an integrity sequence number.

Support for a mechanism for authentication through the exchange of sequence numbers is specified by this ITU-T Recommendation | International Standard. Authentication using this mechanism is completed for the initiating entity when the two-way exchange is complete. For the responding entity, if sequence integrity is selected to protect against replay attacks (i.e. ISN is TRUE), authentication is complete only on receipt of the first SDT PDU from the initiating entity.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

10.2 SA-Attributes

The following security attributes are used to support the connection security control procedures:

a) *Mechanisms selected for the SA:*

Authentication: Boolean

Whether peer entity authentication using enciphered ISN is to be used.

The values of these attributes are defined by the ASSR given the security services selected.

b) *Key distribution mechanism attributes:*

kdm: mode to be used with this SA

The value of this attribute is defined by the ASSR given the security services selected.

This can have the following values:

kdm_mutual: distribution by symmetric keys.

kdm_asymmetric_single: distribution using recipients public key.

kdm_asymmetric_double: distribution using both the remote public and local private keys.

kdm_distributed: distribution by reference to a pre-distributed key or key distributed by other means.

kdm_other: A privately defined distribution mechanism is used.

c) Authentication mechanism attributes:

Auth_Alg: Object identifier allocated under ISO/IEC 9979

The value of this attribute is defined by the ASSR given security services selected.

Enc_Auth_len: Length of the encipher auth-data field in the CSC PDU

The value of this attribute is defined by the ASSR given the security services selected.

Auth_Gen_Key: Form constrained by ASSR

The initial value of this attribute is set up on SA establishment and can be changed during the lifetime of the association.

Auth_Check_Key: Form constrained by ASSR

The initial value of this attribute is set up on SA establishment and can be changed during the lifetime of the association.

The following attributes used by the Security Data Transfer mechanisms can be established by the Connection Authentication mechanism:

a) *ISN mechanism attributes:*

Data_My_ISN

Data_Your_ISN

Exp_My_ISN

Exp_Your_ISN

b) *Encipherment mechanism attributes:*

Data_Enc_Key

Data_Dec_Key

Exp_Enc_Key

Exp_Dec_Key

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

c) *ICV mechanism attributes:*

Data_ICV_Gen_Key

Data_ICV_Check_Key

Exp_ICV_Gen_Key

Exp_ICV_Check_Key

NOTE – Additional mechanism specific attributes may be identified in future versions of this ITU-T Recommendation | International Standard, and for private mechanisms.

10.3 Procedures

The NLSP entities exchange Connection Security Control (CSC) PDUs on each connection establishment or following a reset or on other externally timed events to:

a) optionally, specify the encipherment or integrity key;

b) perform peer entity authentication;

c) establish integrity sequence number.

Peer entity authentication may be provided as defined below. Any alternative method must yield an integrity sequence number if connection integrity is required.

The encipherment/integrity key is specified either:

a) by an indication that the existing key is to be used;

b) by passing a new key enciphered with a mutual key enciphering key;

c) by passing a new key enciphered with the public key of the recipient;

d) by reference to a key distributed previously.

NOTE 1 – Derivation of a encipherment key provides a small amount of integrity checking in that it prevents a replay of cipher text protected with a different key. The key derivation algorithm should be specific to each encipherment algorithm to prevent accidental derivation of weak keys.

NLSP uses a peer entity authentication method based upon the exchange of initial integrity sequence numbers enciphered using an authentication key. This method may be used even if sequence numbers are not used for integrity service.

The Connection Security Control procedures are based on the exchange of two CSC. PDUs and Secure Data Transfer PDU as follows.

A CSC PDU is prepared by the initiator of the security exchange:

a) The Enciphered Auth-Data set to a locally selected value of My-Initial-ISN and a 0 value for Your-Initial-ISN both enciphered using Auth_Gen_Key. The ISN selected must be unique for the authentication and integrity keys.

b) The key information set as required by the key distribution mechanism.

On receipt of a CSC PDU by an NLSP entity which is not already the initiator of a CSC PDU exchange:

a) the Enciphered Auth-Data is deciphered using Auth_Check_Key;

b) the Your-Initial field is checked to be 0;

c) the local SA-Attributes Data_Your_ISN and Exp_Your_ISN are set to the received My-Initial-ISN field;

d) the key information is processed as required by the key distribution mechanism.

Then a CSC PDU is prepared with:

a) The Enciphered Auth-Data set to a locally selected value of My-Initial-ISN and Your-Initial-ISN with the value of the received My-Initial-ISN both enciphered using Auth_Gen_Key. The ISN selected must be unique for the authentication and integrity keys.

b) The key information set as required by the key distribution mechanism.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

On receipt of a CSC PDU at the initiator of the CSC exchange:

a) the Enciphered Auth-Data is deciphered using Auth_Check_Key;

b) the Your-Initial field is checked against the My-Initial-ISN sent previously;

c) the local SA-Attributes Data_Your_ISN and Exp_Your_ISN are set to the received My-Initial-ISN field;

d) the key information is processed as required by the key distribution mechanism.

Following successful checking of the response, if the NLSP entity has no data awaiting and the ISN mechanism is selected for the SDT PDU encapsulation (see clause 11), then a Secure Data Transfer PDU containing no data but including an ISN shall be sent to complete the authentication.

NOTE 2 – The SDT PDU may be sent even if data is awaiting to complete the authentication procedures without the need to carry out normal data transfer procedures.

If the authentication fails, then depending on a local decision the security association may be re-established either in or out of band as well as taking the error recovery procedures described in 8.4.

10.4 CSC-PDU Fields used

The following mechanism specific CSC content fields defined in 13.5.6 are used by the procedures in this clause:

a) Enciphered Auth-Data;

b) Key Information.

11 SDT PDU Based encapsulation Function

11.1 Overview

NLSP-CL, and optionally NLSP-CO, protect user data and related protocol control information using an SDT PDU based encapsulation function. This clause defines such an Encapsulation function. This Encapsulation function is based on four functions:

- ISN;
- Padding;
- ICV; and
- Encipherment.

The decision to employ a particular function shall be based on attributes of the SA.

If sequence numbering is selected, an ISN field shall be added.

NOTE 1 – It is not expected that this protection mechanism would be used with NLSP-CL.

If traffic padding is selected, a traffic padding field may be added.

If a block integrity algorithm is used, an integrity padding field may be added.

If integrity checking is selected, an ICV shall be computed over and appended to the above fields.

NOTE 2 – The ICV can also be used to provide data origin authentication.

If a block encipherment algorithm shall be used, an encipherment padding field may be added.

If encipherment is selected, the above fields are enciphered using the encipherment key for the Security Association.

The procedure described above encapsulates user data and other NLSP protocol parameters to provide protection for transfer over a network. At the remote end, the recipient of a Secure Data Transfer PDU removes and checks protection by reversing the procedure order.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

11.2 SA Attributes

a) *Mechanisms selected for the SA:*

ISN: Boolean
Integrity Sequence Numbers to be included in each Encapsulated-octet-string.

Padd: Boolean
Padding within the Encapsulated-octet-string to support the Traffic Padding mechanism.

ICV: Boolean
Integrity and/or data origin authentication of the Encapsulated-octet-string contents using an integrity check value.

Encipher: Boolean
Encipherment of an encapsulated-octet-string to provide confidentiality.

The values of these attributes are defined by the ASSR given the target security services selected.

b) *ISN Mechanism attributes:*

ISN_Len: Integer

The value of this attribute shall be defined by the ASSR given the security services selected.

Data_My_ISN: ISN for last normal data sent.

Data_Your_ISN: ISN for last normal data received.

Exp_My_ISN: ISN for last expedited data sent.

Exp_Your_ISN: ISN for last expedited data received.

The initial value of these "key" attributes shall be set up on SA establishment and can be changed during the lifetime of the association.

NOTE 1 – The expedited data ISN attributes are applicable to NLSP-CO only.

c) *Padding Mechanism Attributes:*

Traff_Padd: Form constrained by ASSR
Traffic Padding requirements.

d) *ICV mechanism attributes:*

ICV_Alg: Object Identifier

The value of this attribute shall be constrained by the ASSR given the security services selected. This attribute implies certain attributes of the integrity mechanism such as separate generate and check algorithms, initialisation vectors, etc.

ICV_Blk: Integer
Basic block size on which the ICV algorithm operates.

The value of this attribute shall be constrained by the ASSR given the security services selected.

ICV_Len: Integer
The length of the output of the ICV mechanism.

The value of this attribute shall be defined by the ASSR given the security services selected.

It is not necessary that ICV_Len equal ICV_Blk.

Data_ICV_Gen_Key: form constrained by ASSR
ICV generation key reference for normal data

Data_ICV_Check_Key: form constrained by ASSR
ICV check key reference for normal data

Exp_ICV_Gen_Key: form constrained by ASSR
ICV generation key reference for expedited data

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Exp_ICV_Check_Key: form constrained by ASSR
ICV check key reference for expedited data

The initial value of these "key" attributes shall be set up on SA establishment and can be changed during the lifetime of the association.

NOTE 2 – The expedited data key attributes are applicable to NLSP-CO only.

e) *Encipherment Mechanism Attributes:*

Enc_Alg: Object identifier allocated under ISO/IEC 9979

The value of this attribute shall be constrained by the ASSR given the security services selected. This attribute implies certain attributes of the encipherment mechanism such as the form and length of any synchronisation field, separate encipherment and decipherment algorithms, initialisation vectors, etc.

Enc_Blk: Integer

Block size of encipherment algorithm.

The value of this attribute shall be constrained by the ASSR given the security services selected.

Data_Enc_Key: form constrained by ASSR

Encipherment key reference for normal data

Data_Dec_Key: form constrained by ASSR

Decipherment key reference for normal data

Exp_Enc_Key: form constrained by ASSR

Encipherment key reference for expedited data

NOTE 3 – This is only used by NLSP-CO.

Exp_Dec_Key: form constrained by ASSR

Decipherment key reference for expedited data

NOTE 4 – This is only used by NLSP-CO.

The initial value of these "key" attributes shall be set up on SA establishment and can be changed during the lifetime of the association.

NOTE 5 – Additional mechanism specific attributes may be identified in future versions of this ITU-T Recommendation | International Standard and for private mechanisms.

11.3 Procedures

As encapsulation takes place, a PDU shall be formed by appending or pre-pending fields. These fields may be optional. A partially formed PDU is referred to below as "existing fields". During decapsulation a PDU shall be decomposed by removing fields. A partially decomposed PDU is referred to below as "remaining data".

NOTES

1 The description of appending and pre-pending fields is not meant to constrain implementations of NLSP but rather to unambiguously specify the protocol.

2 This encapsulation function does not handle the No_Header option. This is handled by procedures defined in clause 12.

11.3.1 Encapsulate Function

The SA-ID shall be used to reference a Security Association. If the Security Association does not exist, then the error SA-not-available shall be returned and the value of encapsulated-octet-string shall be undetermined.

If (ISN is TRUE) then either:

a) If (data-unit-type = normal) then Data_Your_ISN shall be advanced and placed in the Sequence Number Content Field and appended to the existing fields in Octet-String-Before-Encapsulation.

b) If (data-unit-type = expedited) then Exp_Your_ISN shall be advanced and placed in the Sequence Number Content Field and appended to the existing fields in Octet-String-Before-Encapsulation.

NOTES

1 The ISN may be advanced by incrementing a sequence number or by choosing the next number from a non-repeating sequence. Time stamps can also be regarded as a non-repeating sequence.

2 It is not expected that the ISN mechanism would be used with NLSP-CL.

3 Exp_My_ISN is only applicable to NLSP-CO.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

If (Padd is TRUE) then an amount and form of padding as determined locally by the ASSR rules referred to in Traff_Padd shall be placed in a Traffic Padding Content Field and appended to the existing fields in Octet-String-Before-Encapsulation. If a single octet of padding is required, then the Single Octet Padding Content Field shall be used.

If (ICV is TRUE) and (ICV_Blk >1) then, if necessary, an Integrity Pad field shall be appended to the existing fields such that the length of the existing fields with the Integrity Pad field (including the protected content field) is an integral multiple of the ICV block size (that is, ICV_Blk). If present, then an amount and form of padding as determined locally shall be placed in the Integrity Pad Content Field. If a single octet of padding is required, then the Single Octet Pad Content Field shall be used. The Content Length value shall be increased by the amount of padding added.

A Content Length shall be placed before the existing fields. The length of all existing fields shall be determined and placed in the Content Length.

If (ICV is TRUE) then an ICV of length ICV_Len shall be calculated over, and appended to, the existing fields. The algorithm used shall be identified by ICV_Alg and the key used shall be either:

a) Data_ICV_Gen_Key if data-unit-type = normal; or

b) Exp_ICV_Gen_Key if data-unit-type = expedited.

If (Encipher is TRUE) then a crypto synchronisation Field with a form and length as determined by the Enc_Alg shall be generated and pre-pended to the existing fields.

If (Encipher is TRUE) then an encipherment pad shall be appended to the existing fields so that the length of the existing fields (that is, Protected Data Length, Octet-String-Before-Encapsulation, ISN, Integrity Pad, and ICV fields) plus the length of an encipherment pad shall be an integral multiple of the encipherment block size (that is, Enc_Blk). If present, then the amount and form of padding as determined locally shall be placed in an Encipherment Pad Content Field. If a single octet of padding is required, the Single Octet Padding Content Field shall be used.

If (Encipher is TRUE) then the existing fields are enciphered. The algorithm used shall be identified by Enc_Alg and the key used shall be either:

a) Data_Enc_Key if data-unit-type = normal; or

b) Exp_Enc_Key if data-unit-type = expedited.

The constructed PDU shall be returned as the result in encapsulated-octet-string.

11.3.2 Decapsulate Function

If any of the following checks fail all security relevant status information will be set to the security status information before reception of this message, except for alarm, auditing, and/or accounting information.

The SA-ID argument shall be used to reference a Security Association. If the Security Association does not exist then the error SA-not-available shall be returned and the value of Octet-String-Before-Encapsulation shall be undetermined.

If (Encipher is TRUE) then the following steps are taken:

a) The encapsulated-octet-string shall be decrypted. The decipherment algorithm used shall be identified by Enc_Alg and the key used shall be either:

   1) Data_Dec_Key if data-unit-type = normal; or

   2) Exp_Dec_Key if data-unit-type = expedited.

b) The Crypto Synchronisation field shall be removed by discarding a number of octets, as determined by the Enc_Alg, from the front of the deciphered data.

c) The Encipherment Pad or Single Octet Pad Content Field shall be removed by adding the Contents Length and ICV_Len then discarding any octets in the remaining deciphered data which are beyond the calculated length.

If (ICV is TRUE) then the following steps are taken:

a) The ICV field shall be verified by checking the last ICV_Len octets of the remaining data. The algorithm used shall be identified by ICV_Alg and, if cryptographically based, the key used to calculate the ICV shall be:

   1) Data_ICV_Check_Key if data-unit-type = normal; or

   2) Exp_ICV_Check_Key if data-unit-type = expedited.

b) If the ICV verification fails, then the error data-unit-integrity-failure shall be returned and the value of Octet-String-Before-Encapsulation shall be undetermined.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The ICV shall be removed by discarding any octets in the remaining data which are beyond the length contained in Content Length after the Content Length field.

The Content Length field shall be removed by discarding the first two octets of the remaining data.

Any Traffic Padding, Integrity Padding, or Single Octet Padding Content Fields are removed from the remaining data by removing data beyond the Octet-String-Before-Encapsulation.

NOTE 1 – The Content Fields are located by decoding the contents of the Octet-String-Before-Encapsulation, which is a one-octet Type field followed by a number of TLV fields.

If (ISN is TRUE) then the remaining data shall be checked to ensure that one and only one ISN Content Field is present; or else the remaining data shall be checked to ensure that no ISN Content Field is present. If present and:

a) if (data-unit-type = normal) then Data_My_ISN shall be advanced and the value checked against the window of expected values as determined by Data_My_ISN.

b) if (data-unit-type = expedited) then Exp_My_ISN shall be advanced and the value checked against the window of expected values as determined by Exp_My_ISN.

In both items a) and b), the ISN is advanced before checking.

NOTE 2 – Advancement may be achieved by incrementing a sequence number or by choosing the next number from a pseudo-random, non-repeating sequence.

The value of the Octet-String-Before-Encapsulation shall be returned as the result in Octet-String-Before-Encapsulation.

11.4 PDU Fields used

These procedures use the following fields of an SDT PDU as defined in 13.3:

a) Encapsulated-octet-string;

b) Crypto Synchronization;

c) ICV;

d) Content fields:

1) Encipherment Pad;

2) Sequence Number;

3) Single Octet Pad;

4) Traffic Pad;

6) Integrity Pad.

12 No-Header Encapsulation Function (NLSP-CO only)

12.1 Overview

NLSP-CO can provide user data confidentiality only through the use of a No_Header option. The No_Header option uses an Encapsulation function such as that described within this Clause. This Encapsulation function shall be based on an Encipherment mechanism.

Use of the No_Header option implies that the encipherment mechanism operates on a block length of one octet, and that the algorithm does not alter the size of the enciphered data.

12.2 SA Attributes

a) Mechanisms selected for the SA:

Encipher: Boolean

Encipherment of an encapsulated-octet-string to provide confidentiality.

The values of this attribute shall be defined by the ASSR given the security services selected.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

b) Encipherment Mechanism Attributes:

Enc_Alg:	Object identifier allocated under ISO/IEC 9979 The value of this attribute shall be defined by the ASSR given the security services selected. This attribute implies certain attributes of the encipherment mechanism such as the form and length of any synchronisation field, separate encipherment and decipherment algorithms, initialisation vectors, etc.
Data_Enc_Key:	form constrained by ASSR Encipherment key reference for normal data
Data_Dec_Key:	form constrained by ASSR Decipherment key reference for normal data
Exp_Enc_Key:	form constrained by ASSR Encipherment key reference for expedited data
Exp_Dec_Key:	form constrained by ASSR Decipherment key reference for expedited data

The initial value of these "key" attributes shall be set up on SA establishment and can be changed during the lifetime of the association.

NOTE – Additional mechanism specific attributes may be identified in future versions of this ITU-T Recommendation | International Standard and for private mechanisms.

12.3 Procedures

12.3.1 Encapsulate Function

The SA-ID is used to reference a Security Association. If the Security Association does not exist then the error SA-not-available shall be returned and the value of encapsulated-octet-string shall be undetermined.

If (Encipher is TRUE) then the Octet-String-Before-Encapsulation shall be enciphered. The algorithm used shall be identified by Enc_Alg and the key used shall be either:

a) Data_Enc_Key if data-unit-type = normal; or

b) Exp_Enc_Key if data-unit-type = expedited.

The enciphered data shall be returned as the result in encapsulated-octet-string.

12.3.2 Decapsulate Function

If any of the following checks fail all security relevant status information will be set to the security status information before reception of this message, except for alarm, auditing, and/or accounting information.

The SA-ID argument shall be used to reference a Security Association. If the Security Association does not exist then the error SA-not-available shall be returned and the value of Octet-String-Before-Encapsulation shall be undetermined.

If (Encipher is TRUE) then the encapsulated-octet-string shall be deciphered. The decipherment algorithm used shall be identified by Enc_Alg and the key used shall be either:

a) Data_Dec_Key if data-unit-type = normal; or

b) Exp_Dec_Key if data-unit-type = expedited.

The value of the deciphered data shall be returned as the result in Octet-String-Before-Encapsulation.

13 Structure and Encoding of PDUS

13.1 Introduction

The NLSP protocol uses 3 PDU types:

a) Secure Data Transfer PDU;

b) Security Association PDU;

c) Connection Security Control PDU.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

A further unstructured data format with no PCI is used with the No_Header option for protected data.

All PDUs shall contain an integral number of octets. The octets in a PDU are numbered starting from one (1) and increasing in the order in which they are put into the appropriate "Underlying Network" Request. When consecutive octets are used to represent a binary number, the lower octet number has the most significant value. The bits in an octet are numbered from one (1) to eight (8), where bit one (1) is the low-order bit.

When the encoding of a PDU is represented using a diagram in this clause,

a) octets are shown with the lowest numbered octet to the left or above;

b) within an octet, bits are shown with bit eight (8) to the left and bit (1) to the right.

The notations below a box show the length of each field in octets; "var" indicates that the field length is variable.

The presence or absence of an "optional" field shall be specified by the attributes contained in the Security Association.

NOTE – The optional fields are optional in that a given security association will require the presence of certain fields and the absence of other fields. Once the Security Association is decided, the presence or absence of each field is determined by the SA Attributes.

13.2 Content Field Format

The Content Field is a general field format for data values to be placed in the PDUs defined in this clause (see Figure 13-1).

