SDNS
Secure Data
Network Systems

Security Protocol 4
(SP4)

Forward:

The SDNS architecture, and its associated specifications, were developed as a cooperative project between government and industry. The project was sponsored by the National Security Agency, and supported by the National Institute of Standards and Technology (formerly the National Bureau of Standards) and the Defense Communications Agency. Twelve leading U.S. companies in computers and telecommunications made significant contributions of their technical talents and development resources. The combined efforts of these organizations produced the basis for improved security technology, interoperable security standards, and cost-effective security for computers and telecommunications.

Introductory note:

This document provides the framework for the SDNS Security Protocol at layer four (SP4). This document is being circulated for comment and approval. It is subject to change during the development phase of SDNS.

TABLE OF CONTENTS

0 INTRODUCTION

The transport protocol specified in International Standard (ISO) 8073 provides the connection oriented transport service described in ISO 8072. The transport protocol specified in ISO 8602 provides the connectionless-mode transport service described in ISO 8072/DAD1. This document specifies optional extensions to ISO 8073 and ISO 8602 permitting the use of cryptographic techniques to provide data protection for transport connections or for connectionless-mode TPDU transmission.

ISO 8072 describes Transport Connection (TC) protection as the prevention of unauthorized monitoring or manipulation of Transport Service (TS) user data. The TS users specify TC protection qualitatively by selecting one of four TC protection quality of service options during the TC establishment phase:

a) no protection features;
b) protection against passive monitoring;
c) protection against modification, replay, addition or deletion;
d) both b and c.

DP 7498/2 on OSI Security Architecture uses the following terms for these security services:

a) no security services;
b) connection/connectionless confidentiality;
c) connection/connectionless integrity (with or without recovery); and
d) both connection/connectionless confidentiality and integrity.

The two subclasses of SP4 are distinguished on the basis of the granularity of cryptographic associations that are established. They are:

1. SP4C: Connection oriented protection in which each transport connection is individually protected with a different cryptographic key; can provide full connection integrity and confidentiality.

2. SP4E: End system to end system protection in which all connections between a pair of end systems are protected with the same cryptographic key; can provide connectionless integrity and confidentiality.

Table 1S summarizes the connectionless and connection-oriented security services provided when SP4 is used with a connection-oriented transport protocol.Table 2S

	Connectionless - SP4E	Connection-oriented - SP4C
Confidentiality	prevent cleartext disclosure	prevent cleartext disclosure
Integrity	detect TPDU modification	detect TPDU modification, replay, addition, or deletion

Table 1S: Security Services Available in Conjunction with ISO 8073

summarizes the connectionless security services provided when SP4 is used with a connectionless transport protocol.

	Connectionless
Confidentiality	prevent cleartext disclosure
Integrity	detect TPDU modification

Table 2S: Security Services Available in Conjunction with ISO 8602

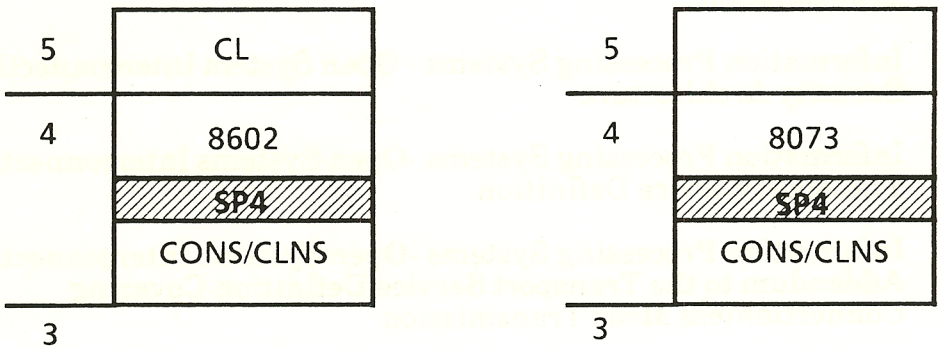
This document specifies protocol extensions for providing confidentiality and integrity data protection, including:

a) procedures incorporating cryptographic techniques in protocol processing,

b)the minimum characteristics of cryptographic algorithms with which these procedures can be used.

c) the structure and encoding of data units necessary to achieve interoperability.

