ISO/IEC JTC 1/SC6 N6779

Project: 06.35.06
Date: 1991-10-11

ISO/IEC JTC 1/SC6
TELECOMMUNICATIONS AND INFORMATION
EXCHANGE BETWEEN SYSTEMS

Secretariat: USA(ANSI)
Editors Draft of the DIS text

Title: Draft International Standard - Transport Layer Security Protocol

Source: Editor

Status: This is the draft of the Transport Layer Security Protocol based on agreements reached during the SC6/WG2/WG4 Security meeting held July 08-19, 1991 By SC6/WG4, SC6 voted at the SC6 plenary to register this document as a Draft International Standard.

Address reply to:

Secretariat ISO/IEC JTC 1 /SC6 - American National Standards Institute,1430 Broadway, New York NY 10018
Tel: 212 642-4931; TX 42 42 96 ANSI UI; FAX 212 302-1286

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/AD1. This document specifies optional additional functions 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.

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 protection achieved by the security protocol defined in this standard depends on the proper operation of security management including key management. However, this standard does not specify the management functions and protocols needed to support this security protocol.

This protocol can support all the integrity, confidentiality, authentication and access control services identified in ISO 7498-2 as relevant to the transport layer. The protocol supports these services through use of cryptographic mechanisms, security labelling and attributes, such as keys and authenticated identities, pre-established by security management.

This protocol supports peer-entity authentication at the time of connection establishment. In addition, re-keying is not supported within the protocol, although re-keying may occur though means outside the protocol.

2 References

ISO 7498:1984	Information Processing Systems -Open Systems Interconnection - Basic Reference Model
ISO 7498/AD1:1984	Information Processing Systems -Open Systems Interconnection - Basic Reference Model Addendum 1: Connectionless-mode Data Transmission
ISO 7498-2:1988	Information Processing Systems - Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture
ISO 8072:1986	Information Processing Systems - Open Systems Interconnection - Transport Service Definition
ISO 8072/AD1:1986	Information Processing Systems -Open Systems Interconnection - Transport Service Definition - Addendum 1 Connectionless-mode Transmission
ISO/IEC 8073:1988	Information Processing Systems -Open Systems Interconnection - Connection Oriented Transport Protocol Specification
ISO/IEC 8073/AD1:1988	Information Processing Systems - Open Systems Interconnection - Connection Oriented Transport Protocol Specification - Addendum 1: Network Connection Management Subprotocol
ISO/IEC 8073/AD2:1988	Information Processing Systems - Open Systems Interconnection - Connection Oriented Transport Protocol Specification - Addendum 2: Class four operation Over Connectionless Network Service
ISO 8602:1987	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.

3.1 Security Reference Model Definitions

This document makes use of the following terms as defined in ISO 7498/2

a) access control

b) asymmetric

c) ciphertext

d) cleartext

e) confidentiality

f) data integrity

g) data origin authentication

h) denial of service

i) end-to-end encipherment

j) key

k) key management

l) symmetric

3.2 Additional Definitions

For the purpose of this document, the following definitions apply.

m) cryptoperiod: The length of time for which a cryptographic key is permitted to be used. After this time has expired, the key must be replaced.

n) in-band: performed by protocol mechanisms defined in this International Standard

o) out-of-band: not performed by protocol mechanisms defined in this International Standard.

p) pairwise key: a key generated for two particular parties in a security association and only available to them.

n) reflection protection: detection that a message has been sent back.

o) security association: A collection of information describing a security relationship between communicating entities.

p) security attributes: The collection of information required to control the security of communications between an entity and its remote peer(s).

4 Symbols and Abbreviations

This standard 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-NR	TPDU number (field)
ER TPDU	Error TPDU
LI	Length indicator (field)
SRC-REF	Source Reference (field)
TPDU	Transport protocol data unit
TPDU-NR	DT TPDU number (field)

Additionally, the following abbreviations are used in this standard:

CBTSS	Connection Based Transport Security Service
Conf_no	Confidentiality is not to be provided
Conf_yes	Confidentiality is to be provided
GTSS	General Transport Security Service
ICV	Integrity Check Value
Integ_no	Integrity is not to be provided
Integ_yes	Integrity is to be provided