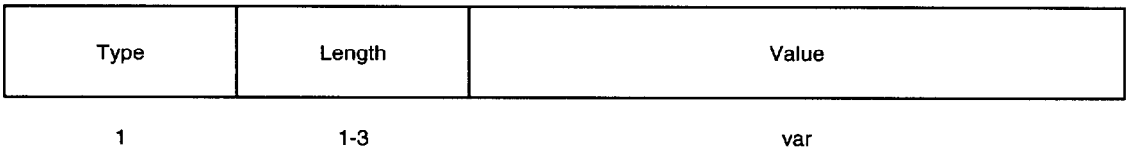


Figure 13-1 – Content Field

The Content Field Type shall be set to one of the following values:

Value	*Content Field Type*
00-5F	Reserved for Private use
60-9F	Reserved for Future use
A0-BF	Reserved for SA-P use (see Annex C)
C0-CF	Reserved for mechanism independent use (see 13.3.4.3)
D0-FF	Reserved for mechanism dependent use (see 13.3.5)

The Content Field Length shall contain the length of the Content Field Value in octets. The Content Field Length shall be one, two or three octets long:

a) if one octet long, then bit 8 shall be 0 and the remaining 7 bits define a value length up to 127 octets;

b) if two octets long, then the first octet shall be encoded as 1000 0001 and the remaining octet defines the fields length up to 255 octets;

c) if three octets long, then the first octet shall be encoded as 1000 0010 and the remaining two octets define the field length up to 65 535 octets.

Other values of the first octet are reserved for future use.

The Content Field Value shall contain data for the PDU field.

13.3 Protected Data

This subclause describes the PDUs used for transfer of protected data. This includes two aspects of the PDUs: those which are independent of the mechanism used (marked generic) and those which are specific to the mechanisms supported by the encapsulation procedures defined in clause 11 (marked mechanism specific). Those which include both generic and mechanism specific aspects are marked mixture.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

13.3.1 Basic PDU Structures (Generic)

Two data structures are defined for the transfer of secure data. The first is mandatory for NLSP-CL, one of the two must be supported for NLSP-CO.

a) The Secure Data Transfer PDU formatted as shown in Figure 13-2.

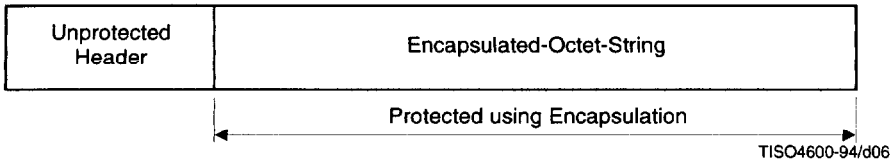


Figure 13-2 – Generic Secure Data Transfer PDU Structure

The structure of the Unprotected header is defined in 13.3.2. The Encapsulated-Octet-String field shall contain the output from an Encapsulate Function (for example, as described in clause 11 using the structure defined in 13.3.3) operating on the Octet-String-Before-Encapsulation as structured as described in 13.3.4.

The conditions (mandatory/optional, etc.) for support of the fields forming this PDU are defined in D.5.3, D.5.4 (mechanism specific fields), D.6.4 (NLSP-CL only) and D.7.6 (NLSP-CO only).

b) An unstructured bit string for the No_Header confidentiality only option formatted as shown in Figure 13-3. No PCI is added.

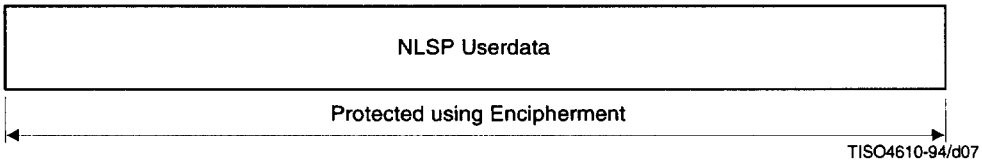


Figure 13-3 – Confidentiality only using No_Header Option

The no-header option shall only be used when all of the following conditions are met:

a) No_Header is TRUE;

b) Label is FALSE;

c) ICV is FALSE;

d) ISN is FALSE;

e) Encipher is TRUE;

f) Enc_Sync_Len = 0;

g) Enc_Blk = 1;

h) Pad is FALSE.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

13.3.2 Unprotected Header (Generic)

The format of the Unprotected Header shall be as shown in Figure 13-4.

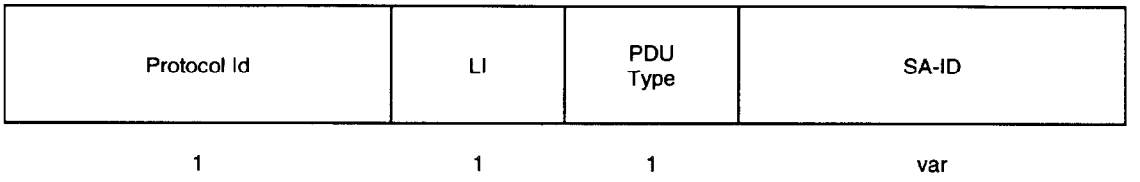


Figure 13-4 – Unprotected Header

13.3.2.1 Protocol Id (generic)

This field shall contain the NLSP protocol identifier, value 1000 1011.

13.3.2.2 LI (generic)

This field contains the length of the PDU Type field plus the SA-ID.

For NLSP-CO, the SA-ID field is not required. Therefore, this field shall be set such that the SA-ID field is not present (that is, value 00000001).

13.3.2.3 PDU Type (generic)

This field shall contain the PDU type value of 01001000 to indicate a Secure Data Transfer PDU.

13.3.2.4 SA-ID (generic)

The SA-ID field shall contain the Security Association Identifier of the remote entity (i.e. the SA attribute Your_SA-ID). This field is not required for NLSP-CO.

13.3.3 Encapsulated-Octet-String (Mechanism Specific)

The structure of the SDT PDU using the mechanism specific procedures defined in clause 13 shall be as shown in Figure 13-5.

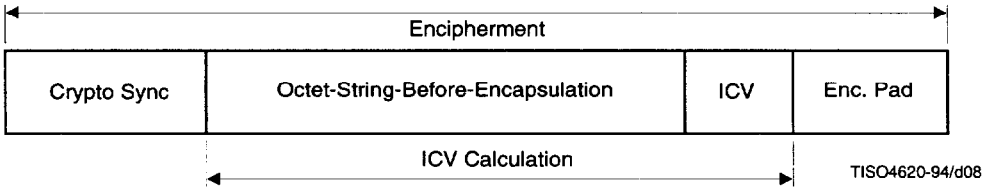


Figure 13-5 – Structure of Encapsulated Octet String

13.3.3.1 Crypto Synchronisation (Mechanism Specific)

This is an optional field which may contain Synchronization data for specific encipherment algorithms. Its presence, form, and length are implied by Enc_Alg.

13.3.3.2 Integrity Check Value (Mechanism Specific)

This field contains an Integrity Check Value (ICV). The length of this field shall be defined by the ICV algorithm identifier contained in the Security Association attributes.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

13.3.3.3 Encipherment Pad (Mechanism Specific)

This field contains encipherment padding (End. Pad) for the purposes of supporting block encipherment algorithms for confidentiality. The choice of padding value is a local matter. All NLSPEs must be able to discard this field. The format of this field shall be encoded either as defined in 13.2 or as defined for the encipherment algorithm. The Type code of this TLV field shall be as defined in 13.3.5. If a two octet pad is required the length shall be zero with no value. If a single octet pad is required a single octet PAD field shall be used instead of an Encipherment PAD field.

The use of this field is dependant on whether the encipherment algorithm requires an independent encipherment pad.

13.3.4 Octet-String-Before-Encapsulation (Mixture)

Figure 13-6 shows the format for the Octet-String-Before-Encapsulation. This contains any number of generic and mechanism specific content fields.

At least the Content Length and Data Type shall be present.

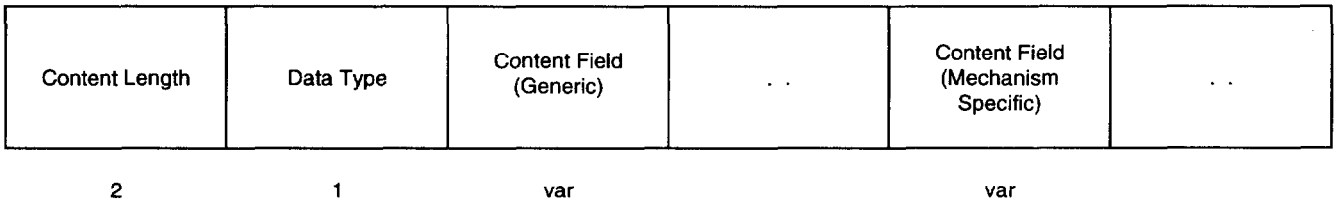


Figure 13-6 – Octet-String-Before-Encapsulation

13.3.4.1 Content Length (Generic)

This field shall contain the combined length of the all the Content Fields and the Data Type.

NOTE – This does not include the ICV or Encipherment Pad fields.

13.3.4.2 Data Type (Generic)

Bit 8 of this field shall be the "Initiator to Responder" flag. A value of 1 indicates Initiator to Responder. A value 0 indicates Responder to Initiator.

Bit 7 of this field shall be the "Last/Not Last" flag. This bit shall take the value 0 when the SDT PDU contains the last segment of a sequence. Otherwise it shall take the value 1. For NLSP-CL this shall always take the value 0.

Bits 1-6 of this field are encoded to identify the NLSP service primitives as follows:

Value	*Service Primitive*
000000	Not related to any NLSP service primitive (for example, Test Data)
000001	NLSP-UNITDATA req/ind
000010	NLSP-CONNECT req/ind
000011	NLSP-CONNECT resp/conf
000100	NLSP-DATA req/ind
000101	NLSP-DATA-ACKNOWLEDGE req/ind
000110	NLSP-EXPEDITED DATA req/ind
000111	NLSP-DISCONNECT req/ind
001000	SA Protocol
001001-011111	Reserved for future use
100000-111111	Reserved for private use

13.3.4.3 Content Fields (Generic)

The content field type encoding shall be as defined in 13.2. The mechanism independent content fields (that is, C0-CF) used by the procedures in clauses 6, 7 and 8 are given below:

Value	*Content Field Type*
00-BF	Reserved
C0	Userdata

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

C1	Test Data
C2	Calling/Source NLSP address
C3	Called/Destination NLSP address
C4	Responding NLSP address
C5	Not used
C6	Label
C7	Label Reference
C8	Confirmation Request
C9	Disconnect Reason
CA-CF	Reserved for future use
D0-FF	Reserved

13.3.4.3.1 NLSP Userdata

This field contains the NLSP Userdata from the service primitive.

13.3.4.3.2 Test Data

The structure of the test data shall be as shown in Figure 13-7.



Figure 13-7 – Test Data

Test Control contains a set of bits allocated as follows:

a) Bit 1 – Direction Flag. 0 for original, 1 for reflected test data.

b) Bits 2-4 – Reserved for future use.

c) Bits 5-8 – Reserved for private use.

13.3.4.3.3 Calling/Source NLSP Address

This field contains a Network Layer address encoded in one of the forms described in CCITT Recommendation X.213 | ISO 8348/AD2.

13.3.4.3.4 Called/Destination NLSP Address

This field contains a Network Layer address encoded in one of the forms described in CCITT Recommendation X.213 | ISO 8348/AD2.

13.3.4.3.5 Responding NLSP Address

This field contains a Network Layer address encoded in one of the forms described in CCITT Recommendation X.213 | ISO 8348/AD2.

13.3.4.3.6 Label

This field shall be used to carry the security label of a PDU. This field is not present if a Label Reference Content field is present (see Figure 13-8).

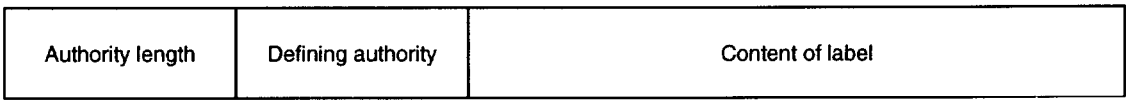


Figure 13-8 – Value of Label

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The defining authority shall be encoded as the contents of a object identifier value using the basic encoding rules of an object identifier defined in clause 22 of CCITT Recommendation X.209 | ISO/IEC 8825.

The structure and interpretation of the Contents of the Label are defined by various Defining Authorities.

NOTE – It is expected that these labels will be registered under procedures defined by ISO/IEC and ITU-T. A Defining Authority will be registered as an Object Identifier using procedures defined in ISO/IEC 9834.

13.3.4.3.7 Label Reference

This field identifies one of the set of security labels defined in the SA attribute Label_Set. When present, this field shall always be encoded so that the value part of the field is two octets. This field shall not be present if a Label Content field is present.

13.3.4.3.8 Confirmation Request

When present this field indicates that confirmation of receipt is requested. This field shall be encoded as a one octet type code (without length or value).

13.3.4.3.9 Disconnect Reason

This field shall carry the NLSP-DISCONNECT reason service parameter encoded as carried on the underlying network.

NOTE – In the case of the underlying network being an ISO/IEC 8208/CCITT X.25 network the first octet is the value is the cause and, if present, the second octet is the diagnostic code mapped from the NLSP-DISCONNECT reason as defined in as defined in CCITT Recommendation X.223 | ISO/IEC 8878.

13.3.5 Content Fields (Mechanism Specific)

Content Field encoding shall be as defined in 13.2. Content Field Type encoding for mechanism specific content fields are given below:

Value	*Content Field Type*
00-CF	Reserved
D0	Sequence Number
D1	Single Octet Pad
D2	Traffic Pad
D3	Integrity Pad
D4	Encipherment Pad
D5-FF	Reserved for future use

13.3.5.1 Sequence Number

This field contains Your_ISN (that is, a PDU integrity sequence number) which shall be unique within under the current key for that data type (expedited or normal).

NOTE – In NLSP CO uniqueness between expedited and normal data streams (and hence replay protection) is provided by the Data Type field (see 13.3.4.2) being different.

13.3.5.2 Single Octet Pad

This field shall be a 1 octet Type (without Length or Value) field for general padding (for example, to support a single octet of integrity padding). This octet may be used, one or more times, instead of a TLV encoded Integrity, Encipherment, or Traffic Pad field to provide integrity, encipherment, or traffic padding. All NLSPEs shall detect and discard this field.

13.3.5.3 Traffic Pad

This field contains padding for the purposes of traffic flow confidentiality. The choice of padding value is a local matter. All NLSPEs shall detect and discard this field. If a two octet pad is required the length shall be zero with no value. If a single octet pad is required a Single Octet Pad shall be used instead of a Traffic Pad.

13.3.5.4 Integrity Pad

This field contains padding for the purposes of supporting block integrity algorithms. The choice of padding value is a local matter. All NLSPEs must be able to discard this field. If a two octet pad is required the length shall be zero with no value. If a single octet pad is required a Single Octet Pad shall be used instead of an Integrity Pad.

This field can also be used to fulfil requirements for encipherment padding.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

13.4 Security Association PDU

The format of the Security Association PDU shall be as shown in Figure 13-9.

The conditions (mandatory/optional, etc.) for support of the fields forming this PDU are defined in D.5.5 and D.5.6 (mechanism specific fields).

Protocol Id	LI	PDU Type	SA-ID	SA-P Type	SA-PDU Contents
1	1	1	var	var	var

Figure 13-9 – Security Association PDU Structure

13.4.1 Protocol Identifier (PID)

This field shall contain the NLSP protocol identifier, value 10001011.

13.4.2 LI

This field shall contain the length of the PDU Type field plus the SA-ID field.

If the SA-P needs to signal that it does not know its peer's SA-ID (for example, on establishing a new SA), this field shall be set to the value 00000001 to indicate that the SA-ID field is not present.

13.4.3 PDU Type

This field shall contain the PDU type value of 01001001 to indicate a Security Association PDU.

13.4.4 SA-ID

The SA-ID field shall contain the Security Association Identifier of the remote entity (that is, the SA attribute Your_SA-ID). This field is not required when the SA-P is being used to establish a new SA (that is, the recipient has not yet assigned an SA-ID).

13.4.5 SA-P Type

This field shall contain an object identifier indicating the mechanism used to provide the SA Protocol. This object identifier shall be encoded as the content of the object identifier value using the basic encoding rules defined in clause 22 of CCITT Rec. X.209 | ISO/IEC 8825, preceded by a single octet length indicator.

The following object identifier is assigned for use of the generic SA-P with Key Token Exchange procedures as defined in Annex C along with the Exponential Key Exchange algorithm described in Annex H:

join-ccitt-iso nlsp (22) sa-p-kte (1) eke (1)

Use of other SA protocols or algorithms with the SA-P defined in Annex C may be indicated by further object identifiers allocated in accordance with ISO/IEC 9834-1.

13.4.6 SA-PDU Contents

The internal structure of this field shall be dependent on the mechanism providing the SA Protocol as specified in 13.4.5 above. Annex C defines one such SA-Protocol.

13.5 Connection Security Control PDU

The format of the Connection Security Control PDU shall be as shown in Figure 13-10.

The conditions (mandatory/optional, etc.) for support of the fields forming this PDU are defined in D.7.7, D.7.8 (mechanism specific fields).

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Protocol ID	LI	PDU Type	SA-ID	Content Length	CSC-PDU Content
1	1	1	var	1	var

Figure 13-10 – Connection Security Control PDU

13.5.1 Protocol Identifier

This field shall contain the NLSP protocol identifier, value 1000 1011.

13.5.2 LI

This field shall contain the length of the PDU Type field plus the SA-ID field.

13.5.3 PDU Type

This field shall contain the PDU type value of xx111111 to indicate a Connection Security Control PDU. The bit values for this field shall be as follows:

a) Bits 1-6 shall contain the PDU type value of 111111 to indicate a Connection Security Control PDU.

b) Bit 7 – UNC-UND flag, if set shall indicate that the NLSP-CONNECT is being be carried in UN-Data, else if clear it shall indicate that the NLSP-CONNECT is being carried in the UN-CONNECT.

c) Bit 8 – SA-P flag, shall indicate that SA-P is being invoked in this connection. If bit 8 is set, then no further fields are present in this PDU.

13.5.4 SA-ID

The SA-ID field shall contain the Security Association Identifier of the remote entity (that is, the SA attribute Your_SA ID). This field shall not be present if the SA-P flag is set.

13.5.5 Content Length

This shall contain the length of the CSC-PDU Content in octets. This field shall not be present if the SA-P flag is set.

13.5.6 CSC-PDU Content

The internal structure of this field shall be dependent on the mechanism supporting connection authentication. This field shall not be present if the SA-P flag is set. The fields required for the specific security control mechanism given in clause 10 are as follows (see Figure 13-11).

Enciphered-Auth-Data	Key Info
(Note 1)	(Note 2)

NOTES

1 The length of Enciphered-Auth-Data is dependent on the encipherment algorithm used and defined by SA Attribute Enc_Auth_len.

2 The length of Key information depends on the key distribution method used. It is not included if the key is not changed.

Figure 13-11 – CSC-PDU Contents

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

13.5.7 Enciphered Auth-Data (Mechanism Specific)

See Figure 13-12.
This field contains a number which is used for authentication and, if selected, as an integrity sequence number, its length is defined as part of the SA Attributes. When sent from the calling to called NLSP entity Your-initial ISN is 0.

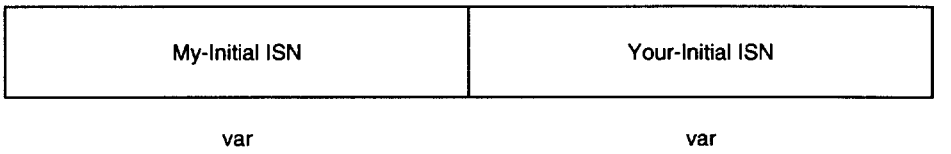


Figure 13-12 – Enciphered Auth-data

13.5.8 Key Information Mechanism Specific

Depending on the key distribution method selected for the security association this parameter is not present, indicating that an existing key is to be used, or contains one of the following depending on SA attributed kdm:

kdm_mutual –	A key enciphered using mutual KEK.
kdm_asymmetric_single –	A key enciphered with the public key of the recipient.
kdm_asymmetric_double –	A key enciphered with the private key of the sender and the public key of the recipient.
kdm_distributed –	A key reference.
kdm_other –	content defined privately.

The presence of this field is implied from the Content Length compared with the SA-Attribute Enc_Auth_len.

14 Conformance

14.1 Static Conformance Requirements

14.1.1 Conformance Classes

The system shall support one or both of the following classes of conformance:

a) NLSP-CL mode;

b) NLSP-CO mode.

Support for these conformance classes is defined in terms of capabilities defined in 14.1.2 and 14.1.3.

Support for each of the classes of conformance shall optionally be by using the security mechanisms supported by this ITU-T Recommendation | International Standard.