The following figures show the location of SP4 in the seven layer ISO model.



1 SCOPE AND FIELD OF APPLICATION

The procedures specified in this document operate as extensions to those defined in ISO 8073 and ISO 8602 and do not preclude unprotected communication between transport entities implementing ISO 8073 or ISO 8602.

The degree of protection achieved will depend upon proper management of cryptographic keys. The procedures in this document assume that:

a) storage for cryptographic keys is available;

b) both the sending and receiving transport entities have the same cryptographic key available (i.e., symetric key for data protection use);

c) cryptographic keys are pairwise (i.e., shared only between two end-systems for data protection).

This document does not define how the cryptographic keys are created, updated or otherwise managed.

This protocol can support the access control service described in ISO 7498/2 using security labeling and using attributes associated with cryptographic keys. This protocol can support the peer entity authentication and data origin authentication services described in ISO 7498/2 using attributes associated with cryptographic keys.

NOTE

The security label function provides access control enforcement (see section 6.5).

2 REFERENCES

ISO 7498	Information Processing Systems -Open Systems Interconnection - Basic Reference Model
ISO 7498/AD1	Information Processing Systems -Open Systems Interconnection - Basic Reference Model - Addendum 1: Connectionless Mode Transmission
ISO 7498-2	Information Processing Systems - Open System Interconnection - Security Architecture
ISO 8072	Information Processing Systems -Open Systems Interconnection - Transport Service Definition
ISO 8072/AD1	Information Processing Systems -Open Systems Interconnection - Addendum to the Transport Service Definition Covering Connectionless Mode Transmission
ISO 8073	Information Processing Systems -Open Systems Interconnection - Transport Protocol Specification
ISO 8602	Information Processing Systems -Open Systems Interconnection - Protocol for Providing the Connectionless-Mode Transport Service

3 DEFINITIONS

This document is based on the concepts developed in the Reference Model for Open Systems Interconnection (ISO 7498) including ISO 7498/2 on Security Architecture, and makes use of the following terms defined in the ISO 7498/2:

a) access control

b) ciphertext

c) cleartext

d) confidentiality

e) data integrity

f) data origin authentication

g) denial of service

h) end-to-end encipherment

i) key

j) key management

Additionally, this document uses the following definitions:

a) cryptographic association: a state between two entities which share a pairwise key. The entities associate common attributes with the key.

b) cryptoperiod: length of time or amount of information that a key is good.

c) pairwise key: a key generated for two specific transport entities and unavailable to any other users.

d) reflection protection: to detect that a message has been sent back.

4 SYMBOLS AND ABBREVIATIONS

This Addendum makes use of the following abbreviations from Clause 4 of ISO 8073:

CR TPDU	Connection request TPDU
DC TPDU	Disconnect confirm TPDU
DR TPDU	Disconnect request TPDU
DST-REF	Destination reference (field)
DT TPDU	Data TPDU
ED TPDU	Expedited Data TPDU
ED-TPDU-NRED	TPDU number (field)
ER TPDU	Error TPDU

LI	length indicator (field)
NSAP	Network service access point
SRC-REF	Source Reference (field)
TPDU	Transport protocol data unit
TPDU-NR	DT TPDU number (field)

Additionally, the following abbreviations are used in this Addendum:

FSN	Final Sequence Number (field)
ICV	Integrity Check Value
KEY-ID	Key Identifier
LABEL	Security Label
LME	Layer Management Entity
NSDU	Network Service Data Unit
PAD	Padding (field)
SE TPDU	Security Encapsulation TPDU

5 OVERVIEW OF THE PROTOCOL

5.1 Transport Security Services

The specific SP4 processing options used in an instance of communications are determined by the attributes associated with the pairwise cryptographic key. SP4 assumes that two transport entities using the same pairwise key will associate identical sets of attributes with that key. Thekey identifier, KEY_ID, points to the appropriate set of attributes for the pairwise key.