KEY-ID	Key Identifier
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
Kg_tc	A separate cryptographic key is used for each Transport connection
LABEL	Security Label
LLSG	Lower Layer Security Guidelines
LME	Layer Management Entity
NLSP	Network Layer Security Protocol
NSAP	Network Service Access Point
NSDU	Network Service Data Unit
PAD	Padding (field)
Ppl_abs	Security label never used on TPDUs
Ppl_pres	Security Label used on every TPDU
SE TPDU	Security Encapsulation TPDU
TLSP	Transport Layer Security Protocol

5 Overview of the Protocol

5.1 Introduction

ISO 7498-2 identifies the following security services as being relevant to the transport layer:

Peer entity authentication
Data origin authentication
Access control Service
Connection confidentiality
Connectionless confidentiality
Connection integrity with recovery
Connection integrity without recovery
Connectionless integrity

Note 1: ISO 8072 currently only defines 4 levels of protection quality:

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

which are equivalent to the following security services.

ISO 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.

ISO 8072 will require changes to allow all the forms of protection to be selected.

Note 2: Connectionless integrity does not protect against addition or deletion of connectionless SDUs and only provides limited replay protection.

TLSP used with ISO/IEC 8073 can support connection integrity with and without recovery, connection confidentiality, access control service and peer entity authentication with each connection individually protected. However, a key may be shared between several connections.

TLSP used with ISO 8602 can support connectionless integrity, connectionless confidentiality, access control service and data origin authentication.

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.

Figures (1 and 2) show the location of TLSP in the seven layer ISO model.

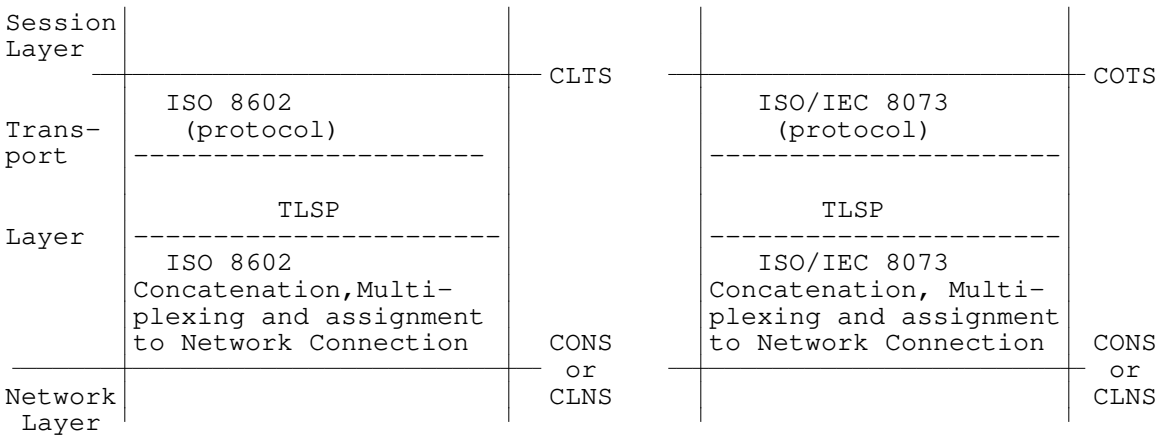


Figure 1 TLSP with ISO 8602 Figure 2 TLSP with ISO/IEC 8073

5.2 Transport Security Services

The specific TLSP processing options used in an instance of communications are determined by the attributes associated with the pairwise security association key. TLSP assumes that two transport entities using the same pairwise key will associate consistent sets of attributes. The Security Association Identifier, SA-ID, points to the appropriate set of attributes for the pairwise key. As a security association may be rekeyed, more than one SA-ID may identify the same security association.

Each security association is defined by a set of attributes at each end system. TLSP uses these security association attributes to determine processing characteristics of the user data. The following describe the attributes for TLSP and list the mnemonics used to refer to these attributes in this specification.

a) SA Identification

I) My_SAID: The local identifier of the SA

II) Your_SAID: The remote identifier of the SA

III) SAID_Len: Integer - Length of the SAID defined by the ASSR
Integer of range 2 to 126

The value of the My_SAID and Your_SAID is set up on SA establishment. The value of SAID_Len is defined for a given ASSR.

Note: As the SA-ID field is also used to convey the Key-ID which performs the security functions on that pdu, there may be one or more SA-ID identifiers used but only one is allowable on a TLSP PDU at any one

time.