The use of security mechanisms supported by this ITU-T Recommendation | International Standard is defined in terms of requirements on the security mechanisms as defined in 14.1.5.

14.1.2 NLSP-CL mode Capabilities

14.1.2.1 Security Services

A system in conformance with NLSP-CL mode shall support the following services:

a) One or more of the following services:

   1) Connectionless confidentiality;

   2) Connectionless integrity;

   3) Data origin authentication.

b) Optionally, access control;

c) Optionally, traffic flow confidentiality.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

14.1.2.2 Scope of Protection

A system claiming conformance with NLSP-CL shall support either or both:

a) protection of All NLSP Service Parameters;

b) protection of NLSP Userdata.

A system claiming conformance with NLSP-CL may, optionally, support:

c) No protection.

14.1.2.3 Other Capabilities

When NLSP-CL mode is supported the system shall be capable of transmitting and/or receiving an SDT PDU.

14.1.3 NLSP-CO mode Capabilities

14.1.3.1 Security Services

A system in conformance with NLSP-CO mode shall support the following security services:

a) One or more of the following services:

1) Connection confidentiality;

2) Connection integrity without recovery;

3) Peer entity authentication.

b) Optionally, access control;

c) Optionally, traffic flow confidentiality.

14.1.3.2 Scope of Protection

A system claiming conformance with NLSP-CO shall support one or more of:

a) protection of All NLSP Service Parameters;

b) protection of NLSP Userdata including NLSP Userdata in NLSP-CONNECT and NLSP-DISCONNECT;

c) protection of NLSP Userdata during data transfer.

A system claiming conformance with NLSP-CL may, optionally, support:

c) No protection.

14.1.3.3 Other Capabilities

When NLSP-CO mode is supported the system shall be capable of:

a) initiating and/or accepting a connection;

b) transmitting and receiving a CSC PDU;

c) transmitting and/or receiving at least one of:

1) data protected using the No_Header based encapsulation mechanisms as defined in 6.4.1.2 and 6.4.2.2;

2) SDT PDU based encapsulation as defined in 6.4.1.1 and 6.4.2.1;

d) at least one of the modes of NLSP connection establishment defined in 8.5;

e) optionally, support test exchanges;

f) optionally, support an in band SA protocol.

14.1.4 Support for PDUs

Table 14-1 shows whether support for a given PDU is mandatory or optional for a given mode of operation.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table 14-1 – NLSP Support for PDUs

PDU	Condition for Support
SDT PDU	Mandatory for CL Mandatory if CO and SDT PDU based encapsulation is supported
SA PDU	Optional if SA-P is supported
CSC PDU	Mandatory for NLSP-CO

14.1.5 Static Requirements for Mechanisms

A system claiming to support the security mechanisms defined in this International Standard ITU-T Recommendation shall meet the following requirements with respect to the mechanisms selected:

a) Each system claiming to support connection or connectionless confidentiality security services shall provide those services through the use of an encipherment mechanism.

b) Each system claiming to support connectionless integrity or connection integrity without recovery security services shall provide those services using a mechanism which uses the ICV field as defined in 13.3.3.2 and, optionally, the ISN field as defined in 13.3.5.1.

d) Each system claiming to support the traffic flow confidentiality security service shall provide that service using a mechanism which uses the traffic pad field as defined in 13.3.5.3.

e) Each system claiming to support the data origin authentication security service shall provide that service using either an encipherment mechanism or a cryptographic mechanism which uses the ICV field as defined in 13.3.3.2.

f) Each system claiming to support the peer entity authentication security service shall support the enciphered auth-data field as defined in 13.5.7.

14.2 Dynamic Conformance Requirements

14.2.1 General Requirements

a) The system shall correctly generate, accept and respond to all valid protocol elements that support each class and mode of operation to which conformance is claimed.

b) The system shall respond correctly to all incorrect sequences of NLSP protocol elements.

14.2.2 Specific Requirements

For each conformance class to which conformance is claimed and for each option of the static conformance requirements implemented, the system shall exhibit external behaviour consistent with having implemented the following:

a) the common protocol functions defined in clause 6;

b) for NLSP-CL mode, the protocol functions defined in clause 7;

c) for NLSP-CO mode, the protocol functions defined in clause 8;

d) for NLSP-CL systems supporting mechanism specific procedures, the protocol functions in clause 11;

e) for NLSP-CO systems support mechanisms specific procedures, the protocol functions in clause 10 for connection security control and the encapsulation protocol functions in either clauses 11 or 12.

f) the structure and encoding of PDUs as described in clause 13, Structure and encoding of PDUs.

14.3 Protocol Implementation Conformance Statement

A Protocol Implementation Conformance Statement (PICS) given in Annex D shall be completed with respect to any claim for conformance of an implementation to this ITU-T Recommendation | International Standard. The PICS shall be produced in accordance with the relevant PICS proforma.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex A

Mapping UN primitives to CCITT Rec. X.213 | ISO/IEC 8348

(This annex forms an integral part of this ITU-T Recommendation | International Standard)

Table A-1

UN Primitive	Conveyed by	Comments
UN-UNITDATA	N-UNITDATA	Simple mapping from UN primitive to CCITT Rec. X.213 | ISO/IEC 8348 AD1 N-UNITDATA primitive
UN-CONNECT	N-CONNECT	Params mapped onto equivalent CCITT Rec. X.213 | ISO/IEC 8348 parameters except: – UN Authentication concatenated with UN Userdata is mapped to Userdata in the N-CONNECT primitives.
UN-DATA	N-DATA	Simple mapping: All params mapped onto equivalent CCITT Rec. X.213 | ISO/IEC 8348 parameters.
UN-EXPEDITED-DATA	N-EXPEDITED-DATA	Simple mapping
UN-DATA-ACKNOWLEDGE	N-DATA-ACKNOWLEDGE	Simple mapping
UN-DISCONNECT	N-DISCONNECT	Simple mapping

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex B

Mapping UN Primitives to CCITT Rec. X.25 | ISO/IEC 8208

(This annex forms an integral part of this ITU-T Recommendation | International Standard)

In OSI environments, mapping between UN service primitives and the ISO/IEC 8208 or the CCITT Recommendation X.25 protocol is as defined in ISO/IEC 8878 for the equivalent network layer services primitives, with the exception of the UN-CONNECT UN Authentication parameter which is conveyed in the DTE "protection facility".

In Table B.1 the middle column describes the ISO/IEC 8208 or X.25 packets used to convey the UN primitives. In this case ISO/IEC 8208 or X.25 may be used in any way permitted by this ITU-T Recommendation | International Standard and, for example, the Q-bit may be invoked. Such ISO/IEC 8208 or X.25 specific features pass through NLSP unchanged.

Table B.1

UN Primitive	Conveyed by	Comments
UN-UNITDATA	N/A	
UN-CONNECT	CALL	All parameters mapped into equivalent ISO/IEC 8208 / X.25 CALL packet facilities except UN Authentication parameter which is conveyed in the DTE "Protection facility".
UN-DATA	DATA	Simple mapping
UN-EXPEDITED-DATA	INTERRUPT	Simple mapping
UN-DATA-ACKNOWLEDGE	RR or RNR	Simple mapping
UN-DISCONNECT	CLEAR	Simple mapping

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex C

Security Association Protocol Using Key Token Exchange and Digital Signatures

(This annex forms an integral part of this ITU-T Recommendation | International Standard)

C.1 Overview

This annex defines a protocol for use of an asymmetric mechanism to perform the SA establishment and abort/release. It allows the communicating NLSP entities to:

a) authenticate the two entities to each other;

b) initialize SA attributes including keys; and

c) establish initial information for use in providing integrity.

This annex describes an SA-Protocol which logically performs the following distinct functions:

a) A key token exchange is used to establish a shared secret. This supports an exchange of key tokens. The form of these tokens is mechanism specific. An example of mechanism specific key tokens, supporting exponential key exchange, also known as Diffie Hellman exchange, is outlined in Annex H.

b) Certificates, digital signatures and elements from the key token exchange are used to achieve authentication.

c) Protocol exchanges are used to negotiate SA attributes.

d) Protocol exchanges to signal that the SA is being released.

Prior to establishing an SA using this SA-Protocol each NLSP entity must have pre-established the following information:

a) the mechanisms it supports as expressed by:

   1) a list of ASSRs supported; and

   2) the set of security services supported for each of the ASSRs identified above;

b) an asymmetric key pair for each asymmetric algorithm supported which can be used by the NLSP entity to sign data for authentication purposes;

c) a certificate from a trusted authority for each asymmetric algorithm supported which identifies the NLSP entity, and its public asymmetric key, for authentication purposes;

d) the public keys, and the implied asymmetric algorithms, of any trusted certification authorities which would issue certificates to NLSP entities which this NLSP entity will be communicating with.

This SA-Protocol dynamically establishes the following security information which it needs to secure its own communication:

a) negotiation of the encipherment algorithm to protect SA-Protocol communication;

b) negotiation of the asymmetric algorithm and digital signature scheme used to provide SA-Protocol authentication;

c) generation of keying information needed by the encipherment algorithm to protect SA-Protocol communication.

This SA-Protocol establishes the following shared information between two NLSP Entities:

a) local and remote SA-IDs;

b) security services to be used between the associated entities for instances of communication;

c) the mechanisms and their parameters as implied through the security services selected;

d) initial shared keys for integrity, encipherment mechanisms and authentication of an instance of communication;

e) the set of security labels that may be used on this association for access control.

An SA can be established using the same selected security services, mechanisms and their parameters and set of security labels from a previously established SA. In this case only the SA-ID and keys are changed, all other attributes shall remain the same.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Whenever a new SA is established new key values shall be established.

In the case of connectionless mode NLSP, after an SA has been released, the SA-ID shall placed in a frozen state. Whilst frozen, the SA-ID shall not be re-used. The period in which the SA-ID is frozen shall be greater than the maximum lifetime of a PDU in the underlying network.

The SA Attribute Adr_Served is established by means outside this protocol.

The SA Attribute Initiator is set to true for the initiator of the SA protocol exchange and false for the responder.

C.2 Key Token Exchange (KTE)

The NLSP entities start their SA-Protocol with a key token exchange to generate a shared secret (i.e. a bit string) between the entities. The NLSP entities then use a subset of this secret bit string in conjunction with a private key algorithm to encipher the remainder of the communications between them, thus providing confidentiality to the remainder of the SA-Protocol exchanges.

The KTE involves the exchange of two values, Key-Token-1 and Key-Token-2 calculated from mechanism specific parameters along with locally generated numbers using mechanism specific algorithms such as those outlined in Annex H. The exchanged values are then used by the two communicating entities to generate the shared secret bit string.

A subset of this bit string is used in conjunction with a private key algorithm to encipher the remainder of the SA Protocol exchange supporting SA-Protocol Authentication and SA Attribute negotiation. In addition, subset of this bit string is also referenced to be used as key and ISN attributes of the security association being established. This is referenced either:

1) by exchanging position information in the SA Attribute Negotiation; or

2) via apriori knowledge.

C.3 SA-Protocol Authentication

In order for an NLSP entity to authenticate another during SA establishment, it requires an authentication certificate and public key pair.

The NLSP entities exchange certificates and digital signatures (such as defined in CCITT Recommendation X.509 | ISO 9594-8 to verify each other's identity. A certificate contains, as a minimum, some identifying information for an NLSPE plus the entity's public key.

The certificate is certified by a trusted authority and provided to the NLSP using a procedure outside the scope of the NLSP protocol. The certificate carries the authentication signature of the trusted authority. An NLSP entity partaking in this SA-Protocol must have the public key of the trusted authority which issued the certificate. The method used to attain the trusted authority's public key is outside the scope of this ITU-T Recommendation | International Standard. For an NLSP entity to demonstrate that it owns a particular certificate, it must prove that it knows the secret key corresponding to the public key in the certificate.

Proof of timeliness and prevention of replay attacks is addressed by the signed data consisting of the specific numbers jointly determined and specific to this protocol operation. This is done as follows for two communicating entities A (the initiator of the SA) and B (the responder):

a) The SA contents is created, including A's Certificate and Key-Token-3 (calculated using an algorithm such as described in Annex H), and then signed (using, for example, the authentication signature defined in CCITT Recommendation X.509 | ISO/IEC 9594-8). This signature excludes the exchange ID and content length. The SA Contents, including the signature and the content length but excluding the exchange ID, is then enciphered. The encipherment key is the first n bits of the bit string produced by the KTE exchange, where n is the number of bits required by the algorithm used.

b) The SA contents is created carrying the SA Attribute negotiation (see C.4) or Abort/Release reasons (see C.5). This is then signed and enciphered as for (a) above using equivalent information relating to B and Key-Token-4 instead of Key-Token-3.

Each entity verifies the authentication signature of the peer entity by first decrypting the received exchange, then verifying the signature and checking the Key-Token to protect against replay attacks. Verification requires use of the peer entity's public key, and the agreed process for signature verification.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

C.4 SA Attribute Negotiation

C.4.1 Security Service Selection

As a local decision, the initiating NLSP Entity issues a set of one or more acceptable security service selections. Each element in the set contains the following:

a) the ASSR_ID which defines the semantics of the security services selected (listed below) for this element in the set; and

b) a Service selection values (semantics defined by the ASSR_ID) for each of: Confidentiality, Authentication, Access Control, Integrity, and Traffic Flow Confidentiality.

As a local decision, the recipient NLSP Entity will return the following PCI to the originator:

a) If one of the proposed set of services is acceptable, the recipient will return single selected service element.

b) If none of the proposed set of services is acceptable, the recipient will reject the SA by returning a Status indicating the reason for rejecting the SA.

NOTE – This negotiation allows both NLSP entities to select security services which are consistent with its local security policy.

C.4.2 Label Set Negotiation

Based on its local security policy, the initiating NLSP Entity issues a set of security labels and references which it is willing to have transferred under the protection of this SA. Each element in the set contains the following:

a) a reference which can be subsequently carried in place of the label during the lifetime of the SA for efficiency reasons; and

b) the full semantics of the label.

Based on its local security policy, the recipient NLSP Entity will determine which of the proposed set of labels it is willing to have transferred under protection of this SA. The recipient NLSP Entity will return the following PCI to the originator:

a) if one or more labels in the proposed set is acceptable, the recipient will return a subset of the proposed set of references. Null sets are not allowed.

b) If no labels in the proposed set are acceptable, the recipient will reject the SA by returning a Status indicating the reason for rejecting the SA.

NOTE – This negotiation allows either NLSP entity to select a label set which is consistent with its local security policy.

C.4.3 Key and ISN Selection

As a local decision, the initiating NLSP Entity selects those portions of the bit string resulting from the KTE for use as keys and/or ISNs during communications (i.e. NLSP communications and not SA-Protocol communications) to the recipient NLSP entity. The key/ISN is identified by communicating the starting bit position within the EKE resultant bit string. The key/ISN length is determined from the parameters associated with the selected service. A set of pointers is sent to the recipient NLSP entity for the following:

a) Normal Data Encipherment Key;

b) Expedited Data Encipherment Key;

c) Normal Data Integrity Check Generation Key;

d) Expedited Data Integrity Check Generation Key;

e) My ISN for Normal Data;

f) My ISN for Expedited Data; and

g) Authentication Generation Key.

Similarly, the recipient NLSP Entity will determine locally which portions of the EKE resultant bit string it will use for its keys/ISNs. The recipient NLSP Entity will return the following PCI to the originator:

a) if the recipient chooses to use the same bit positions as proposed by the initiating NLSP entity, no explicit PCI is returned;

b) if the recipient is rejecting the SA due to other negotiation failures, no explicit PCI is returned;

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

c) if the recipient selects different bit positions for its keys/ISNs, it will return a set of pointers;

NOTES

1 The same key value may be used for multiple purposes by providing the same pointer for more than one key/ISN.

2 This procedure need not be used if the positions for selecting keys and ISNs is known *a priori*.

C.4.4 Miscellaneous SA Attribute Negotiation

As a local decision, the initiating NLSP Entity determines the value of the following SA attributes for the SA being established:

a) retain these SA attributes on disconnection (NLSP-CO only);

b) protect the CO parameters (NLSP-CO only);

c) the No-Header option should be used (NLSP-CO only).

The initiating NLSP entity sends the recipient NLSP entity this set of proposed SA attributes in a Miscellaneous flags field.

As a local decision, the recipient NLSP Entity will return the following PCI to the originator:

a) If the recipient accepts all of the proposed SA attributes then no explicit PCI is returned. If the recipient does not reject the SA, it implies that the SA attributes are acceptable to the recipient NLSP entity.

b) If any one of the attributes is not acceptable, the recipient rejects the SA by returning a status indicating which attributes caused the rejection.

C.4.5 Re-keying

If an SA is being establish to rekey an old SA then only Key and ISN Selection are carried out. Instead of service, label set and miscellaneous SA Attribute negotiation the reference to the old SA from which these attributes are to be inherited is placed in Old-Your-SA-ID.

C.5 SA Abort/Release

An entity can indicate that it is no longer using a security association through a two way exchange of SA PDUs with a reason code signed and enciphered using the procedures defined in C.3.

C.6 Mapping of SA-Protocol Functions to Protocol Exchanges

This SA-Protocol performs the three functions described above during three distinct protocol exchanges:

a) the first exchange consists of EKE and certificate exchange and has no encipherment applied;

b) the second exchange consists of a security negotiation protected to provide authentication as defined in C.3;

c) a separate exchange initiated when the SA is no longer required consisting of a reason code protected to provide authentication as defined in C.3.

C.6.1 KTE (First) Exchange

C.6.1.1 Request to Initiate the SA-Protocol

The NLSP Entity or local security management initiates the SA-Protocol.

The initiating NLSP entity performs the following functions and sends the following information to the recipient:

a) An available SA-ID is selected and placed as the originator's My_SA-ID.

b) KTE is started and the Key-Token-1 is sent.

c) A list of proposed confidentiality mechanisms which could be used to protect the second SA-Protocol exchange. This list is expressed as a set of one or more elements which include: ASSR_ID, and confidentiality security services selected. This list need not be sent if mechanisms have been agreed in advance.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

d) A list of proposed integrity mechanisms, one of which would be used to digitally sign the second SA-Protocol exchange. This list is expressed as a set of one or more elements which include: ASSR_ID and integrity security services selected. This list need not be sent if mechanisms have been agreed in advance.

NOTES

1 The confidentiality security services selected should only identify a symmetric encipherment algorithm and its mode of operation. The integrity security services selected should only identify an asymmetric algorithm and its associated digital signature scheme.

2 Items c) and d) may be known *a priori*.

In the CO case, if no PDU is returned for the first exchange after a timeout, the SA is not established and no further attempts are made.

In the CL case, if no PDU is returned for the first exchange after a timeout, the initiating NLSP entity re-transmits its first exchange PDU. Re-transmissions are limited to a finite number which is locally defined.

C.6.1.2 Receipt of the First SA PDU by Recipient

Upon receipt of the first SA PDU, the recipient NLSP entity performs the following functions and sends the following information to the initiator:

a) The received My_SA-ID is placed in the Your_SA-ID field of the generic header as described in 13.4.

b) An available SA-ID is selected and sent as the originator's My_SA-ID.

c) As a local decision, the recipient NLSP Entity will return the following PCI to the originator:

1) If the recipient accepts one of the proposed confidentiality mechanism, then it returns the selected mechanism. If the initiator proposed a single mechanism, no explicit PCI is returned.

2) If all of the confidentiality mechanisms are not acceptable, the recipient rejects the SA by returning a status indicating the cause of rejection.

d) As a local decision, the recipient NLSP Entity will return the following PCI to the originator:

1) If the recipient accepts one of the proposed integrity mechanism, then it returns the selected mechanism. If the initiator proposed a single mechanism, no explicit PCI is returned.

2) If all of the integrity mechanisms are not acceptable, the recipient rejects the SA by returning a status indicating the cause of rejection.

e) Provided both a confidentiality and integrity mechanism have been selected, the KTE calculation is started and Key-Token-2 is sent.

In the CO case, if a PDU from the second exchange is not returned after a timeout, the SA is not established and no further attempts are made.

In the CL case, if a PDU from the second exchange is not returned after a timeout, the initiating NLSP entity re-transmits its first exchange PDU. Re-transmissions are limited to a finite number which is locally defined.

In the CL case, if the PDU from the first exchange is received again, the return PDU is resent.