The following paragraphs define these attributes and list the defined mnemonics used to refer to the attributes in this specificaition. Note that the selections under each attribute are mutually exclusive - only one can be active for each cryptographic association.

- KEY GRANULARITY

A SP4 entity shall support one or more of the following key granularities:

kg_tc	A separate cryptographic key is used for each transport connection
kg_esp	A separate cryptographic key is used for each end system pair.
kg_esp_sr	a separate cryptographic key is used for each end system pair and security level set

- CONFIDENTIALITY

The confidentiality attribute specifies whether a confidentiality service is to be provided with this cryptographic key for the cryptographic association.

conf_yes	confidentiality is to be provided
conf_no	confidentiality is not to be provided

- CONFIDENTIALITY ALGORITHM

This attribute identifies the algorithm to be used, and all of its associated parameters, if the confidentiality attribute specifies that confidentiality is to be supplied under this key (conf_yes).

- INTEGRITY

The integrity attribute specifies whether integrity services are in effect for the key.

integ_yes	integrity is to be provided
integ_no	integrity is not to be provided

- INTEGRITY ALGORITHM

This attribute identifies the algorithm to be used, and all of its associated parameters, if the integrity attribute specifies that integrity is to be supplied under this key (integ_yes).

- EXPLICIT SECURITY LABEL

This attribute specifies whether a security label is included in every TPDU exchanged on this cryptographic association. The possible values for this attribute are:

ppl_abs	Security label never used on TPDUs
ppl_xxx	xxx security label used on every TPDU

NOTE

Explicit security labels must be used when the cryptographic association supports more than one security level. They are optional when the cryptographic association supports only one security level.

- SECURITY LEVEL SET

This attribute specifies the set of allowable security levels for the cryptographic association.

- FINAL SEQUENCE NUMBER

This attribute specifies whether the final sequence number procedure (6.3.3.2) is to be used with this cryptographic association. The possible values for this attribute are:

fsn_yes	Final sequence number procedure is used
fsn_no	Final sequence number procedure is not used

- INITIATOR

This attribute specifies whether this end-system was the initiator of the cryptographic association.

- REMOTE IDENTIFIER

This attribute contains the key identifier used by the peer entity for this cryptographic association.

- PEER ADDRESS

This attribute contains the address of the peer for the cryptographic association. When the per end-system (kg_esp) or per end-system and security level (kg_esp_sr) keying is used, the address is the NSAP of the peer transport entity. When per connection (kg tc) keying is used the peer address information identifies the connection in use via the local and remote transport reference number.

5.1.1 Connection-Oriented Security Services

SP4C is used to provide connection oriented security services. The transport entity shall associate a key with each protected transport connection(kg_tc). The key shall be created explicitly for each protected transport connection. The security services to be provided on the connection are those associated with the key. All TPDUs sent or received over a protected transport connection shall be protected according to the services associated with the key. It should be noted that in this case, transport connection and cryptographic association are the same.

If connection-oriented integrity is desired, the security services associated with the key shall include Integrity Check Value (ICV) processing (integ_yes) and connection truncation protection (fsn_yes).

NOTE

If session integrity is desired, the session entity shall not reuse transport connections.

5.1.2 Connectionless Security Services

SP4E is used to provide connectionless security services. The transport entity shall associate a key with either:

- each transport entity pair (kg_esp)
- each transport entity and security level set pair (kg_esp_sr)

The sending transport entity shall protect each TPDU according to the services associated with the key and shall place the key identifier in the KEY-ID parameter of the SE TPDU. Upon receiving an SE TPDU, the key specified in the KEY-ID

parameter shall be used to decipher the TPDU set and/or to verify its ICV. Any improperly protected TPDU received shall be discarded.

5.2 Service Assumed of the Network Layer

Security services provided by the SP4 protocol are independent of any security services that may be used by the network layer.