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

Initiator: Boolean

The value of this attribute is set up on SA establishment

c) Address of peer TLSP entity(s)

Peer_Adr: Octet string

The value of this attribute is set up on SA establishment and indicates either the NSAP address of the transport entity if the same key is shared between several connections or the connection is use via the local and remote transport reference number if the key is for only the one connection.

d) Identifier for the agreed set of security rules to be applied for this association

ASSR_ID: Object Identifier as defined in ASN.1 ISO 8824

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

e) Protection QOS selected for the SA

QOS_Label: Format defined by ASSR

AC: Access Control Level Integer of range defined by the ASSR

The following QOS parameters are only relevant to TLSP used in conjunction with ISO 8602:

DOAuth: (Data Origin Authentication level) Integer of range defined by ASSR

CLConf: (Connectionless Confidentiality level) Integer of range defined by ASSR

CLInt: (Connectionless Integrity level) Integer of range defined by ASSR

The following QOS parameters are only relevant to TLSP used in conjunction with ISO/IEC 8073:

PE Auth: (Peer Entity Authentication level) Integer of range defined by ASSR

CO Conf: (Connection Confidentiality level) Integer of range defined by ASSR

CO Int: (Connection Integrity without recovery Integer of range defined by ASSR

CO Intr: (Connection Integrity with recovery Integer of range defined by ASSR

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

f) Mechanisms selected for the SA

Label: Boolean - Explicit labelling TPDUs

Conf: Boolean - Confidentiality of a Secure Data Transfer by encipherment

ICV: Boolean - Integrity of a Secure Data Transfer contents using an integrity check value

SN: Boolean - Connection Integrity Sequence number procedure to be used

Padd: Boolean - Padding of Secure Data Transfer PDU to support ICV mechanism, Encipherment mechanism

PE-Authentication: Boolean - Peer Entity Authentication using exchange of encapsulated Connect Request / Connect Response PDUs

TPDUUN: Boolean - Unprotected TPDUs

g) Label mechanism attributes

```
Label_set: Set of {
                    Label_Ref: Integer
                    Label_Auth: (To be defined)
                    Label_Content: To format defined by Label_Auth
                }
```

The following attribute is relevant only to TLSP operating in conjunction with ISO/IEC 8073.

Conn_Label: Integer - Label reference of current connection

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

h) ICV mechanism attributes

ICV_Alg: Object Identifier

ICV_Len: Integer

ICV_Kg: Integer of value Kg_tc or Kg_esp or Kg_esp_sr

Key granularity is either:

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.

The values of these attributes are defined by the ASSR given the protection QOS.

ICV_Gen_key: ICV generation key reference - form defined by ASSR

ICV_Check_Key: ICV check key reference - form defined by ASSR

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

i) SN Mechanism attributes

The following attributes are only relevant for TLSP used in conjunction with ISO/IEC 8073.

Data_My_SN: SN for last normal data sent

Data_Your_SN: SN for last normal data received

The initial values of these attributes are set up as part of the normal connection. The SN is the sequence number used by ISO/IEC 8073.

j) Encipherment Mechanism Attributes

Enc_Alg: Object identifier allocated under ISO 9979

Enc_Kg: Integer of value Kg_tc or Kg_esp or Kg_esp_sr

The Key Granularity attributes are defined in h)

The value of this attribute is defined by the ASSR given the protection QOS.

Enc_Key: Encipherment key reference - form defined by ASSR

Dec_Key: Decipherment key reference - form defined by ASSR

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

k) Padding Mechanism Attributes

Enc_Blk: Integer - Block size of encipherment algorithm

ICV_Blk: Integer - Block size of ICV algorithm

Note: Additional mechanisms select attributes and mechanism specify attributes may be identified in future versions of this standard and for private mechanisms.

5.2.1 Security Services for Connection-Oriented Transport Protocol

When TLSP is used to provide connection oriented security services, the transport entity shall associate a key with each protected transport connection (Kg_tc), each transport end system pair (Kg_esp) or each transport end system and security level set (Kg_esp_sr). The key shall be created explicitly for the protected transport connection(s). The security services to be provided on the connection are those associated with the attributes of the security association. All TPDUs sent or received over a protected transport connection(s) shall be protected according to the services associated with the security association. If Kg_tc a one to one correspondence exists between a transport connection and a security association.

If connection-oriented integrity is desired, the security services associated with the security association shall include Integrity Check Value (ICV) processing (Integ_yes). Any improperly protected TPDUs received shall be discarded. This reception of improperly protected TPDUs is a security relevant event; however further action hereon is outside the scope of this International Standard (e.g., such as filling audit reports).