C.6.2 Authentication and Security Negotiation (Second) Exchange

C.6.2.1 Receipt of First SA PDU by Initiator

On receipt of the first SA PDU, the initiating NLSP entity performs the following functions:

a) the received My_SA-ID is placed in the Your_SA-ID field of the generic header as described in 13.4;

b) the initiator certificate associated with the selected integrity mechanism is placed in Content Field Certificate;

c) the initiator generates Key-Token-3;

d) a list of proposed security services which could be used to protect the NLSP communication are placed in Content Field Service Selection;

e) a set of proposed labels which could be protected using this SA during NLSP communication are placed in Label_Def;

f) a set of key/ISN selections are placed in Key Selection;

g) the miscellaneous SA attributes required for this SA are placed in SA Flags;

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS Not for Resale

h) if SA establishment is to rekey an old SA, then Old Your SA-ID is set to the SA-ID for the old SA being rekeyed; if this process is carried out d), e) and g) above shall not be carried out;

i) protect SA contents as described in C.3.

In the CO case, if a PDU from the second exchange is not returned after a timeout, the SA is not established and no further attempts are made.

In the CL case, if a PDU from the second exchange is not returned after a timeout, the initiating NLSP entity re-transmits its second exchange PDU. Re-transmissions are limited to a finite number which is locally defined.

In the CL case, if the PDU from the first exchange is received again, the second exchange PDU is resent.

C.6.2.2 Receipt of the Second Exchange PDU by Recipient

Upon receipt of the second exchange PDU, the recipient NLSP entity performs the following functions and sends the following information to the initiator:

a) The received My_SA-ID is placed in the Your_SA-ID field of the generic header as described in 13.4.

b) The following items are checked. If any item fails its check, the SA is rejected and a Status field is returned indicating the cause of rejection:

   1) The received digital signature is checked to be valid.

   2) The received Key-Token-3 is checked to be valid.

   3) The set of proposed security services is checked to determine if any are acceptable. Only one of the proposed security services can be selected.

   4) The set of proposed labels is checked to determine if any are acceptable.

   5) The miscellaneous SA attributes are checked to determine if all are acceptable.

c) If Old Your SA-ID is present in the received PDU then the appropriate SA are copied from the referenced SA-ID. In this case use of fields described in c, d below cannot be sent.

Provided all the checks pass the following items are sent:

a) The initiator certificate associated with the selected integrity mechanism is sent.

b) The selected security services to be used to protect the NLSP communication are sent. If the set of proposed services contained one element, no PCI is returned.

c) The recipient generates Key-Token-4.

d) The selected subset of proposed labels which could be protected using this SA during NLSP communication is sent.

e) A set of key/ISN pointers are sent. If the initiator's proposed keys for the responder to use are acceptable, no new values is sent.

f) Protect SA contents as described in C.3.

In the CL case, if the PDU from the second exchange is received again, the recipient re-sends its second exchange PDU.

C.6.3 SA Release/Abort Exchange

C.6.3.1 Request to Initiate SA Release/Abort

The NLSP entity or local security management initiates the SA Release/Abort. The initiator of an SA Abort/Release need not be the initiator of the SA establishment.

a) If the local entity is the SA establishment initiator then Key-Token-3 is generated else Key-Token-4 is generated. In either case the generated token is placed in the SA contents.

b) The appropriate reason code is placed in SA Content field Abort/Release Reason.

c) Protect SA contents as described in C.3.

In the CO case, if a confirm PDU from the abort/release request is not returned after a timeout, the SA is not established and no further attempts are made.

In the CL case, if a confirm PDU from the abort/release exchange is not returned after a timeout, the initiating NLSP entity re-transmits its SA release/abort request PDU. Re-transmissions are limited to a finite number which is locally defined.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

C.6.3.2 Receipt of SA Abort/Release Request

Upon receipt of the SA Abort/Release Confirm PDU, the recipient NLSP entity performs the following functions and sends the following information to the initiator:

a) If the local entity is the SA establishment initiator then Key-Token-3 is generated else Key-Token-4 is generated. In either case the generated token is placed in the SA contents.

b) The appropriate reason code is placed in SA Content field Abort/Release Reason.

c) Protect SA contents as described in C.3.

In the CL case, if the PDU from the abort/release request is received again, the recipient re-sends its second exchange PDU up to a given limited number of times.

C.7 SA PDU – SA Contents

For this specific SA-Protocol, the format of the SA Contents field of the SA PDU defined in 13.4 is shown in Figure C.1.

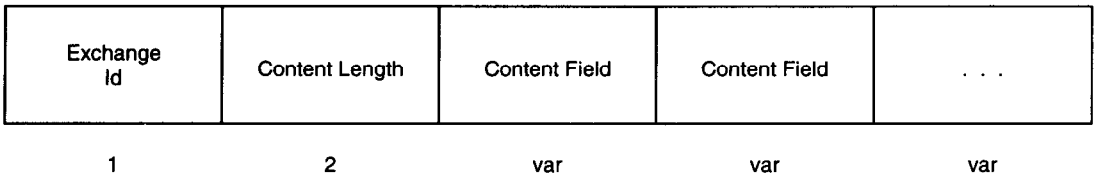


Figure C.1 – SA Contents

C.7.1 Exchange ID

This field contains a value of 00000000 if the PDU is associated with the first key token exchange and a value of 00000001 if the PDU is associated with the second Authentication/Negotiation Exchange. This field contains a value of 10000000 if the PDU is associated with a SA Abort/Release request 10000001 if the PDU is associated with an SA Abort/Release confirm.

C.7.2 Content Length

The length in octets of all Content fields but excluding the Content Length field.

C.7.3 Content Fields

The content field type encoding is defined in 13.2. The SA-P content fields (that is, A0-BF) used by the procedures in this annex are given below:

Value	*Content Field Type*
A0	My SA-ID
A1	Old Your SA-ID
A2	Key Token-1
A3	Key-Token-2
A4	Authentication digital signature
A5	Authentication certificate
A6	Service Selection
A7	SA Rejection Reason
A8	SA Abort/Release Reason
A9	Label-Def
AA	SA Flags
AB	Key Selection
AC	ASSR
AD	Key-Token-3
AE	Key-Token-4
AF-BF	Reserved for future use

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

NOTE – Further codes are reserved for private use in 13.2 in the main body of this ITU-T Recommendation | International Standard.

The Service Selection, SA Rejection Reason, Label-Def, SA Flags, and Key Selection Fields are optional within this specific SA-Protocol content definition.

C.7.3.1 My SA-ID

This mandatory field is used in the first exchange only. This parameter is the local identifier for a Security Association.

C.7.3.2 Old Your SA-ID

This field is used on the second exchange if attributes, other than keys, are to be inherited from the old SA.

C.7.3.3 Key-Token-1, Key-Token-2, Key-Token-3 and Key-Token-4

These mandatory fields are used to support the KTE and authentication as described earlier in this annex.

C.7.3.4 Authentication Digital Signature – Certificate

These mandatory fields are used to support the authentication as described earlier in this annex.

C.7.3.5 Service Selection

This optional field is used in both the first and second exchanges:

a) If used during the first exchange, it is used to identify proposed confidentiality and/or integrity mechanisms to be used during the second SA-Protocol exchange. In this case, only the first two octets are present.

b) If used during the second exchange, it is used to propose all mechanisms to be used during the NLSP communications protected by the SA being established.

This Field shall follow an occurrence of the ASSR parameter and may be included one or more times within either the first or second exchange PDU to form a proposed set of security services for negotiation. Each parameter relates to the immediately preceding ASSR parameter.

This parameter contains a sequence of octets indicating the levels of security services selected required. The semantics of the levels is defined as part of the security policy. The octets for each of the security services appear in the order indicated below. The sequence of octets can be truncated if the truncated octets all relate to the services that have the value 0. A single octet of value 255 indicates that security services selected have been pre-established.

Octet	*Meaning*
1	Connectionless Confidentiality/Connection Confidentiality
2	Connectionless Integrity/Connection Integrity without Recovery
3	Data Origin Authentication/Peer Entity Authentication
4	Access Control
5	Traffic Flow Confidentiality

C.7.3.6 SA Rejection Reason

This optional field may be present in either the first or second exchange PDU. It is present to indicate a rejection of the SA during its establishment. It contains the reason for rejection as follows:

Value	*Meaning*
1	Confidentiality Mechanism not supported
2	Integrity Mechanism not supported
3	Access Control Mechanism not supported
4	Authentication Mechanism not supported
5	Traffic Flow Confidentiality not supported
6	Confidentiality Mechanism rejected
7	Integrity Mechanism rejected
8	Access Control Mechanism rejected
9	Authentication Mechanism rejected
10	Traffic Flow Confidentiality rejected
11	Authentication signature invalid
12	Certificate invalid
13	Proposed Label set rejected

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

14	Retain_on_Disconnect rejected
15	Param_Prot rejected
16	No_Header rejected

C.7.3.7 SA Abort/Release Reason

This mandatory field is present in the SA Abort/Release request and indication. It is used to indicate the reason of an SA Abort release.

It is set to 0 for abort and 1 for normal release. Value 2 to 127 are reserved for future use. Other values can be used for privately defined reason codes.

C.7.3.8 Label-Def

This optional field is for use in the second exchange PDU only. The Label-Def Field may be included one or more times:

a) To propose a set of security labels if used by the originator. The initiator shall always use both sub-fields.

b) To select a subset of the proposed label set if used by the recipient. The recipient shall only use the Label_Ref sub-field.

The Label-Def Field is sub-divided into two sub-fields:

a) a two octet Label_Ref sub-field (value FF FF hex shall not be used as this is reserved for a NULL label reference);

b) a Label sub-field whose content is defined in 13.3.4.3.7.

The Label_Ref is a number associated with the security label defined in the Label sub-field. The Label_Ref is used in other PDUs as an alternative to carrying the associated security label.

C.7.3.9 Key Selection

This optional field is for use in the second exchange PDU only. It can occur any number of times within the SCI-Contents.

This field is sub-divided into three sub-fields:

a) Usage Flag (two octets);

b) Key Selection Information (two octets);

c) Key Reference (variable).

C.7.3.9.1 Usage Flags

This sub-field contains flags indicating the security purposes for which the key defined in the previous sub-field is to be used. The bits are encoded such that value 0 means FALSE: value 1 means TRUE. The key may be used for any combination of the following purposes. The allowable combinations will be dependant on the local security policy.

Bit No. Octet 1	*Service*	*Data*	*Data Source*
1	Confidentiality	Normal	SA Initiator
2	Confidentiality	Normal	SA Responder
3	Confidentiality	Expedited	SA Initiator
4	Confidentiality	Expedited	SA Responder
5	ICV Generation	Normal	SA Initiator
6	ICV Generation	Normal	SA Responder
7	ICV Generation	Expedited	SA Initiator
8	ICV Generation	Expedited	SA Responder

Bit No. Octet 2	*Service*	*Data*	*Data Source*
1	Authentication		SA Initiator
2	Authentication		SA Responder
3	ISN	Normal	SA Initiator
4	ISN	Normal	SA Responder
5	ISN	Expedited	SA Initiator
6	ISN	Expedited	SA Responder

The responder can override selections for its own use.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

C.7.3.9.2 Key Selection Information

This field indicates the position within the EKE resultant bit string where a selected key is to take its value. The length of the key is determined from the associated security services selected which identifies the associated algorithm. Multiple keys may use the same bit position (that is, the same key). The allowable combinations will be dependant on the local security policy.

C.7.3.9.3 Key Reference

This optional sub-field can be used to enable later reference to the key. This may be used for example for auditing purposes or for selection of a new key for a connection using the Connection Security Control PDU. The value of this reference shall be unique for the security association.

C.7.3.10 SA Flags

This optional field is for use in the second exchange PDU only. The following bit positions are used to signal the identified SA attributes. Value 0 means false; value 1 means true.

Bit	*SA Attribute*
1	Retain-on-Disconnect
2	Param_Prot
3	No_Header
4-8	Reserved for future use

Bits 4-8 are set to 0 on transmission and ignored on receipt.

C.7.3.11 ASSR

This field must be present if the Service Selection field is present. It is the object identifier (as defined in ISO/IEC 9834-3) which identifies the set of security rules which define the mechanisms to be applied given the protection quality of service selected.

This field may be present more than once, in which case the Service Selection parameters following each occurrence relate to the immediately preceding ASSR parameter.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex D

NLSP PICS Proforma [2)]

(This annex forms an integral part of this ITU-T Recommendation I International Standard)

D.1 Introduction

The supplier of a protocol implementation which is claimed to conform to this ITU-T Recommendation I International Standard shall complete the following Protocol Implementation Conformance Statement (PICS) proforma.

A completed PICS proforma is the PICS for the implementation in question. The PICS is a statement of which capabilities and options of the protocol have been implemented. The PICS can have a number of uses, including use:

- by the protocol implementor, as a check-list to reduce the risk of failure to conform to the standard through oversight;
- by the supplier and acquirer – or potential acquirer – of the implementation, stated relative to the common basis for understanding provided by the standard PICS proforma;
- by the user – or potential user – of the implementation, as a basis for initially checking the possibility of interworking with another implementation (note that, while interworking can never be guaranteed, failure to interwork can often be predicted from incompatible PICSs);
- by a protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

D.2 Abbreviations and Special Symbols

D.2.1 Status Symbols

M	Mandatory
O	Optional
O.<n>	Optional, but support of at least one of the group of options labelled by the same numeral <n> is required
X	Prohibited
<item>	Conditional-item symbol, dependent upon the support marked for <item> (see D.3.4)

D.2.2 General Abbreviations

N/A	Not applicable
PICS	Protocol Implementation Conformance Statement

D.3 Instructions for Completing the PICS Proforma

D.3.1 General Structure of the PICS Proforma

The first part of the PICS proforma – Identification and protocol summary – is to be completed as indicated with the information necessary to identify fully both the supplier and the implementation.

The main part of the PICS proforma is a fixed-format questionnaire divided into three major subclauses covering features common to NLSP-CL and NLSP-CO, followed by clauses specific to each of these two modes of operation; these are divided into further subclauses each containing a group of individual items. Answers to the questionnaire items are to be provided in the rightmost column, either by simply marking an answer to indicate a restricted choice (usually Yes or No), or by entering a value or a set or range of values. Note that there are some items where two or more choices from a set of possible answers can apply: all relevant choices are to be marked.

---

2) **Copyright release for PICS Proformas**

Users of this Recommendation I International Standard may freely reproduce the PICS proforma in this annex so that it can be used for its intended purpose and may further publish the completed PICS.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Each item is identified by an item reference in the first column; the second column contains the question to be answered; the third column contains the reference or references to the material that specifies the item in the main body of this ITU-T Recommendation | International Standard. The remaining columns record the status of the item – whether support is mandatory, optional, prohibited or conditional – and provide the space for the answers: see also D.3.4 below.

A supplier may also provide, or can be required to provide, further information, categorised as either Additional Information or Exception Information. When present, each kind of further information is to be provided in a further subclause of items labelled A<i> or X<i> respectively for cross-referencing purposes, where i is any unambiguous identification for the item (e.g. simply a numeral): there are no other restrictions on its format and presentation.

A completed PICS proforma, including any Additional Information and Exception Information, is the Protocol Implementation Conformance Statement for the implementation in question.

NOTE – Where an implementation is capable of being configured in more than one way according, for example, to the items in D.5.1, a single PICS may be able to describe all such configurations. However, the supplier has the choice of providing more than one PICS, each covering some subset of the implementation's configuration capabilities, in case that makes for easier and clearer presentation of the information.

D.3.2 Additional Information

Items of Additional Information allow a supplier to provide further information intended to assist the interpretation of the PICS. It is not intended or expected that a large quantity will be supplied, and a PICS can be considered complete without any such information. Examples might be an outline of the ways in which a (single) implementation can be set up to operate in a variety of environments and configurations; or a brief rationale – based perhaps upon specific application needs – for the exclusion of features which, although optional, are nonetheless commonly present in implementations of the network layer security protocol.

References to items of Additional Information may be entered next to any answer in the questionnaire, and may be included in items of Exception Information.

D.3.3 Exception Information

It may occasionally happen that a supplier will wish to answer an item with mandatory or prohibited status (after any conditions have been applied) in a way that conflicts with the indicated requirement. No pre-printed answer will be found in the Support column for this: instead, the supplier shall write the missing answer into the Support column, together with an X<i> reference to an item of Exception Information, and shall provide the appropriate rationale in the Exception item itself.

An implementation for which an Exception item is required in this way does not conform to ITU-T Recommendation | International Standard.

NOTE – A possible reason for the situation described above is that a defect in this ITU-T Recommendation | International Standard has been reported, a correction for which is expected to change the requirement not met by the implementation.

D.3.4 Conditional Status

The PICS proforma contains a number of conditional items. These are items for which both the applicability of the item itself, and its status if it does apply – mandatory, optional or prohibited – are dependent upon whether or not certain other items are supported.

Individual conditional items are indicated by a conditional symbol of the form <item>:<s> in the status column, where <item> is an item reference that appears in the first column of the table for some other item, and <s> is one of the status symbols M, O, O.n or X.

If the item referred to by the conditional symbol is supported, the conditional item is applicable, its status is given by <s> and the support column is to be completed in the usual way. Otherwise, the conditional item is not relevant and the Not applicable (N/A) answer is to be marked.

Each item whose reference is used in a conditional symbol is indicated by an asterisk in the Item column.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

D.4 Identification

D.4.1 Implementation Identification

Supplier	
Contact point for queries about the PICS	
Implementation Name(s) and Version(s)	
Other information necessary for full identification – e.g. name(s) and version(s) of machines and or operating systems; system names	

NOTES

1 Only the first three items are required for all implementations; other information may be completed as appropriate in meeting the requirement for full identification.

2 The terms Name and Version should be interpreted appropriately to correspond with the supplier's terminology (e.g. Type, Series, Model).

D.4.2 Protocol Summary

Identification of protocol specification	CCITT Recommendation X.273 (1994) | ISO/IEC 11577:—[1)]
Identification of amendments and corrigenda to this PICS proforma which have been completed as part of this PICS	CCITT Recommendation X.273 (1994) | ISO/IEC 11577:—[1)] Am. : Corr. : Am. : Corr. : Am. : Corr. : Am. : Corr. :

Have any exception items been required (see D.3.3)? NOTE – The answer **Yes** means that the implementation does not conform to this ITU-T Recommendation | International Standard.	Yes ☐	No ☐

Date of statement	

1) To be published.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

D.5 Features Common to NLSP-CO and NLSP-CL

D.5.1 Major Capabilities (Common)

Item	Questions/Features	Reference (subclause)	Status	Support
CO*	Is the connection-mode supported?	5.1	O.1	Yes ☐ No ☐
CL*	Is the connectionless-mode supported?	5.1	O.1	Yes ☐ No ☐
AC	Is Access Control supported?	5.2	O	Yes ☐ No ☐
TFC*	Is Traffic Flow Confidentiality supported?	5.2	O	Yes ☐ No ☐
ParamProt*	Is protection of all NLSP service parameters supported?	5.5.1a	O.2	Yes ☐ No ☐
UserDatProt	Is protection of NLSP Userdata supported?	5.5.1b	O.2	Yes ☐ No ☐
NoProt*	Is no protection supported?	5.5.1c	O	Yes ☐ No ☐
SdtBase*	Is any SDT PDU based encapsulation function supported?	5.5.3	CO:O.3 CL:M ParamProt:M	Yes ☐ No ☐
NoHead	Is any No Header encapsulation function supported?	5.5.3	CO:O.3 CL:X ParamProt:X	Yes ☐ No ☐ N/A ☐
SA-P*	Is any in-band SA-P supported?	5.4.1	O	Yes ☐ No ☐
LabMech*	Is the label mechanism supported?	6.2g, 6.4.1.1e, 6.4.2.1f	SdtBase:O	Yes ☐ No ☐ N/A ☐
SDTMech*	Is the standardised SDT PDU based encapsulation function supported?	11	SdtBase:O	Yes ☐ No ☐ N/A ☐
NoHeadMech	Is the standardised No Header encapsulation function supported?	12	NoHead:O	Yes ☐ No ☐ N/A ☐

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

D.5.2 PDUs (Common)

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on Receipt
SDT*	Is the Secure Data Transfer PDU supported on transmision/receive?	6.4.1.1 13.3	SdtBase:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SA*	Is the Security Association PDU supported on transmission/receive?	5.4.1, 13.4	SA-P:O	Yes ☐ N/A ☐	Yes ☐ N/A ☐

D.5.3 SDT PDU Fields Common to CO and CL and Generic to Mechanisms

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on Receipt
SdtPID	PID field value 10001011 in each SDT PDU	13.3.2.1	SDT:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SdtLI	Length Indicator field in each SDT PDU	13.3.2.2	SDT:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SdtPDUType	PDU Type field with value 01001000 in each SDT PDU	13.3.2.3	SDT:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SdtContLen	Content Length in each SDT PDU	13.3.4.1	SDT:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
DataType	Data Type field in each SDT PDU	13.3.4.2	SDT:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
UserData	Content field type CO – Userdata	13.3.4.3	SDT:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
CSAddr	Content field type C2 – Calling/Source NLSP address	13.3.4.3	ParamProt:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
CDAddr	Content field type C3 – Calling/Destination NLSP address	13.3.4.3	ParamProt:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
Label	Content field type C6 – Label	13.3.4.3	LabMech:O.4	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
LabRef	Content field type C7 – Label Reference	13.3.4.3	LabMech:O.4	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
LabelExc	Is the mutual exclusion of label and label reference in any SDT PDU enforced?	13.3.4.3	LabMech:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

D.5.4 SDT PDU Fields Common to CO and CL with Specific SDT Based Encapsulation Mechanisms

Item	Questions/Features	Reference (subclause)	Status (Note)	Support on Transmission	Support on Receipt
Synch	Crypto synchronisation	11.3, 13.3.3.1	O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
ICV	ICV field	11.3, 13.3.3.2	COInteg:M CLInteg:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
EncPad	Padding for Encipherment	11.3, 13.3.3.3	COConf:O CLConf:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
SeqNo	Sequence Number Content field	11.3, 13.3.5.1	COInteg:O CLInteg:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
SinglePad	Single octet general padding field	11.3, 13.3.5.2	O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
TFCPad	Traffic padding	11.3, 13.3.5.3	TFC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
IntegPad	Padding for Integrity	11.3, 13.3.5.4	COInteg:O CLInteg:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
NOTE – All the above fields are conditional on SDTMech selected.					