5.3 Service Assumed of the Key Manager

The protocol specified in this addendum to the ISO 8073 requires the availability of cryptographic keys prior to an instance of protected communication. Keys are established by a combination of system, layer and security management functions. Any specific procedure for establishing keys is outside the scope of this document. The specific procedures for maintaining cryptographic key storage as well as for associating keys with specific TPDUs, are considered a local matter.

5.4 Minimum Algorithm Characteristics

Both the sending and receiving transport entities must use the same cryptographic algorithm or algorithms. The assumptions regarding cryptographic algorithms are as follows:

1) The same algorithm may be used for providing both confidentiality and integrity services.

2) It is beyond the scope of this document to specify a particular algorithm or to assess the security strengths or weaknesses of particular algorithms.

3) Encipherment and decipherment is performed in multiples of octets.

4) Cryptographic synchronization or initialization is realized on an individual TPDU basis.

5.5 Security Encapsulation Function

Encapsulation is used in conjunction with the encipherment and/or cryptographic check function to provide the connection or connectionless confidentiality and integrity services. When used by the sending entity, encapsulation is applied subsequent to all other protocol processing functions as described in ISO 8073 and ISO 8602. Further concatenation (in accordance with the concatenation rules described in 6.1) may occur after encapsulation. Decapsulation is applied by the receiving entity prior to any other protocol processing functions.

5.5.1 Data Encipherment Function

An encipherment mechanism provides data confidentiality. Each SE TPDU contains sufficient information for decipherment independent of information in any other SE TPDU. This includes identification of the cryptographic key (KEY-ID) to be used for decipherment as well as any cryptographic synchronization or algorithm initialization sequences.

5.5.2 Integrity Function

An integrity function provides data and/or data stream integrity. The elements of integrity and the mechanisms used to provide them are:

- Modification protection is provided by a ICV computed over the protected header and encapsulated TPDU.
- Insertion protection is provided by the use of the ICV and the transport sequence numbers.
- Deletion protection is provided by the use of the ICV and the transport sequence numbers.
- Connection truncation protection is provided by the transmission of final sequence numbers during connection release (fsn_yes).
- Connection replay protection is provided by the use of a separate key per transport connection (kg_tc).
- Protection against replay of a PDU is provided by the use of a separate key per transport connection (kg_tc) and the use of unique sequence numbers under each key.
- Reflection protection is provided by the use of a direction indicator (FLAGS field) in each SE TPDU (see 8.2.2.2).

5.5.3 Security Label Function

Security labeling is an optional function which can be used to associate a security label with each encapsulated TPDU set. The label indicates the sensitivity of the data. The security label supports access control mechanisms and helps meet computer security labeling requirements.

5.5.4 Security Padding Function

Security padding is an optional function which can be used to extend the length of an encapsulated TPDU set as needed. This supports cryptographic algorithm requirements.

6 ELEMENTS OF PROCEDURE

The elements of procedure are as specified in Clause 6 of the Connection-oriented Transport Protocol specification (ISO 8073) and Clause 6 of the Protocol for Providing the Connectionless-mode Transport Service (ISO 8602), with the additions in the following sections.

The protocol mechanisms described below are those used for data encapsulation. A SE TPDU contains:

a) a clear text header;

b) a protected header; if confidentiality is not used, this header is also cleartext;

c) a single TPDU or set of TPDUs concatenated according to the rules in ISO 8073;

d) an ICV parameter field, if integrity protection is used.

A TPDU shall be protected based on the attributes of the cryptographic association and encapsulated in a SE TPDU. On receipt of a SE TPDU, the transport entity shall verify that all the protection specified by the key attributes is present. An improperly protected TPDU shall be discarded.

NOTE

This is a security relevant event and shall be reported to the layer management entity.