5.2.2 Security Service for Connectionless Transport Protocol

When TLSP is used to provide security services for the connectionless mode transport service, the transport entity shall associate a key with either:

- o each transport entity pair (Kg_esp)
- o each transport entity and security level set pair (Kg_esp_sr)

The sending transport entity shall protect each TPDU according to the attributes associated with the key and shall place the remote identifier in the SA-ID parameter of the SE TPDU. Upon receiving an SE TPDU, the key specified in the SA-ID parameter shall be used to decipher the TPDU and or to verify its ICV. Any improperly protected TPDUs received shall be discarded. This reception of improperly protected TPDUs is a security relevant event; however further action hereon is outside the scope of this International Standard (e.g., such as filling audit reports).

5.3 Service Assumed of the Network Layer

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

5.4 Security Management Requirements

This security protocol requires that the attributes of a security association have been established prior to an instance of protected communication of user data. These attributes may be established through use of security management functions which are outside the scope of this International Standard.

The degree of protection achieved will depend upon proper management of security including key management. 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 if symmetric keying is used. For asymmetric keying the same cryptographic keys is not available for both the sending and receiving TLSP entities. Either symmetric or asymmetric keying is allowed by this International Standard.

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

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

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

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

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

5.6 Security Encapsulation Function

Encapsulation is used in conjunction with the encipherment and/or integrity check function to provide the connection or connectionless confidentiality and integrity services. The encipherment and integrity check functions may or may not be cryptographically based. This is dependent on the user's requirements. When used by the sending entity, encapsulation is applied subsequent to all other protocol processing functions as described in ISO 8073 and ISO 8602. Decapsulation is applied by the receiving entity prior to any other protocol processing functions.

5.6.1 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 (SA-ID) to be used for decipherment as well as any cryptographic synchronization or algorithm initialization sequences.

5.6.2 Integrity Function

This function supports connectionless integrity and data origin authentication or connection integrity. An integrity function provides data and/or data stream integrity. The elements of integrity and the mechanisms used to provide them are:

Protection Against	Mechanism	CBTSS	GTSS (CO)	(CL)
Modification	ICV Computed over the protected header and encapsulated PDU	x	x	
Insertion	ICV and Transport sequence numbers	x		
Deletion	ICV and Transport sequence numbers	x		
Connection Replay	Separate key per Transport Connection (Kg_tc) or unique connection identifier under each key	x		
PDU Replay	Separate key per Transport Connection (Kg_tc)and use of unique sequence numbers under each key or Unique connection identifier and sequence number under each key	x		
Reflection	Direction indicator (Flags Field) in each SE TPDU	x	x	
Masquerade	ICV and, integrity or encipherment key, unique to a transport address	x		

5.6.3 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.

5.6.4 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 for both confidentiality and integrity.

Note: Use Label's syntax registered according to ISO/CCITT Registration procedures, national body procedures or private procedures.

5.6.5 Peer Entity Authentication

This function performs peer entity authentication through exchange of encapsulated connection establishment PDUs containing a connection identifier as shown below (see Figure 3):

INITIATOR RESPONDER

CR(scr-ref$_a$)---------->

<---------- CC(scr-ref$_b$,dst-ref$_a$)

ACK/DT(dst-ref$_b$)---------->

Figure 3: Illustration of exchanges to support peer entity authentication.

The source and destination references must be:

- integrity protected and
- unique within the lifetime of the integrity key

6 Elements of Procedure

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

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 security 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 security association key attributes is present. An improperly protected TPDU shall be discarded.

Note

This reception of improperly protected TPDUs is a security relevant event; however further action hereon is outside the scope of this International Standard (e.g., such as filling audit reports).

If the security encapsulation function is invoked for a TPDU for which a suitable SA doesn't exist, the TLSP may invoke either an SA Establishment Protocol as specified in Amendment 1 to TLSP (ISO/IEC 10736) or take any other appropriate action.

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 shall only take place prior 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 security association key may be concatenated.

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

NOTE

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

6.2 Confidentiality

6.2.1 Purpose

Confidentiality may be used by the transport protocol connection and connectionless mode for end-to-end protection of user data and security control information 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;
- SA-ID.

6.2.3 Procedure

If confidentiality is specified for a security association (Conf_yes), then all TPDUs shall be protected by being encapsulated within an SE TPDU. All octets following the SA-ID (protected header and TPDU) shall be enciphered. See Figure 4.