D.5.5 SA PDU Fields Generic to SA-P

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on Receipt
SaPID	PID field value 10001011 in each SA PDU	13.4.1	SA:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SaLI	Is the Length Indicator field transmitted in each SA PDU?	13.4.2	SA:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SaPDUType	PDU Type field with value 01001001 in each SA PDU	13.4.3	SA:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SaSA-ID	SA-ID field	13.4.4	SA:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SA-PType	SA-P Type field	13.4.5	SA:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SAKTE*	Is the example SA protocol using Key Token Exchange supported?	Annex C	SA:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

D.5.6 SA PDU Content Fields Specific to Key Token Exchange SA-P

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on Receipt
SAExchId	Exchange ID	C.7.1	SAKTE:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
ContLen	Is the Length Indicator field transmitted in each SA PDU?	C.7.2	SAKTE:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
MySA-ID	My SA-ID Content field	C.7.3.1	SAKTE:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
OldYrSA-ID	Old Your SA-ID Content field	C.7.3.2	SAKTE:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
KeyTokens	Key-Token-1, Key-Token-2, Key-Token-3 and Key-Token-4 Content fields	C.7.3.3	SAKTE:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
AuthFields	Authentication digital signature and Authentication certificate Content fields	C.7.3.4	SAKTE:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
ServSel*	Service Selection Content field	C.7.3.5	SAKTE:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
SARejReas	SA Rejection Reason Content field	C.7.3.6	SAKTE:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
SAAbReas	SA Abort/Release Reason Content field	C.7.3.7	SAKTE:M	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
LabDef	Label Definition Content field	C.7.3.8	SAKTE:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
KeySel*	Key Selection Content field	C.7.3.9	SAKTE:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
KeyUse	Usage Flags sub-field	C.7.3.9.1	KeySel:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
KeySelInfo	Key Selection Information sub-field	C.7.3.9.2	KeySel:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
KeyRefx	Key Reference sub-field	C.7.3.9.3	KeySel:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
SAFlags	SA Flags Content field	C.7.3.10	SAKTE:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
ASSR	ASSR Content field	C.7.3.11	ServSel:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

D.5.7 Algorithms Supported

Item	Questions/Features	Reference (subclause)	Status	Support
RegKTE	List of registered Key Token Exchange algorithms supported	–	O	Names: Object Identifers:
UnRegKTE	List the unregistered Exponential Key Exchange algorithms supported	–	O	Names:
RegICV	List the registered names of ICV algorithms supported	–	O	Names: Object Identifers:
UnRegICV	List the unregistered ICV algorithms supported	–	O	Names:
RegConf	List the registered names of Confidentiality algorithms supported	–	O	Names: Object Identifers:
UnRegConf	List the unregistered Confidentiality algorithms supported	–	O	Names:

D.6 Features Specific to NLSP-CL

D.6.1 Major Capabilities (NLSP-CL)

Item	Questions/Features	Reference (subclause)	Status	Support
CLConf*	Is connectionless confidentiality supported?	5.2	CL:O.5	Yes ☐ No ☐ N/A ☐
CLInteg*	Is connectionless integrity supported?	5.2	CL:O.5	Yes ☐ No ☐ N/A ☐
DOA	Is Data Origin Authentication supported?	5.2	CL:O.5	Yes ☐ No ☐ N/A ☐

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

D.6.2 Initiator/Responder (Connectionless Mode)

Item	Questions/Features	Reference (subclause)	Status	Support
CLXmtProt	Is the implementation capable of transmitting protected connectionless data units?	7.6	CL:O.6	Yes ☐ No ☐ N/A ☐
CLRcvProt	Is the implementation capable of accepting incoming protected connectionless data units?	7.7	CL:O.6	Yes ☐ No ☐ N/A ☐
CLXmt	Is the implementation capable of transmitting unprotected connectionless data units?	7.6.1	NoProt:M	Yes ☐ N/A ☐
CLRcv	Is the implementation capable of accepting incoming unprotected connectionless data units?	7.7.1	NoProt:M	Yes ☐ N/A ☐

D.6.3 Environment (Connectionless Mode)

Item	Questions/Features	Reference (subclause)	Status	Support
CL1	Are the mandatory elements of IS 8348 AD1 supported?	5.2	CL:M	Yes ☐ N/A ☐

D.6.4 SDT PDU Fields (Connectionless Mode)

Item	Questions/Features	Reference (subclause)	Status	Support
SdtSA-ID	SA-ID field transmitted in each SDT PDU?	13.3.2.4	CL:M	Yes ☐ N/A ☐

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

D.7 Features Specific to NLSP-CO

D.7.1 Major Capabilities (NLSP-CO)

Item	Questions/Features	Reference (subclause)	Status	Support
SNAcP	Is the protocol mapping directly onto CCITT Rec. X.25 | ISO/IEC 8208?	5.3, Annex B	CO:O.7	Yes ☐ No ☐
SNISP*	Is the protocol mapping onto CCITT Rec. X.213 | ISO/IEC 8348?	5.3, Annex A	CO:O.7	Yes ☐ No ☐
COConf*	Is connection confidentiality supported?	5.2	CO:O.8	Yes ☐ No ☐ N/A ☐
COInteg*	Is connection integrity without recovery supported?	5.2	CO:O.8	Yes ☐ No ☐ N/A ☐
PEA	Is peer entity authentication supported?	5.2	CO:O.8	Yes ☐ No ☐ N/A ☐
ExCSC*	Is Example CSC PDU procedures defined in NLSP supported?	10	CO:O	Yes ☐ No ☐ N/A ☐

D.7.2 PDUs (Connection Mode)

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on Receipt
CSC*	Connection Security Control PDU	8.5, 13.5	CO:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

D.7.3 Modes of Connection Establishment/Release

Item	Questions/Features	Reference (subclause)	Status	Support as Calling entity	Support as Called entity
UNConn	NLSP-CONNECT in UN-CONNECT	8.5.1.2	CO:O.9	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
UNConnSAP	NLSP-CONNECT in UN-CONNECT with SA-P	8.5.1.2	CO:O.9	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
UNData	NLSP-CONNECT in UN-DATA	8.5.1.2	CO:O.9	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
UNDataSAP	NLSP-CONNECT in UN-DATA with SA-P	8.5.1.2	CO:O.9	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
DUNDisc	NLSP-DISCONNECT in UN-DISCONNECT	8.10	CO:O.10	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
DUNData	NLSP-DISCONNECT in UN-DATA	8.10	CO:O.10	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐

D.7.4 Environment (Connection Mode)

Item	Questions/Features	Reference (subclause)	Status	Support
CO1	Are the mandatory elements of IS 8348 supported?	5.3	SNISP:M	Yes ☐ N/A ☐
ConOpt1	Does the implementation provide Expedited Data?	8.7	CO:O	Yes ☐ No ☐ N/A ☐
ConOpt3	Does the implementation provide Receipt Confirmation?	8.9	CO:O	Yes ☐ No ☐ N/A ☐

D.7.5 Timers and Parameters (Connection Mode)

Item	Questions/Features	Reference (subclause)	Status	Support
T1	Is the timer between transmitting NLSP-DISCONNECT and issuing UN-DISCONNECT supported?	8.10	CO:O	Yes ☐ No ☐ N/A ☐

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

D.7.6 SDT PDU Fields (Connection Mode)

Item	Questions/Features	Reference (subclause)	Status (Note)	Support on Transmission	Support on Recceipt
TestData	Content field type C1 – Testdata	13.3.4.3	O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
RAddr	Content field type C4 – Responding NLSP address	13.3.4.3	ParamProt:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
ConfReq	Content field type C8 – Confirmation Request	13.3.4.3	ParamProt:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
Reason	Content field type C9 – Disconnect Reason	13.3.4.3	ParamProt:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
NOTE – All the items in D.7.6 are conditional on SDT being supported.					

D.7.7 CSC PDU Fields – Generic (Connection Mode)

Item	Questions/Features	Reference (subclause)	Status	Support on Transmission	Support on Receipt
CscPID	PID field value 10001011 in each CSC PDU	13.5.1	CSC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
CscLI	Length Indicator field in each CSC PDU	13.5.2	CSC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
CscPTyp	PDU Type field with a value of xx111111 in each CSC PDU	13.5.3	CSC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
UNC-UNDFlg	Is the UNC-UND flag in PDU Type field transmitted in each CSC PDU?	13.5.3	CSC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
SA-PFlg	Is the SA-P flag in PDU Type field transmitted in each CSC PDU?	13.5.3c	CSC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐
CscSA-ID	SA-ID field	13.5.4	CSC:O	Yes ☐ No ☐ N/A ☐	Yes ☐ No ☐ N/A ☐
ContLen	Content Length field in each CSC PDU	13.5.5	CSC:M	Yes ☐ N/A ☐	Yes ☐ N/A ☐

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

D.7.8 Example CSC PDU Content (Connection Mode)

Item	Questions/Features	Reference (subclause)	Status	Support
CscInit	Is the implementation capable of initiating a CSC PDU exchange?	10.3	ExCSC:O.11	Yes ☐ No ☐ N/A ☐
CscResp	Is the implementation capable of responding to a peer initiated CSC PDU exchange?	10.3	ExCSC:O.11	Yes ☐ No ☐ N/A ☐
EncAuth	Enciphered AUTH-DATA field	13.5.7	ExCSC:M	Yes ☐ N/A ☐
KeyInfox	Key Information field	13.5.8	ExCSC:O	Yes ☐ No ☐ N/A ☐

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex E

Tutorial on some Basic Concepts of NLSP

(This annex does not form an integral part of this ITU-T Recommendation | International Standard)

E.1 Basis of Protection

The basis for protection of user data in NLSP is the Secure Data Transfer PDU (SDT PDU) or No_Header protection. The SDT PDU protects data by an encapsulation function which appends an Integrity Check Value (ICV) and then enciphers it for confidentiality. Padding fields can be placed with the protected data to support for traffic flow confidentiality and block ICV mechanisms. A separate padding field can be placed after the ICV for block encipherment mechanisms.

Before being protected in a SDT PDU additional security control information (e.g. label, sequence number) can be placed along with the user data, to produce the Octet-String-Before-Encapsulation. The Octet-String-Before-Encapsulation is then protected using an encapsulation function as described above. A clear header is placed at the front of the PDU to identify the PDU type and the set of "security attributes" (keys, etc. – see clause 5) used to protect the data unit. The building of an SDT PDU is illustrated in Figure E.1 below.

NLSP-CO supports a second, optional, approach to protecting NLSP Userdata called No_Header. With this approach the NLSP data is encrypted directly without the addition of any security control information or clear header.

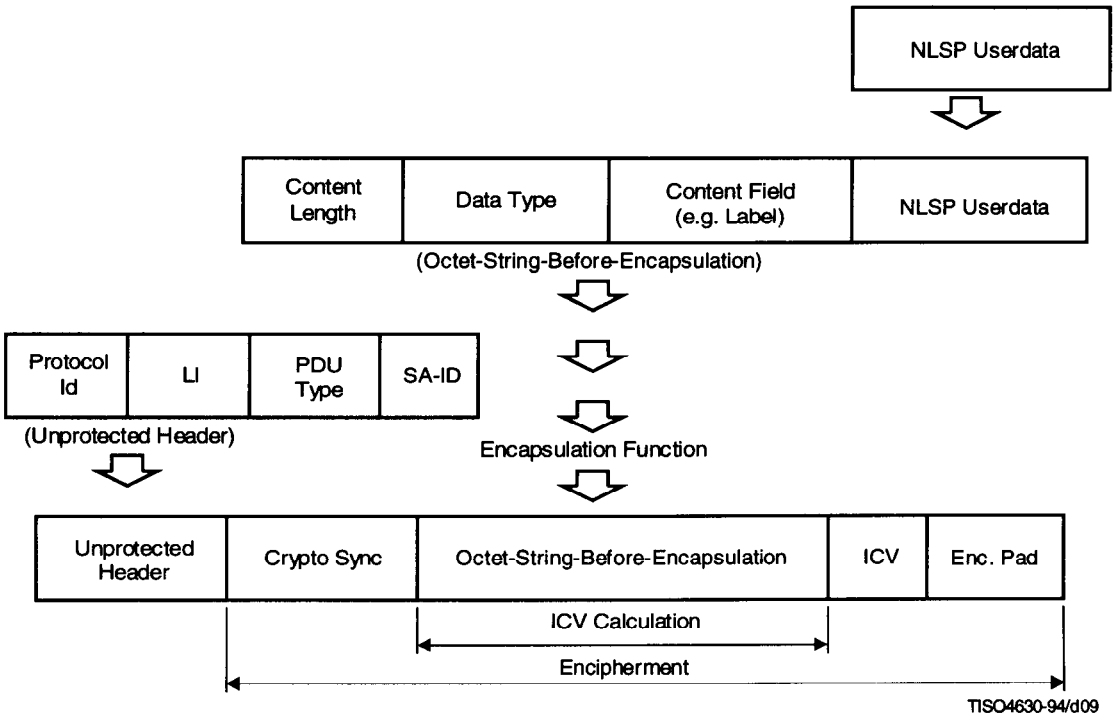


Figure E-1 – Building a Secure Data Transfer PDU

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

E.2 Underlying vs NLSP Service

NLSP has two notional service interfaces. One, called the NLSP service, is the interface provided to protocols "above" "NLSP" (i.e. protocols which makes use of the protected communications). The other, called the UN (Underlying Network) service, is used by NLSP to invoke the underlying communication protocols. NLSP may be added transparently without effecting the operation of protocols above and below NLSP. The NLSP interface mirrors the service expected by the protocols above and the UN service is mapped onto the form of service provided by the underlying protocols.

User data at the NLSP service interface, is protected (e.g. by encapsulating it in a SDT PDU) before it is passed down to the underlying UN service interface.

The NLSP and UN service interfaces are both similar to the OSI network service except in one major aspect. The entity served by the NLSP is not always the transport entity and the UN service never interfaces directly to a transport entity. As described later, in some cases (see Figure E.2) the NLSP service may interface to a relay and routing function within an intermediate system or even to an entity supporting a Network layer protocol (see Figures). With the UN service, from the point of the of the underlying protocols the service interface may appear as though it were the network service but from the view of the whole OSI stack it interfaces to an NLSP entity within the Network layer and hence it is not a pure OSI network service.

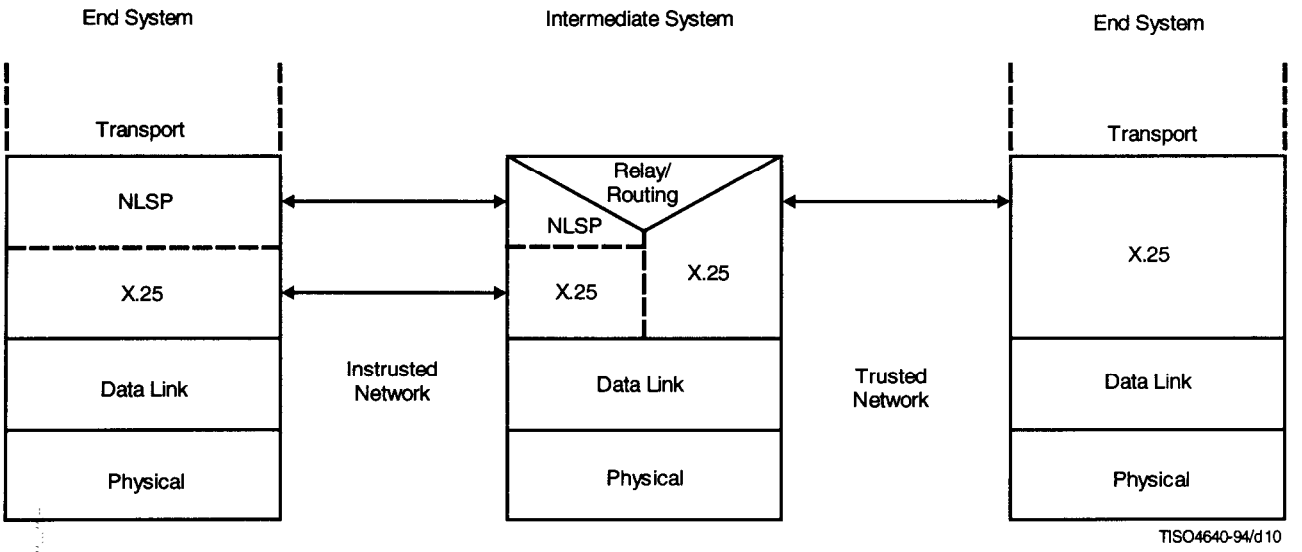
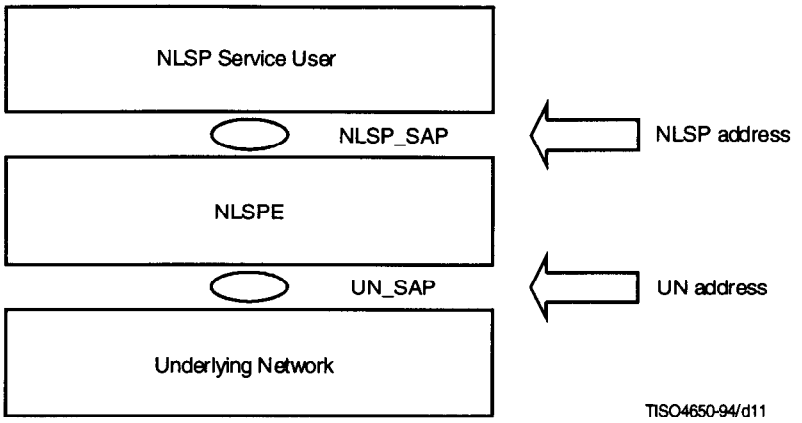


Figure E.2 – Illustration of NLSP-CO with an Intermediate System

E.3 NLSP Addressing

The NLSP entity (NLSPE) is embedded between the NLSP service user and the underlying network. The corresponding service access points are the NLSP_SAP and the UN_SAP. In configurations currently supported by NLSP (see Figure E.3-1 and Note) the address identifying the entity attached to the NLSP_SAP, e.g. NLSP service user is the NLSP address. The address identifying the entity attached to the UN_SAP, e.g. NLSPE is the UN address. Peer NLSPEs form a sublayer within the Network layer. The upper and lower boundaries are interaction points where addresses are exchanged. The following figure depicts service access points and the corresponding addresses.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale



NOTE – In configurations relaying CO-mode N-services, the NLSP address may identify a NSAP address in an end system rather than a NLSP_SAP in an intermediate system (see also E.4 and E.5).