6.1 Concatenation and Separation

The procedure for concatenation and separation is as specified in sub-clause 6.4 of the Connection-oriented Transport Protocol specification (ISO 8073), with the following changes:

a. Concatenation may take place both prior to and subsequent to encapsulation. Any TPDU defined in ISO 8073 may be transferred after being encapsulated within an SE TPDU. Only TPDUs which are to be protected under the same cryptographic key may be concatenated.

b. If the final sequence number option is specified (fsn_yes) for the cryptographic key, at most one TPDU from the following list may be present in a set of concatenated TPDUs: DC, DR, ER.

c. An encapsulated SE TPDU may itself be concatenated according to the concatenation rules which apply to a DT TPDU type; that is, there shall be at most one SE within a set of concatenated TPDUs and, if present, it shall always be placed last in the set of concatenated TPDUs.

NOTE

Concatenation following encapsulation is only of use when a mix of protected and unprotected transport connections are in use for the same end system.

d. A SE TPDU shall never itself be encapsulated within another SE TPDU.

NOTE

This procedure is not used with the connectionless transport service (ISO 8602).

6.2 Cryptographic Confidentiality

6.2.1 Purpose

Cryptographic confidentiality is used in all classes of transport protocol for end-to-end protection of user and control data in transit between communicating transport entities.

6.2.2 TPDUs and parameters used

The procedure makes use of the following TPDU and parameters:

- SE TPDU;
- key-id.

6.2.3 Procedure

If confidentiality is specified for a cryptographic association (conf_yes), then all TPDUs shall be protected by being encapsulated within an SE TPDU. All octets following the key-id (protected header and TPDU) shall be enciphered.

The cryptographic algorithm is an attribute of the cryptographic association which is identified by the key identifier (KEY-ID).

Upon receipt of a SE TPDU the transport entity uses the key identified by the key identifier in the SE TPDU to identify the security service and to decipher the TPDU. If the key is not available, the SE TPDU is discarded.

NOTE

This is a security relevant event and shall be reported to the layer management entity.

6.3 Integrity Processing

The following procedures are used to provide connectionless and connection-oriented integrity services.

6.3.1 Integrity Check Value (ICV) Processing

6.3.1.1 Purpose

ICV processing is used in all classes to detect unauthorized modification of user and control data while in transit between communicating transport entities.

6.3.1.2 TPDUs and parameters used

The procedure makes use of the following TPDU and parameters:

- SE TPDU;
- key-id

- ICV.

6.3.1.3 Procedure

If data integrity is specified (integ_yes) for a cryptographic association, then an ICV shall protect every SE TPDU. The message authentication code (MAC) is carried in the ICV parameter and occurs as the last field in the SE TPDU. The ICV is computed over the protected header and encapsulated TPDU. If confidentiality is specified (conf_yes) in addition to integrity, the manipulation detection code (MDC) is computed prior to encipherment.

The integrity check function and ICV field length are attributes of the cryptographic association.

Upon receiving a SE TPDU on a cryptographic association with integrity protection, the ICV field shall be verified by computing a test Integrity Check Value over the protected header and encapsulated TPDU set. If the key is not available or the test Integrity Check Value is not equal to the ICV field, then the entire SE TPDU shall be discarded.

NOTES

This is a security relevant event and shall be reported to the layer management entity.

If decipherment is also required, the testing of the Integrity Check Value shall be performed subsequent to decipherment.

6.3.2 Direction Indicator Processing

6.3.2.1 Purpose

The purpose of the direction indicator is to provide reflection protection.

6.3.2.2 TPDUs and parameters used

The procedure makes use of the following TPDU and parameters:

- SE TPDU;
- FLAGS.

6.3.2.3 Procedure

Each SE TPDU must contain the direction indicator bit (FLAGS field) indicating the sender of the TPDU. When a SE TPDU is sent by the initiator of the cryptographic association, the direction indicator bit is set to 1. When a SE TPDU is sent by the responder of the cryptographic association, the direction indicator bit is set to 0. Upon receipt of a SE TPDU the transport entity shall validate the direction indicator bit. If a SE TPDU is received with an incorrect direction indicator the TPDU shall be discarded.

NOTE

This is a security relevant event and shall be reported to the layer management entity.

6.3.3 Connection Integrity Sequence Number Processing

Replay, insertion, and deletion detection requires that each TPDU in a cryptographic association have a unique sequence number. When connection-oriented integrity is specified for a connection (kg_tc and integ_yes), this is provided using a key per connection in conjunction with the unique sequence number procedure (6.3.3.1) and the final sequence numbers procedure (6.3.3.2).

6.3.3.1 Unique Sequence Numbers

6.3.3.1.1 Purpose

The purpose of unique sequence numbers is to uniquely identify each DT and ED TPDU within a connection.

6.3.3.1.2 Procedure

If the connection-oriented integrity service is specified for a transport connection (kg_tc and integ_yes), each TPDU shall have a unique sequence number in a CA. Neither transport entity shall transmit a new DT or ED TPDU bearing a sequence number (either TPDU-NR or ED-TPDU-NR) which was previously used with that key. Retransmissions as part of normal error control and recovery may repeat the sequence number under the original key or use a new key.When either the DT or ED sequence number space is exhausted on a particular connection, a different cryptographic key than any previously used to protect data using that connection identifier (DST-REF) shall be used for transmitting any further data TPDUs. The key replacement procedure (6.8) shall be invoked. The new key shall exist prior to this procedure being employed. If no such key exists, the connection shall be released. Upon receipt of a DT or ED TPDU which duplicates a previously received sequence number on the current cryptographic key the transport entity shall discard the TPDU.

NOTE

This procedure is not used with the connectionless transport service (ISO 8602).

6.3.3.2 Final Sequence Numbers

6.3.3.2.1 Purpose

The final sequence number is used in transport classes 2 (except when the non-use of explicit flow control option is selected), 3, and 4. Its purpose is to detect connection truncation, the deletion of the final PDUs of a connection.

6.3.3.2.2 TPDUs and parameters used

The procedure makes use of the following TPDU and parameter:

- SE TPDU encapsulating a DR, DC or ER TPDU
    - FSN.

6.3.3.2.3 Procedure

If the connection truncation protection service is specified (kg tc and fsn yes) for a transport connection, then the FSN field of the SE TPDU shall be included when encapsulating the DR, DC, and ER TPDUs. The sequence numbers of the final DT and ED TPDUs sent and received on the connection shall be placed in the LAST SENT and LAST RECEIVED subfields of the FSN field.

Upon receipt of a DR, DC, or ER TPDU on a connection for which the connection truncation protection service is specified, the transport entity shall compare the final sent and received sequence numbers with the sequence numbers of the final sent and received DT and ED TPDUs.

NOTE

The handling of a mismatch of sequence numbers is a local matter. This is a security relevant event and reporting to an audit authority is recommended.

This procedure is not used with the connectionless transport service (ISO 8602).

6.4 Peer Address Check Processing

Upon receipt of a TPDU, the peer address associated with the cryptographic key shall be compared to the source address of the TPDU. If the addresses do not match, the SE TPDU shall be discarded.

NOTE

This is a security relevant event and shall be reported to the layer management entity.

6.5 Security Labels for Cryptographic Associations

6.5.1 Purpose

Security labels are used in all classes to provide support for access control and to provide support for data separation based on sensitivity.

6.5.2 TPDUs and parameters used

The procedure makes use of the following TPDU and parameter:

- SE TPDU;
    - key-id
    - label.

6.5.3 Procedure

When a cryptographic asociation specifies use of an explicit security label on every TPDU, the label shall be sent in the LABEL field of the protected header of each SE TPDU. Upon receipt of a SE TPDU containing the LABEL parameter, the transport entity shall verify that the LABEL parameter falls within the set of acceptable security levels for the cryptographic association. If a SE TPDU is received with an improper LABEL, the TPDU shall be discarded.

NOTE

This is a security relevant event and shall be reported to the layer management.

6.6 Pad Parameter

6.6.1 Purpose

Pad parameter processing is used in all classes for cryptographic algorithms which process data in blocks of specific sizes.