Figure E.3-1 – Upper and lower SAPs and addresses

The NLSP is positioned inside the Network layer. It can be placed at the lower boundary, the upper boundary or somewhere in between. The NLSP and its lower UN service boundary act in different roles dependent on this placement. Similarly the addresses used have different semantics depending on this placement. Figure E.3-2 shows the possible placements of the NLSPE within the Network layer:

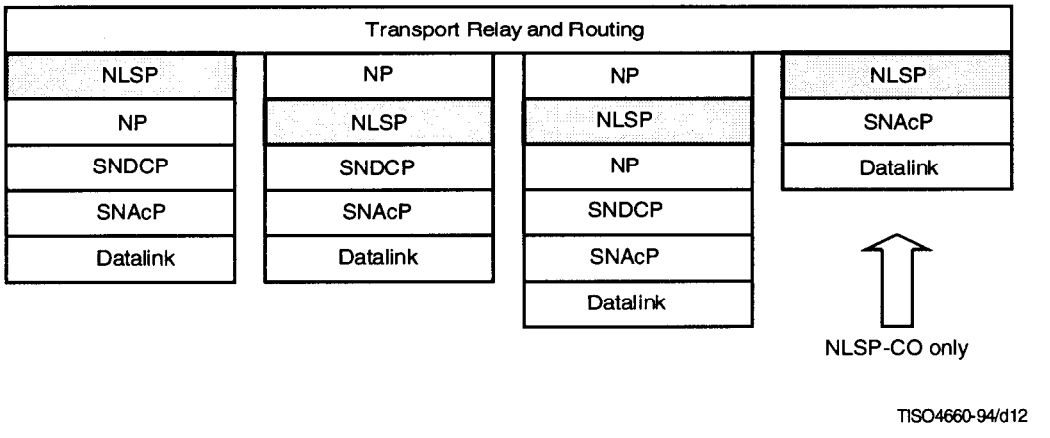


Figure E.3-2 – NLSP Placement in the Network layer

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Figures E.3-3 and E.3-4 identify the form of addresses used within the Network layer containing a NLSP sublayer in different placements.

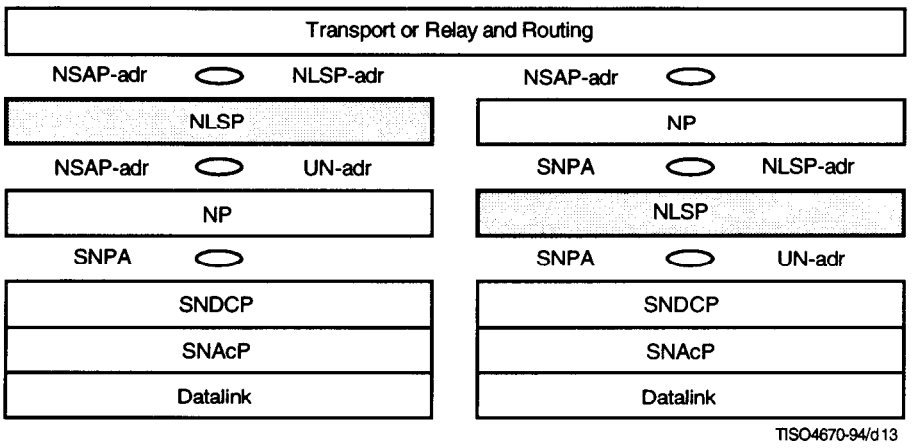


Figure E.3-3 – Addresses in a Network layer containing a NLSP sub-layer – With one Network Protocol (NP) above and below NLSP

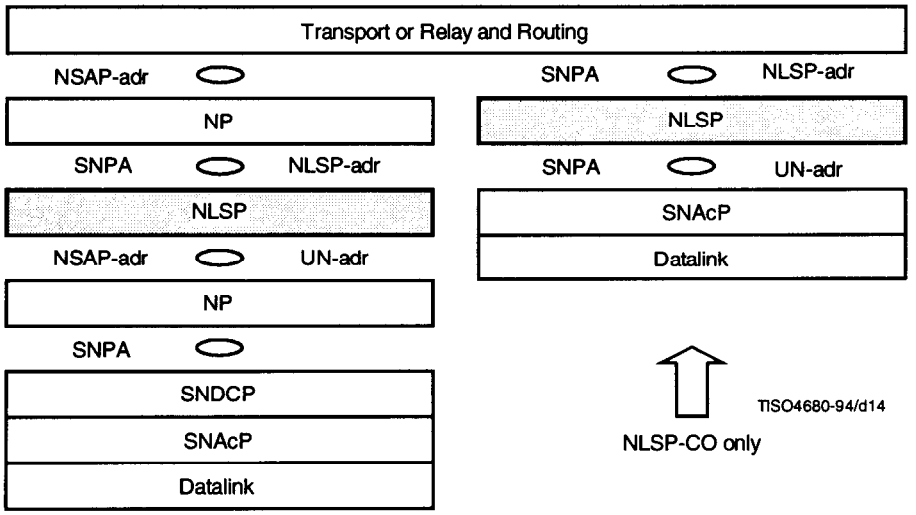


Figure E.3-4 – Addresses in a Network layer containing a NLSP sub-layer – With Network Protocol (NP) above and below NLSP – No Network Protocol

The NSAP`-adr (UN-adr) is used by the NLSP for addressing within an underlying network in cases where a Network protocol (connection or connectionless mode) lies under the NLSP sublayer. NSAP` addresses form an encapsulated addressing domain enclosed by the NLSP sublayer. The NSAP` addresses have an identical syntax as NSAP addresses and are registered using the NSAP address registration procedure. NSAP addresses forming a trusted network domain are used only within a domain protected by NLSP sublayers.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

The SNPA` may be identical to the SNPA determined by the NP-entity above. However, the SNPA` address may be different according to the location of the peer NLSPE.

The encapsulated addressing domain can be regarded as a virtual subnetwork within an OSIE. It is bounded by a group of NLSP entities either in ES or IS each having an identical N-layer stack above the technology-dependent subnetwork protocols (SNAcP, Subnetwork Network Dependent Convergence Protocol). These NLSPEs therefore all have the same placement within the network layer.

Figure E.3-5 shows a possible scenario of an OSIE containing a virtual UN enclosed by NLSP entities within ESs and ISs:

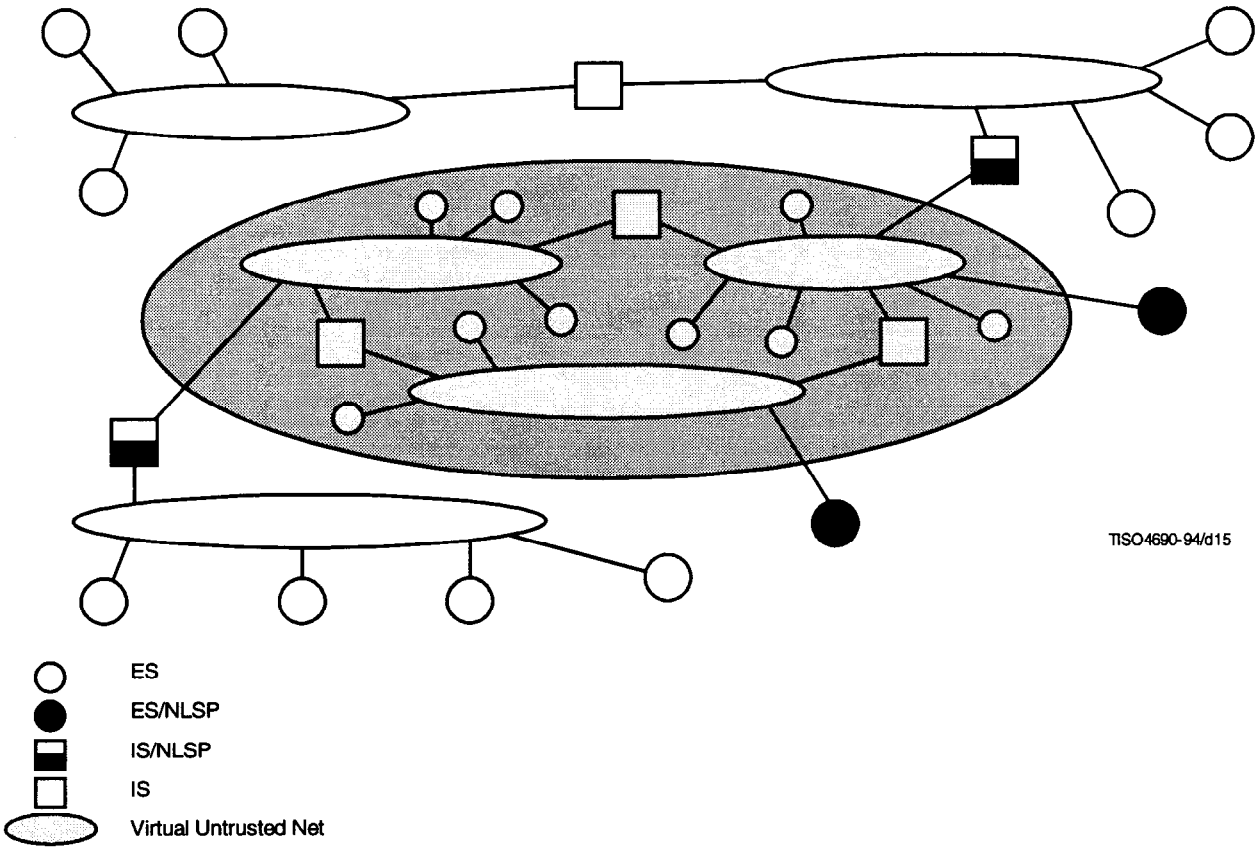


Figure E.3-5 – Virtual UN within an OSIE

The Network layer protocol stacks and the placement of the NLSP entities depends of the protocols used within the subnetworks and their configuration. The selection process takes place by an "authority" defining a static configuration of a combination of trusted and untrusted networks. This requires additional secure management and routing functions which are outside of the scope of this ITU-T Recommendation | International Standard.

Depending on the placement of the NLSPE inside the Network layer, the NLSP address and the UN address have different semantics. Conceptually, two placements are differentiated (see Figure E.3-6).

- *Placement A* – The NLSP_SAP corresponds to the OSI NSAP. The user of the NLSP service is a transport entity. The address identifying the transport entity is defined as NSAP address and is identical with the NLSP address.

  The underlying network is regarded as an unprotected network domain, which is in fact the OSI network. The address identifying the NLSPE corresponds therefore to the OSI NSAP address. However, the parameters transferred in service primitives via the NLSP_SAP and UN_SAP boundaries can be different if NLSP service parameters are protected (Param_Prot is TRUE).

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

– *Placement B* – The NLSPE is placed between two network sublayers. The sublayer on top delineates a protected network domain, whereas the underlying subnetwork represents an unprotected network domain.

Within an end system, the NSAP address identifies different network service users collocated in the end system. The NLSP address identifies the end system routing entity which is responsible for the ES routing functions.

Within an intermediate system, the NSAP address contains routing information for the relaying of NPDUs within the protected network domain. The NLSP address identifies the ES/IS routing entity within the IS. The UN address identifies the NLSPE attached to the UN.

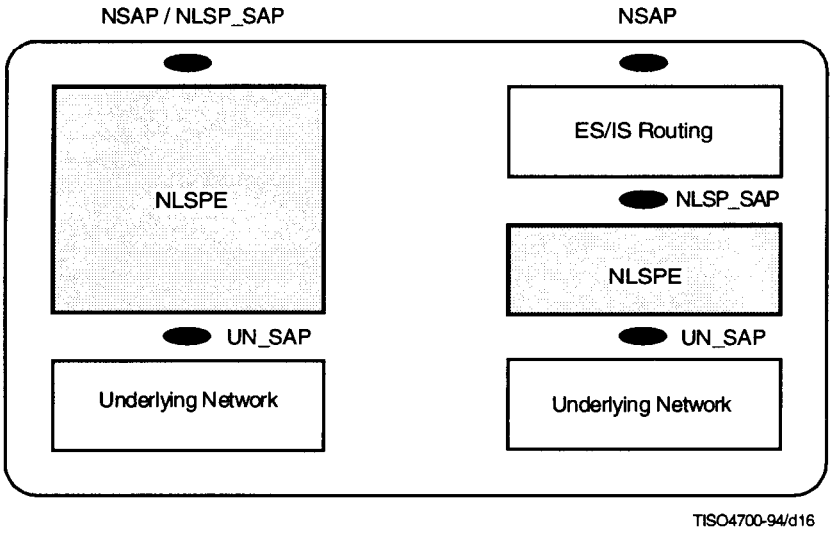


Figure E.3-6 – Placements of the NLSPE in the Network layer

The NLSP address(es) served by a remote NLSPE is held in a SA attribute Adr_Served. UN address of a remote NLSPE is held in SA attribute Peer_Adr.

– if Param_Prot is FALSE

The NLSP functions are limited to the mapping of service primitives from the NLSP_SAP to UN_SAP. The NSAP address is directly mapped into the UN address. NLSP SA attribute Adr_Served holds the same value as SA attribute Peer_Adr.

– if Param_Prot is TRUE

Protected mode – Address mappings are dependent on the placement of the NLSPE and are provided through use of attributes Adr_Served and Peer_Adr.

Table E.1 includes the address mapping functions of the NLSPE depending on their various placements and the correspondence between Peer_Adr and Adr_Served attributes. Table E.1 covers destination addresses only.

E.4 Connection Mode NLSP

E.4.1 Basic Operation

Most of the complexity of NLSP is related to the handling of connection establishment for connection mode communications.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Table E.1

Placement	Param_Prot	NLSP address	UN address	NLSP vs UN address
A	FALSE	NSAP address	NSAP address	Same
A	TRUE	NSAP address	Peer UN address	Different
B: End system	FALSE	NLSP address (Note)	Peer UN address	Same
B: End system	TRUE	NLSP address (Note)	Peer UN address	Different
B: Intermediate system	FALSE	NLSP address (Note)	Peer UN address	Same
B: Intermediate system	TRUE	NLSP address (Note)	Peer UN address	Different
NOTE – The mapping from NLSP address to or from NSAP address is the concern of routing functions relating to the protocol above the NLSP.				

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 and in-band SA-P, 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 on the UN connection, the exchange of CSC PDUs is also used to:

a) establish mechanism specific security attributes for use in protecting the connection (for example, keys, integrity sequence numbers);

b) perform peer entity authentication.

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.

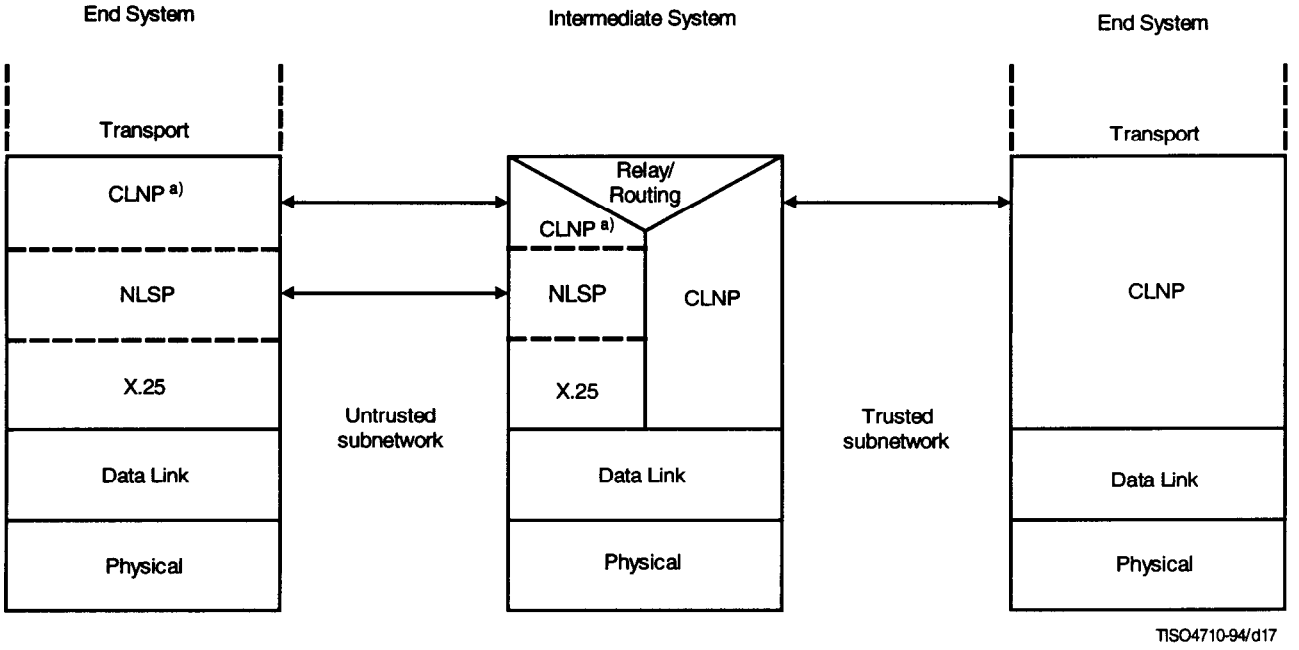
If NLSP-CONNECT parameters are required to be protected, they will either be encapsulated in an SDT PDU or encrypted (No_Header selected) before transfer.

Once a connection has been established, user data is protected by encapsulating it in a SDT PDU or if the No_Header mode is selected by just encrypting the NLSP Userdata.

E.4.2 Placement

Connection mode NLSP may be placed at various locations within the Network layer. It provides to the NLSP user either an OSI network service interface (in this case the user corresponds to a transport entity) or, if the user is an additional network protocol entity (e.g. ITU-T Recommendation X.233 | ISO/IEC 8473-1 CLNP), the service corresponds to a subnetwork interface. The interface below NLSP is virtually identical to the OSI network service excepting that the service user is NLSP instead of the transport service and the service can operate in either an end system or intermediate system. The protocol operating below NLSP operates as though it were operating between two end systems providing the OSI network service, although with regards to the overall picture it may only be operating with an intermediate system and does not directly interface to the transport service. The operation of NLSP-CO with an intermediate system and end to end is illustrated in Figures E.4-1, E.4-2, E4-3 and E.4-4. Other placements of NLSP may be possible.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale



a) This includes convergence function to CO mode.

Figure E.4-1 – Illustration of NLSP within an Multi-network Environment

E.4.3 NLSP/UN Service Interface Mapping

In an end system the NLSP service interface maps directly onto the OSI network service.

Two forms of UN service mapping are supported. In one, the UN service interface maps onto the equivalent to the OSI network service with the CSC PDU carried in the UN Connect user data field. The other maps directly onto Recommendation X.25 as defined in CCITT Recommendation X.223 | ISO/IEC 8878 except that the CSC PDU is carried in the X.25 protection facilities field.

E.4.4 Addressing

The addresses used at the NLSP service interface are OSI network service NSAP addresses if NLSP is operating at the top of the network layer, or SNPA addresses if operating below another network layer protocol such as CLNP. If there is address hiding (i.e. Param_Prot is FALSE), then the addresses at the UN service interface are the same as those at the NLSP service interface.

If addresses hiding is provided (i.e. Param_Prot is TRUE) the addresses used at the UN service interface (UN addresses) are of the same form as the NLSP addresses (e.g. in case of the NLSP address being an NSAP address structured according to CCITT Recommendation X.213 | ISO/IEC 8348), however, they are used to identify NLSP entities which may lie within an intermediate or end system. These UN addresses can be managed in the same way as NSAP addresses. The same registration schemes can be used to allocate addresses and the same routing protocols can be used to manage routing. However, they are in isolated routing domains. The mapping from NSAP address to UN address is handled by NLSP using the Adr-served security association attribute to identify the NSAP address served by the UN addresses held in the Peer_Adr security association attribute.

E.5 Connectionless Mode NLSP

E.5.1 Basic Operation

The protection for NLSP-CL is provided simply by encapsulating user data in a SDT PDU.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

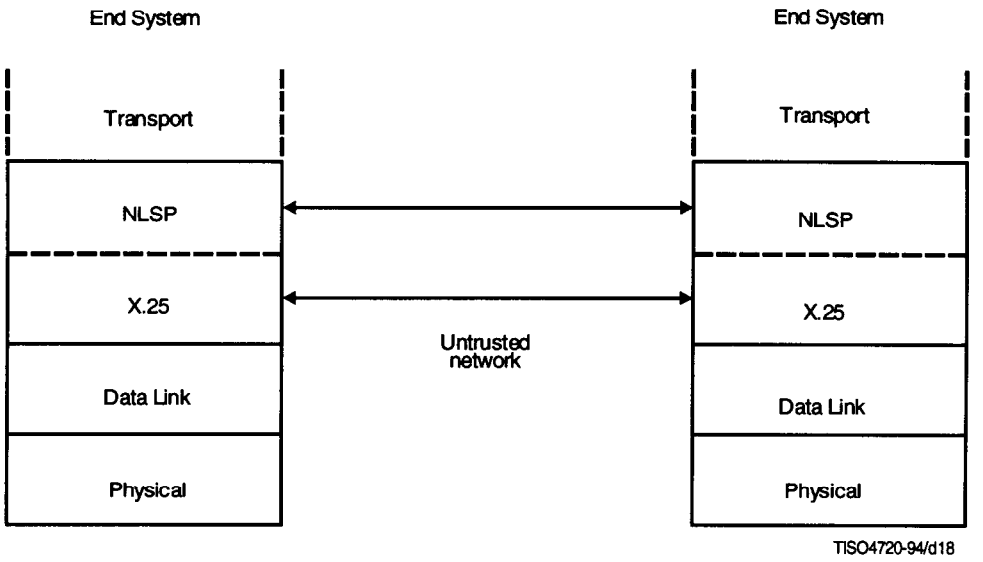


Figure E.4-2 – Illustration of NLSP-CO between End Systems

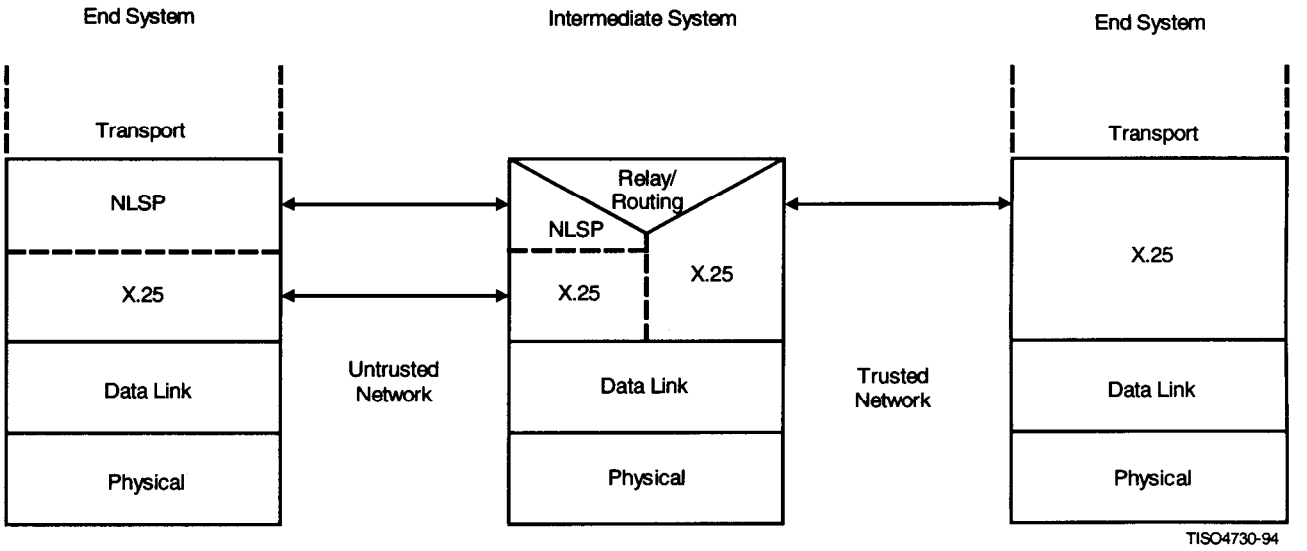


Figure E.4-3 – NLSP-CO with an Untrusted Network

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

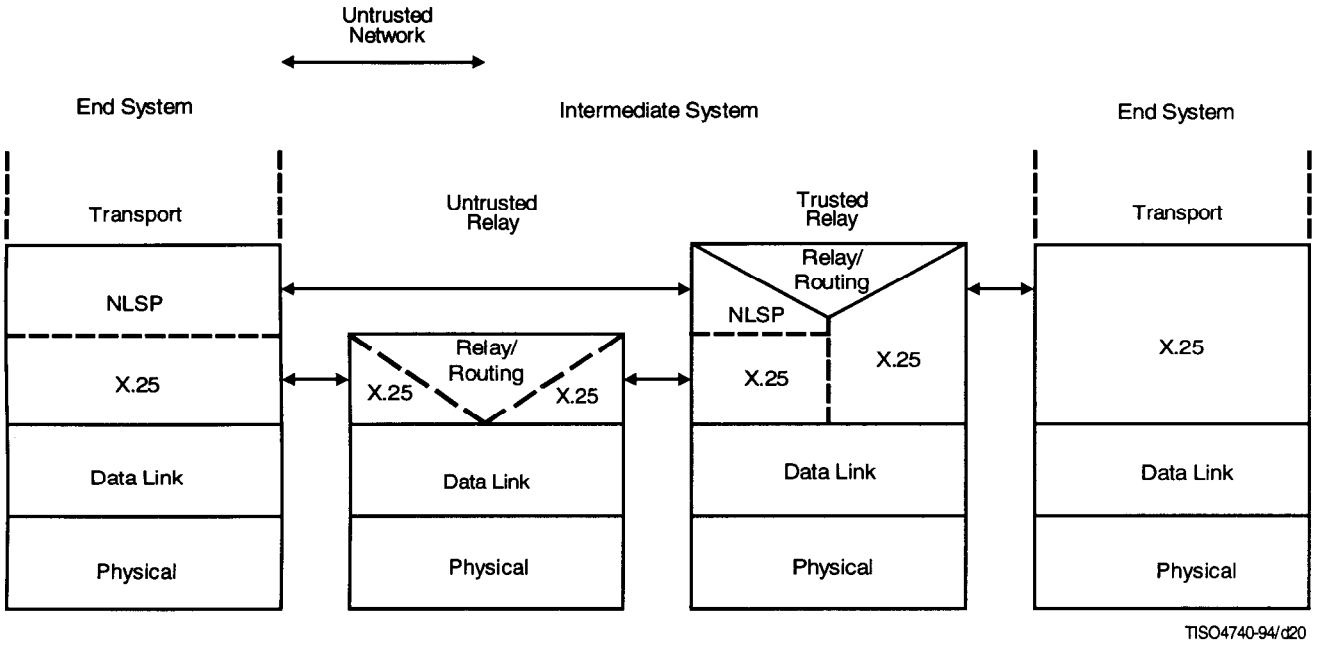


Figure E.4-4 – Illustration of NLSP-CO with Untrusted Relay System

E.5.2 Placement

NLSP for connectionless mode can operate either:

a) at the top of the network layer, encapsulating NSDUs in a SDT PDU before being handled by the Connectionless Network Protocol (ITU-T Recommendation X.233 | ISO/IEC 8473-1) (see Figure E.5-1). This stack can only be used between two end systems; or

b) below the connectionless network protocol encapsulating connectionless protocol PDUs before they are mapped onto the underlying subnetwork (see Figure E.5-2). This stack is for use in conjunction with "trusted" relay intermediate systems, or end to end where there are no network relays between two communicating systems; or

c) operating under one ITU-T Recommendation X.233 | ISO/IEC 8473-1 (CLNP) protocol layer for the "trusted"/"red" domain and mapping onto another CLNP protocol layer for the "untrusted"/"black" domain. This stack is the most flexible and can operate in any environment. "Trusted" intermediate systems relay the upper CLNP protocol after removing the security protection provided by NLSP. Other "untrusted" relay systems relay on the lower CLNP protocol passing NLSP protected data through transparently (see Figure E.5-3).

NOTE 1 – The representation of two ITU-T Recommendation X.233 | ISO/IEC 8473-1 layers and an NLSP layer does not necessarily imply separate protocol machines. This depends on the local implementation policy.

NOTE 2 – The existence of two CLNP protocol layers does not necessarily imply the existence of separate implementations.

E.5.3 NLSP/UN Service Interface Mapping

In the case of NLSP operating at the top of the network layer, the NLSP service interface is identical to the OSI network service and the UN service interface is the same except that it interfaces to an NLSP entity rather than the transport service.

In the second case of NLSP operating below CLNP, the NLSP service interface is equivalent to the service provided by a subnetwork operating below CLNP and the UN service is the same as the subnetwork service.

In the final case, the interface above NLSP looks to the CLNP protocol above as though it were a subnetwork. The UN interface appears to the CLNP protocol below as though it were the OSI network service.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

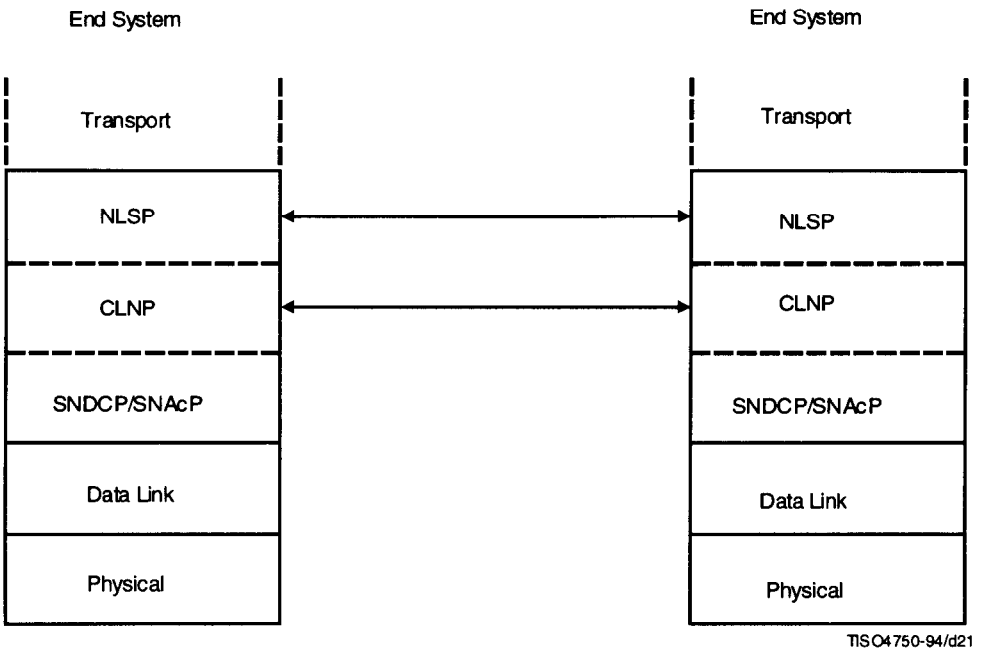


Figure E.5-1 – Illustration of NLSP-CL between End Systems

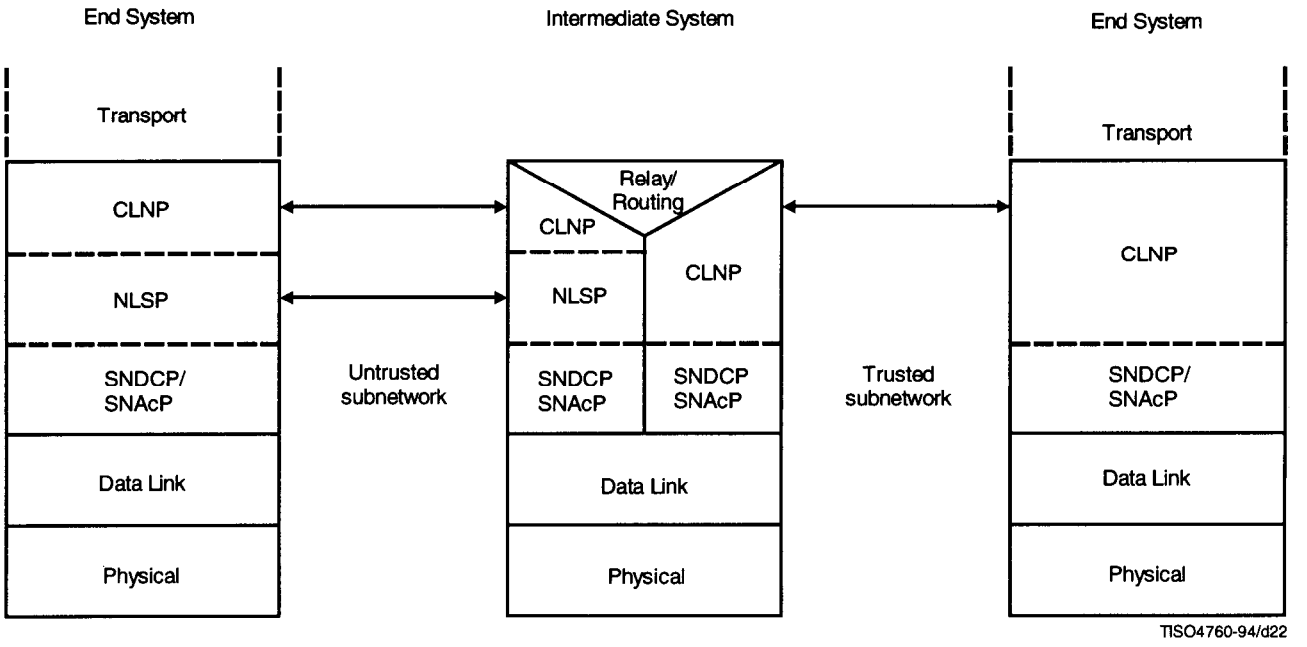


Figure E.5-2 – Illustration of NLSP-CL with Untrusted Subnetwork

--`,,```,,,,````-`-`,,`,,`,`,,`---
Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

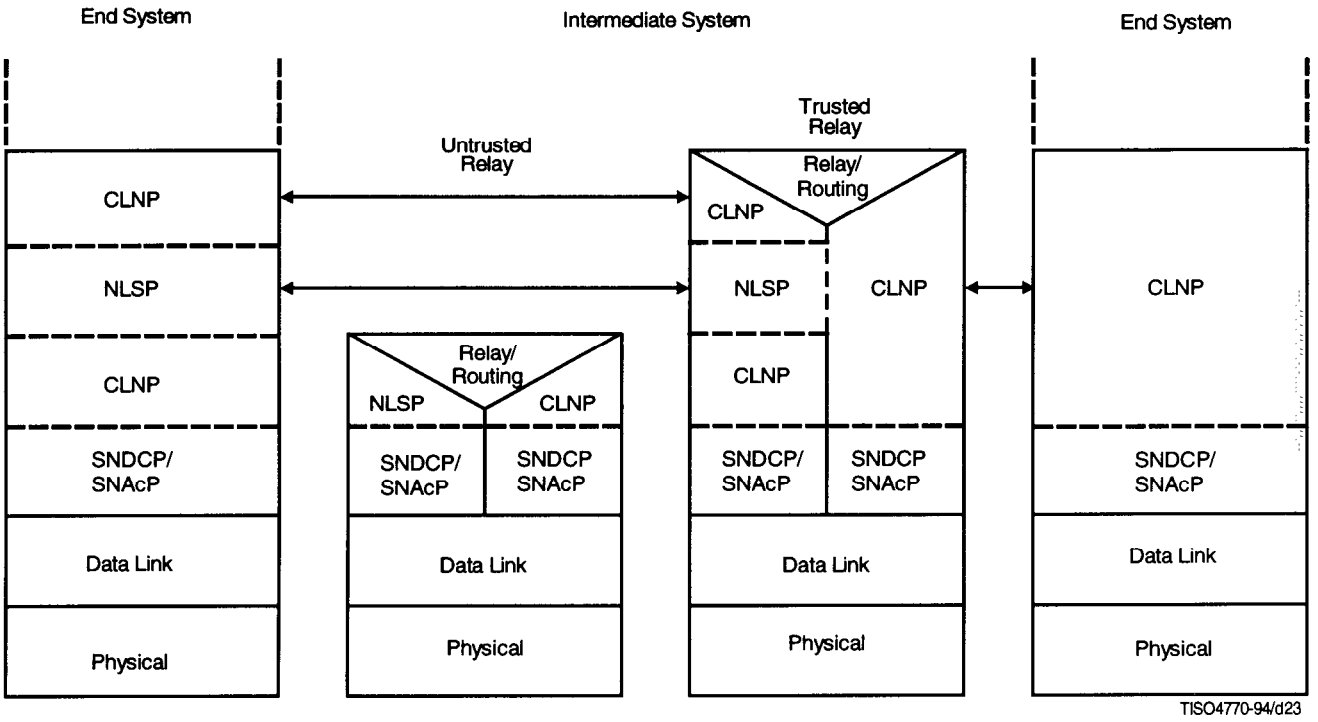


Figure E.5-3 – Illustration of NLSP-CL with Untrusted Relay System

E.5.4 Addressing

In the case of NLSP operating at the top of the network layer, the address used by NLSP is an OSI network NSAP address. In the case of NLSP operating below ITU-T Recommendation X.233 | ISO/IEC 8473-1 (CLNP) before it is mapped onto the underlying subnetwork, the address used at the interface above and below NLSP is a subnetwork address (e.g. Local Area Network MAC Address). In the case of NLSP operating between two layers of CLNP, the address passed down to the NLSP entity is a subnetwork address.

If there is address hiding (i.e. Param_Prot is FALSE), then the addresses at the UN service interface are the same as those at the NLSP service interface.

If addresses hiding is provided (i.e. Param_Prot is TRUE) the addresses used at the UN service interface (UN addresses) are of the same form as the NLSP addresses, however, they are used to identify NLSP entities which may lie within an intermediate or end system. These UN addresses can be managed in the same way as NSAP addresses. The same registration schemes can be used to allocate addresses and the same routing protocols can be used to manage routing. However, they are in isolated routing domains. The mapping from NSAP address to UN address is handled by NLSP using the Adr-served security association attribute to identify the NSAP address served by the UN addresses held in the Peer_adr security association attribute.

E.5.5 Segmentation

Segmentation and reassembly are handled by ITU-T Recommendation X.233 | ISO/IEC 8473-1 (CLNP). Segmentation can take place before and after NLSP processing depending on the underlying subnetworks that the PDU has crossed. If segmentation takes place before NLSP then each segment is NLSP encapsulated, forwarded to the NLSP decapsulation device, decapsulated and then reassembled by CLNP. If segmentation takes place after NLSP, then CLNP will first reassemble the segments. The complete PDU will be decapsulated by NLSP. CLNP will then deliver the decapsulated PDU to the destination address indicated via normal communication protocols.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

E.6 Security Attributes and Associations

Both NLSP-CO and NLSP-CL require a set of corresponding attributes, called security association attributes, for secure communications to take place. These include:

a) basic "policy" related information which defines or constrains the operation of NLSP, e.g. encipherment algorithm, encipherment block size, integrity sequence number length, label defining authority;

b) initial values needed to control the operation of NLSP, e.g. master keys, initial integrity sequence numbers;

c) the current values needed to control the operation of NLSP: working key for a specific connection, current integrity sequence number.

The existence of a collection of corresponding attributes is called a Security Association. The set of attributes used for protecting a connectionless PDU or a connection is referenced by a Security Association Identifier.

The first set of "policy" related information is called an "Agreed Set of Security Rules" (ASSR). It is suggested that this is established through registration.

The second set of initial control information can either be establish, out-of-band using either a local management interface or OSI management, or in-band using a protocol which operates in conjunction with NLSP called the "Security Association Establishment Protocol".

The third set of information is updated as part of the operation of basic NLSP protocol. For example, working keys can be established in NLSP-CO through the exchange of Connection Security Control PDUs; current integrity sequence numbers are updated on each Secure Data Transfer PDU.

E.7 Dynamic Functional Relationship between NLSP and CLNP

E.7.1 Introduction

Subclause E.5.2 describes the relationship of NLSP and CLNP for an instance of communication. The aim of this clause is to demonstrate the flexibility of NLSP used in conjunction with CLNP to support both protected and unprotected communications independent of the communications architecture.

Figure E.7-1 depicts the flow of data in and out of these combined protocols. The following text describes this data flow and the communication parameters required for this.

E.7.2 SN-UNITDATA Indication

a) On a SN-UNITDATA indication (1) [ITU-T Recommendation X.233 | ISO/IEC 8473-1 (CLNP) (see 5.5)] the protocol identifier (PID) in the first octet (or if addressing is used to identify the protocol the address) is checked to identify if the first part of the PDU contains a CLNP or NLSP header (2).

b) If the first header identifies CLNP, then a decision is made based on the destination address in the CLNP Header (3). If the destination address is recognised as one of this system's own end system address, then the CLNP PDU is sent to the re-assembly process (4) [CLNP (see 6.8)]. If this is not one of the end system's addresses, then the CLNP Header is processed for forwarding (8) as described in E.6.4.

c) If the first header identifies NLSP, then the subnetwork service parameters and user data are processed by NLSP as UN-UNITDATA. The resultant NLSP-UNITDATA user indication is then checked to see if the first octet is a CLNP PID (8). If it is, NLSP-UNITDATA is processed as in b) above (3), otherwise the NLSP-UNITDATA indication is mapped onto N-UNITDATA indication (7).

d) After CLNP re-assembly (if required) (4) another decision is required (5). If the CLNP PDU contains an NLSP PDU (i.e. the first octet contains the NLSP PID), then the CLNP service parameters and user data are processed by NLSP as UN-UNITDATA indication (6), otherwise it is mapped directly onto a N-UNITDATA indication (7). The resultant NLSP-UNITDATA user indication is then checked to see if the first octet is a CLNP PID (8) (or if addressing is used to identify the protocol the address is checked). If it is, NLSP-UNITDATA is processed as in b) above (3), otherwise the NLSP-UNITDATA indication is mapped onto N-UNITDATA indication (7).