6.6.2 TPDUs and parameters used

The procedure makes use of the following TPDU and parameter:

- SE TPDU encapsulating any TPDUs defined in ISO 8073 or ISO 8602;
- pad.

6.6.3 Procedure

A received pad parameter value is discarded.

6.7 Connection Release

If the connection-oriented service (kg_tc) is in use, the key associated with a connection shall be deleted as part of the connection release procedure.

6.8 Key Replacement

The key replacement procedure is used if the cryptoperiod of a key expires. When the connection-oriented service is in use (kg_tc) it is also used when the sequence number spaces have been exhausted (see section 6.3.3.1).

Key replacement associates a new cryptographic key with an ongoing transport connection. The new key shall exist prior to key replacement and shall have attributes which are identical to the old key. If no such key exists, the layer management entity shall be notified and the original cryptographic key shall be discarded.

Following a key replacement, unacknowledged DT and ED TPDUs requiring retransmission shall be sent under the new key.

7 PROTOCOL CLASSES

Table 6 gives an overview of which elements of procedure are included in each class. This table applies if cryptographic protection is implemented. This table is part of this addendum to the international standard.

NOTE

The key to Table 6 in ISO 8073 applies. Part of this table is reproduced below, with the additions applicable to the addendumto IS 8073.

KEY TO TABLE 6

* Procedure always included in class

Not applicable

m Negotiable procedure whose implementation in equipment is mandatory

o Negotiable procedure whose implementation in equipment is optional

Protocol mechanism	Reference	0	1	2	3	4	CLTS
Cryptographic Confidentiality	6.2	m	m	m	m	m	m
ICV Processing	6.3.1	m	m	m	m	m	m
Direction Indicator Processing	6.3.2	*	*	*	*	*	*
Unique Sequence Nos.	6.3.3.1			o	o	o	
Final Sequence Nos.	6.3.3.2			o	o	o	
Peer Address Check Processing	6.4	*	*	*	*	*	*
Security Labels for Cryptographic Associations	6.5	o	o	o	o	o	o
Pad Parameter	6.6	*	*	*	*	*	*
Connection Release	6.7			o	o	o	
Key Replacement	6.8	m	m	m	m	m	m

TABLE 6: SP4 Elements of Procedure

8 STRUCTURE AND ENCODING OF TPDUS

8.1 Structure

The structure is defined in Section 13.2 of ISO 8073.

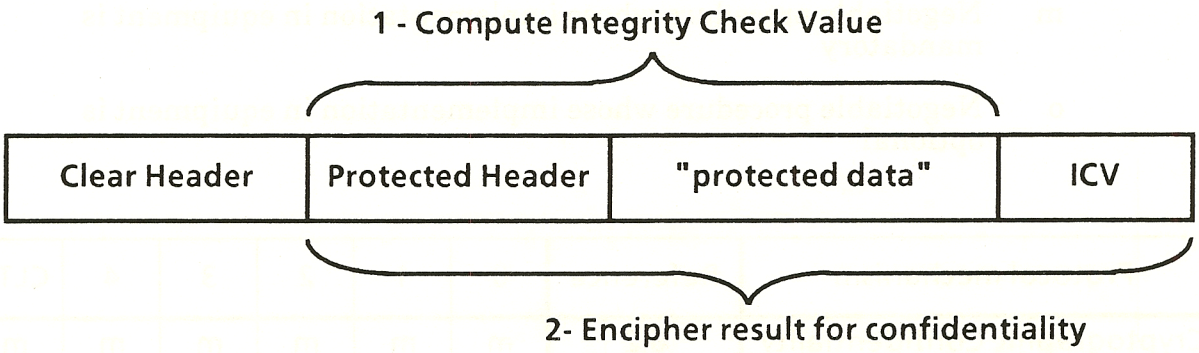
All the transport protocol data units (TPDUs) shall contain an integral number of octets. The octets in a TPDU are numbered starting from 1 and increasing in the order they are put into an NSDU. The bits in an octet are numbered from 1 to 8, where bit 1 is the low-order bit.

When consecutive octets are used to represent a binary number, the lower octet number has the most significant value.

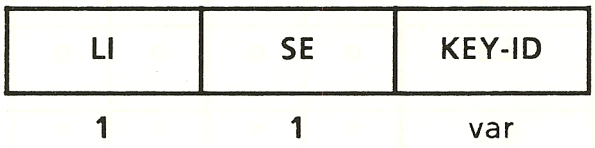
For each fixed length field the number of octets for the field is listed below the field in the following figures.

8.2 Security Encapsulation TPDU

The structure of the SE TPDU shall be as follows:



8.2.1 Clear Header



8.2.1.1 LI

The length indicator field (LI) contains the length of the Clear Header in octets, excluding the length indicator field.

8.2.1.2 SE

This field contains the TPDU code. It is used to define the structure of the remaining header. The value of the SE TPDU code is: 0100 1000.

8.2.1.3 KEY-ID

The key identifier field (KEY-ID) identifies the cryptographic key used to protect the TPDU.

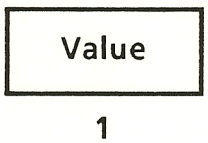
8.2.2 Protected Header

The LABEL, FSN, and PAD fields are optional. When present, they must appear in the order shown above.

8.2.2.1 LI

The LI contains the length of the Protected Header in octets, excluding the LI field. It has a maximum value of 254 (1111 1110).

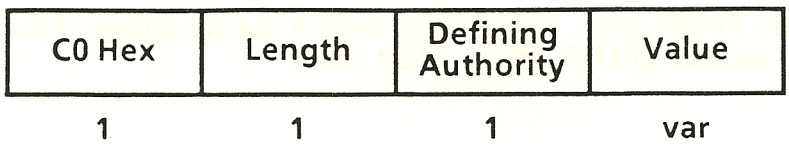
8.2.2.2 FLAGS



The currently defined bits in this field are:

- bit 1 direction indicator
  0 = responder to initiator
  1 = initiator to reponder

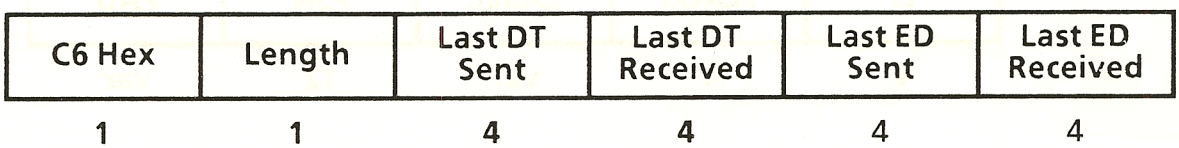
8.2.2.3 LABEL



C0 Hex	Length	Defining Authority	Value
1	1	1	var

The format of the Value is defined by the Defining Authority.

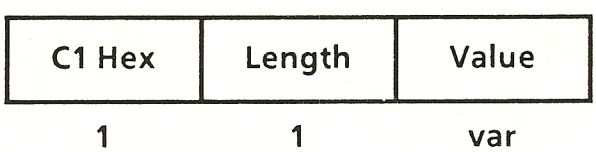
8.2.2.4 FSN



C6 Hex	Length	Last DT Sent	Last DT Received	Last ED Sent	Last ED Received
1	1	4	4	4	4

Last DT Sent is the last sequence number sent in a DT-TPDU. Last DT Received is the last sequence number received in a DT-TPDU. Last ED Sent is the last sequence number sent in a ED-TPDU. Last ED Received is the last sequence number received in a ED-TPDU.

8.2.2.5 PAD



C1 Hex	Length	Value
1	1	var

The Value field contains arbitrary data.

8.2.3 Protected Data

The data field contains a TPDU or concatenated set of TPDUs as per ISO 8073 or ISO 8602.

8.2.4 ICV

The ICV field contains the Integrity Check Value.