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

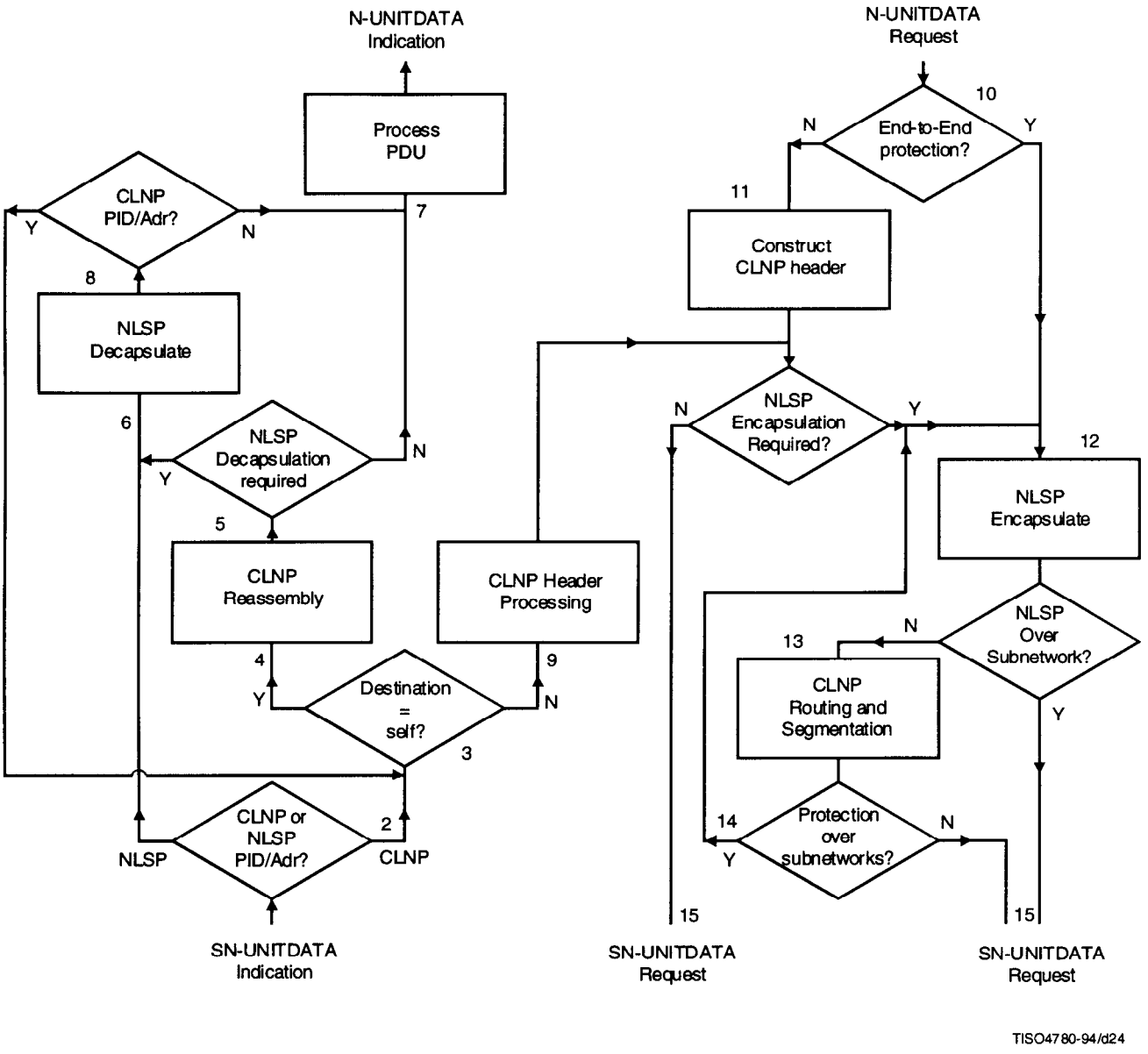


Figure E.7-1 – Flow Chart of NLSP with CLNP

E.7.3 N-UNITDATA Request

a) Upon a N-UNITDATA request (10), depending on the service parameters (e.g. source, destination address) and local security policy, the request is either directly mapped onto CLNP (see 5.4) (11) or mapped onto an NLSP-UNITDATA request and processed accordingly (12).

b) If the N-UNITDATA is processed by CLNP (11), the resulting CLNP PDU is either mapped directly onto a SN-UNITDATA request (15) or onto a NLSP-UNITDATA request (10) for processing by NLSP.

c) If the N-UNITDATA or a CLNP PDU is processed by NLSP (12), the resulting UN-UNITDATA request is either mapped directly onto the SN-UNITDATA request (15) or onto CLNP for processing as if it were a N-UNITDATA (13) depending the service parameters and local security policy. Following the CLNP processing further NLSP protection may be provided if additional protection is required over the subnetwork (14), otherwise the CLNP PDU is mapped onto SN-UNITDATA.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

E.7.4 Forwarding of CLNP PDU

The decision to protect a forwarded CLNP PDU is based on information in the CLNP PDU header and user data, as well as the local security policy. If protection is required, the CLNP PDU is mapped onto a NLSP-UNITDATA request for processing by NLSP (12). Depending the service parameters and local security policy requirements, the resulting protected UN-UNITDATA is either mapped directly onto a SN-UNITDATA request [CLNP (see 6.5)] (15) or onto CLNP for processing as if it were N-UNITDATA (13) depending the service parameters and local security policy requirements.

E.7.5 CLNP NLSP-CL Interface Recapitulation

The preceding subclauses show the functional relationship between NLSP-CL and CLNP. For reasons of simplicity the operation of these protocols are shown as distinct separated by service interfaces. The operation of the two protocols may be implemented as a single layer 3 protocol combining the functionality of the CLNP and NLSP protocol machines.

E.8 Dynamic Functionality Related to Layered Model

The layered approach to describing NLSP can related to the flow chart description for the example configuration given in Figure E.7-2 as follows:

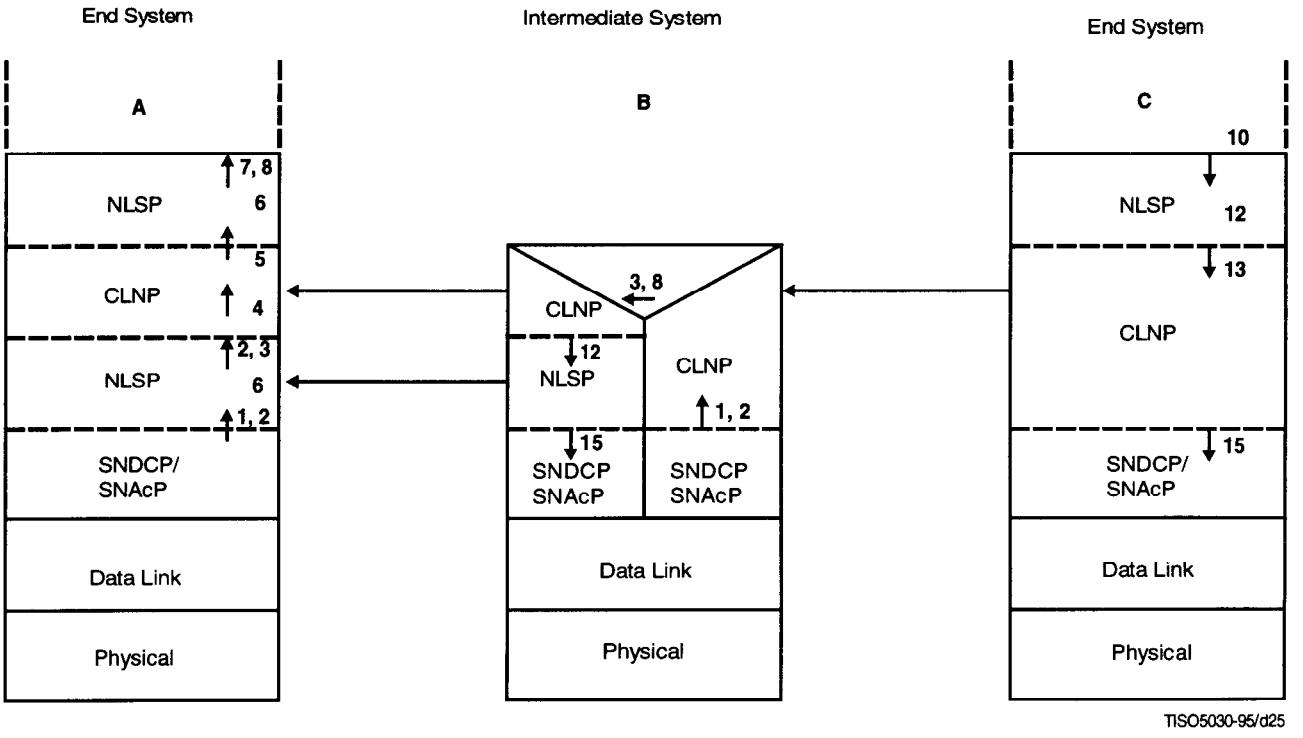


Figure E.7-2 – Layered Model Related to Flow Chart

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Action	Flow chart reference
In End System A	
SN-UNITDATA indication in End System C	1
Check if CLNP or NLSP	2
Check if destination is local	3
CLNP re-assembly	4
Check if NLSP	5
Map onto UN-UNITDATA and NLSP decapsulate	6
Map onto N-UNITDATA indication	7
Check if CLNP	8
In Intermediate System B	
SN-UNITDATA indication in Intermediate System B	1
Check if CLNP or NLSP	2
Check if destination is local	3
Process CLNP for forwarding	8
Map onto NLSP-UNITDATA and NLSP encapsulate	12
Map UN-UNITDATA onto SN-UNITDATA request	15
In End System C	
N-UNITDATA request in End System A	10
Map onto NLSP-UNITDATA and NLSP encapsulate	12
Map UN-UNITDATA onto CLNP for processing as N-UNITDATA	13
Map CLNP PDU on SN-UNITDATA request	15

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex F

Example of an Agreed Set of Security Rules

(This annex does not form an integral part of this ITU-T Recommendation | International Standard)

An Agreed Set of Security Rules (ASSR) establish the security mechanisms to be used including all parameters needed to define the operation of the mechanism for a given the security services selected. This annex gives an example of how values on SA attributes that may be established by an ASSR might be written out on a proforma.

ASSR-ID **XYZ(Object identifier)** -- *This gives the object reference used in the SA-P.*

SA-ID_Length **4**

Security services selected Definition Module -- *This indicates the security services that might be supported under the security rules and gives names to the levels of protection that are supported using different algorithms, key lengths, etc.*

PE Auth:	**none,**	**low,**	**high**
AC:	**none,**	**low,**	**high**
Confid:	**none,**	**low,**	**high**
Integ:	**none,**	**low,**	**high**

Security Label Mapping -- *This maps the security label to security service selections.*

Label_Def_Auth XYZ

Label->Sensitivity = Unclass
implies:
PE Auth none, AC none, Confid none, Integ none

Label-Sensitivity = Confidential
implies:
PE Auth low, AC low, Confid low, Integ none

Label-Sensitivity = Secret
implies:
PE Auth high, AC high, Confid high, Integ high

Param_Prot TRUE -- *This selects what levels of protection requires protection of all service parameters.*

For Security services selected: Integ = high or Conf = high

Mechanism Module – Security labels for Access Control
For Security services selected: AC = high or Conf = high
-- *This indicates what security service selection requires security labels.*

Label_Def_Auth XYZ
(Note this must be the same as Auth for protection QOS labels)

Explicit indication Yes

Mechanism Module – Integrity Check Value
For security service selection: Integ > none or PE Auth = High or Mechanism Security Labels

ICV_Alg XYZ
Rekey after 10 000 PDUs
Key distrib mechanism Asymmetric

Mechanism Module – Integrity Sequence Number
For security services selected: Integ = high or Auth = High
ISN_Len 8 octets total
Sequence Number 4 octets
incremented by 1
Timestamp 4 octets
milliseconds from sync point
Receive ISN Window Discard previous sequence #.
Timestamp should be within 2*maximum
variation in network
delay. If outside
window then a replay attack.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Mechanism Module – Encipherment

For security services selected: Conf > low

Enc_Alg_ID	**XYZ**
Mode Chained	
Enc_Blk	**8 octets**
key exchange info	**(e.g. Prime p, Generator a)**
Rekey after	**1 000 PDUs**
Key distrib mechanism	**Asymmetric**

Mechanism Module – No Header

For security services selected: Conf = low and Integ = none and not Label mechanism

Mechanism Module – Connection Authentication

For security services selected: AC > Low or PE Auth > Low

Enc_Alg_ID XYZ

Mechanism Module – Asymmetric Key Distribution

For mechanism encipherment or Integrity check value

Enc_Alg RSA

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex G

Security Associations and Attributes

(This annex does not form an integral part of this ITU-T Recommendation | International Standard)

In order to protect an instance of communication (a connectionless SDU or a connection) a collection of information (keys and other attributes needed to control the operation of security) has to be established between the communicating entities. This collection of information is referred to as a Security Association (SA).

The information forming an SA is either static information, which may be "customised" when the SA is established and then remains fixed for the duration of the association, or dynamic information which may be updated during the lifetime of a security association.

An SA may be established either out-of-band or, for NLSP-CO, in-band by the exchange of SA PDUs. When the in-band method is used, specific mechanisms for realising the SA-P may be as defined in this ITU-T Recommendation | International Standard or may be private mechanisms.

Prior to establishing an SA each NLSP entity must have pre-established:

a) A common set of security rules which, given a security services selected, specify the security mechanisms to be used, including all parameters needed to define the operation of the mechanisms (e.g. algorithm, key length, key lifetime). These security rules are mutually agreed to and uniquely identified by communicating entities. Security rules and their identifiers may be registered by third parties. See Annex F for an example set of security rules.

b) The security services, and hence the security mechanisms, that may be used.

If the in-band method of establishing an SA is to be used, the following must be pre-established:

c) An initial security services selected, and hence the security mechanisms, to be applied in establishing an SA.

d) Basic keying information needed to establish an SA.

On SA establishment, an NLSP entity establishes the following shared information with its remote peer:

e) Local and remote SA-IDs.

f) Security services to be used between the associated entities for instances of communication.

g) The mechanisms and their parameters as implied through the security services selected.

h) Initial shared keys for integrity, encipherment mechanisms and authentication of an instance of communication.

i) The set of security labels and addresses that may be used on this association for access control.

The SA-References and shared keys [items e) and h) above] must be established on a per association basis. The other information may be pre-established and common to several associations. In addition, as part of establishing a customised SA the identity of the remote peer must be authenticated. Annex C defines a mechanism which can be used for key distribution and authentication.

The following information can be dynamically updated for an instance of communication:

j) Integrity sequence number(s) as needed for normal and expedited data in each direction.

k) A security label.

l) Re-key information for the encipherment/integrity mechanisms.

To achieve authentication, authentication mechanisms need to be applied to each instance of communication.

The different SA attributes that may be established at the different stages of a security association are illustrated in Figure G-1.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Pre-established	Static	Dynamic
Range of security services selected Initial security services selected Basic key information Agreed set of security rules	Initial keys SA-ID Authentication Security label	ISN Authentication SA-ID Re-key information
Selected security services Selected mechanisms Security label set/address set		

Figure G.1 – Illustration of 3 tiers of Security Association

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

Annex H

Example Key Token Exchange – EKE Algorithm

(This annex does not form an integral part of this ITU-T Recommendation | International Standard)

The following is an example of a key token exchange algorithm which may be used with the security association protocol defined in Annex C.

There are two parameters required for EKE. One is a large prime number p (such that p 1 has a large prime factor) and the other is a number "a" which is in the range $1 < a < p - 1$.

Let A and B be the two communicating parties (see Figure H.1). EKE begins with A selecting a large random number X, and B selecting a large random number Y. A then calculates (a**X mod p) and sends a, p, and (a**X mod p) to B, and B calculates (a**Y mod p) and sends it to A. Both A and B calculate (a**XY mod P). An eavesdropper only sees (a**X mod p) and (a**Y mod p). An eavesdropper cannot determine X or Y and, therefore, cannot calculate (a**XY mod p).

A and B may subsequently use subsets of the bits in (a**XY mod P) as keys and as information to counter replay attacks on the second exchange.

The values described in SA protocol defined in Annex C are:

- The shared KTE bit string is (a**XY mod P).
- Key-Token-1 is a, p, (a**X mod P) where the 'a', 'p', and (a**X mod P) are encoded as an concatenated octet strings.
- Key-Token-2 is (a**Y mod P).
- Key-Token-3 is information derived from the shared KTE bit string (a**XY mod P) to counter replay attacks.
- Key-Token-4 is information derived from the shared KTE bit string (a**XY mod P) to counter replay attacks.

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

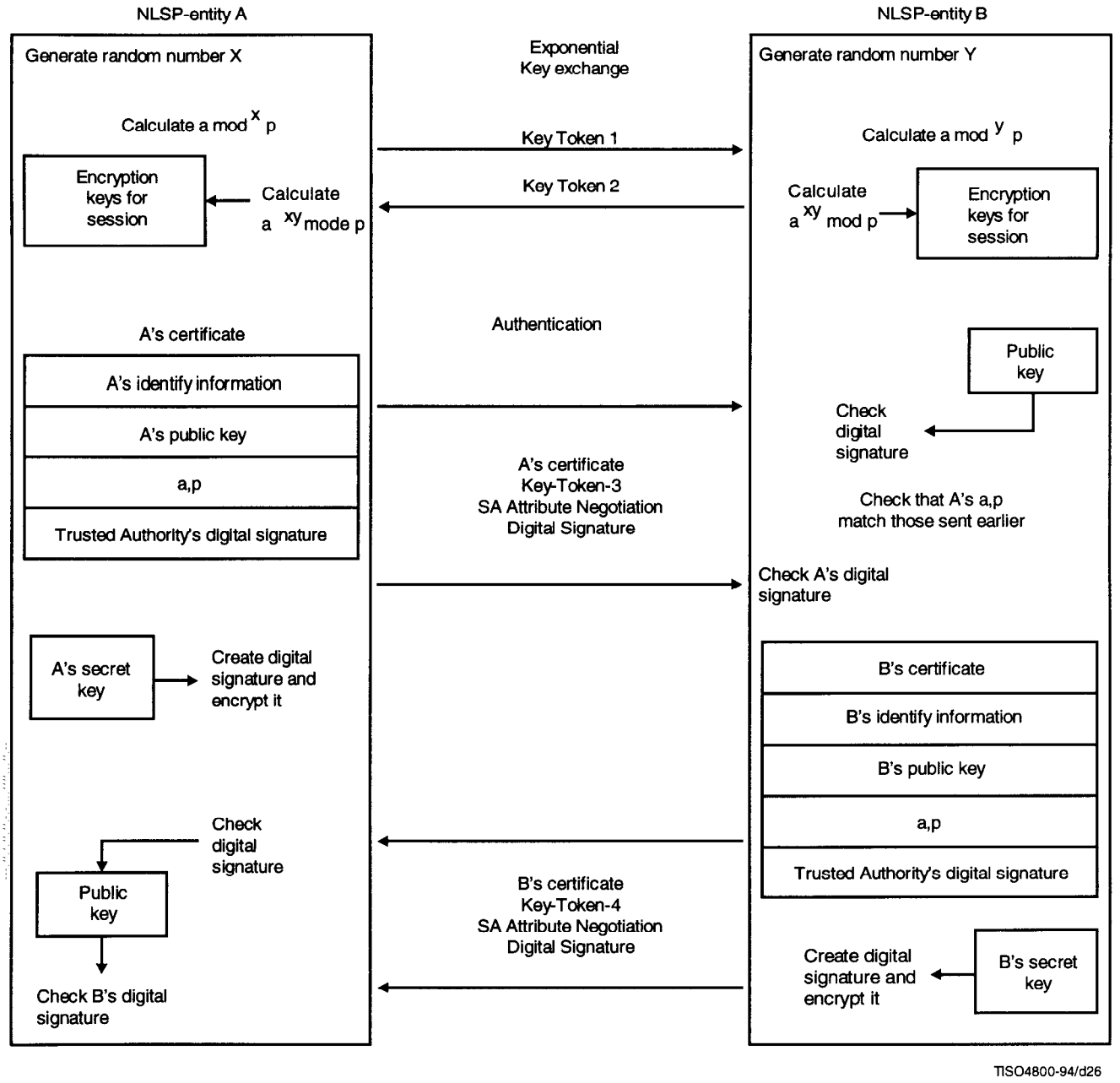


Figure H.1 – Illustration of On-line Key Derivation and Derivation using EKE

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS
Not for Resale

© ISO/IEC

ICS 35.100.30

Descriptors: data processing, information interchange, telecommunications, network interconnection, data transmission, network layer, security techniques, protocols.

Price based on 108 pages

Copyright International Organization for Standardization
Provided by IHS under license with ISO
No reproduction or networking permitted without license from IHS

Not for Resale