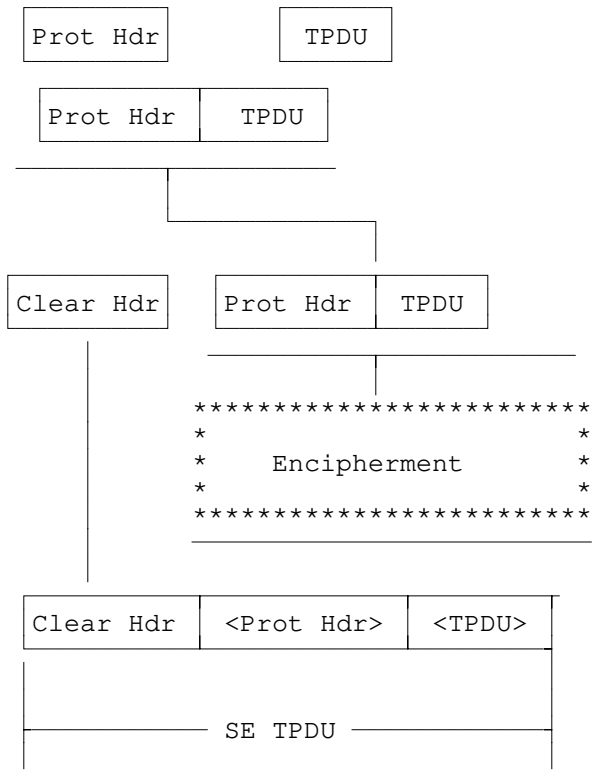
The cryptographic algorithm is an attribute of the security association which is identified by the security association identifier (SA-ID).

Upon receipt of a SE TPDU the transport entity uses the key identified by the SA-ID 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 reception of improperly protected TPDUs is a security relevant event; however further action hereon is outside the scope of this International Standard (e.g., such as filling audit reports).

Processing in Support of Confidentiality



Note Quantities in brackets are enciphered quantities

Figure 4. TLSP Encapsulation Methods. TLSP's method for encapsulation and encipherment in support of Confidentiality as indicated in Clause 6.2

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 may be used by TLSP for both Transport Protocol connection mode (ISO 8073) and connectionless mode (ISO 8602) to detect unauthorized modification of user data and security control information 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:

- o SE TPDU;
  - o SA-ID
  - o ICV.

6.3.1.3 Procedure

There are two types of ICV processing - message authentication code (MAC) and manipulation detection code (MDC). The difference between the use of MAC or MDC is directly related to what is specified - integrity or integrity and confidentiality. If only integrity is selected then a cryptobased MAC should be used. If integrity and confidentiality is selected the ICV may either be a non-cryptobased manipulation detection code (MDC) such as XOR or checksum or it may be cryptobased such as MAC. It does not need to be cryptobased because the whole protected header will be encrypted since confidentiality was also selected. If only confidentiality is selected then there is no ICV field.

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. See figure 5.

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

Upon receiving a SE TPDU on a security 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 reception of improperly protected TPDUs is a security relevant event; however further action hereon is outside the scope of this International Standard (e.g., such as filling audit reports).

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

Processing in Support of Integrity

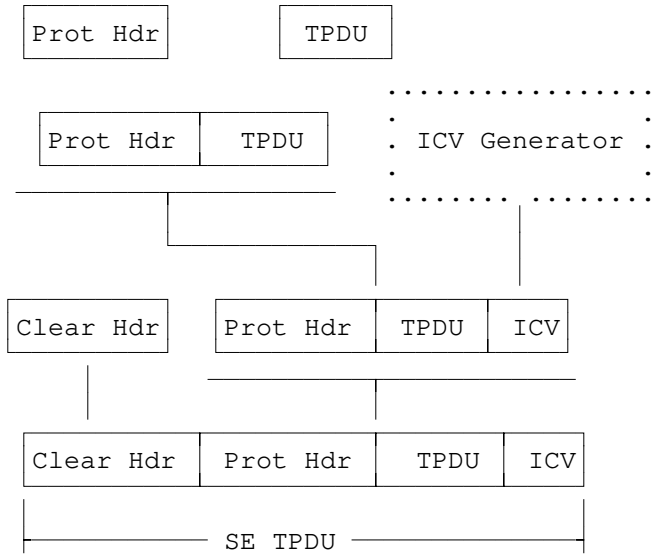
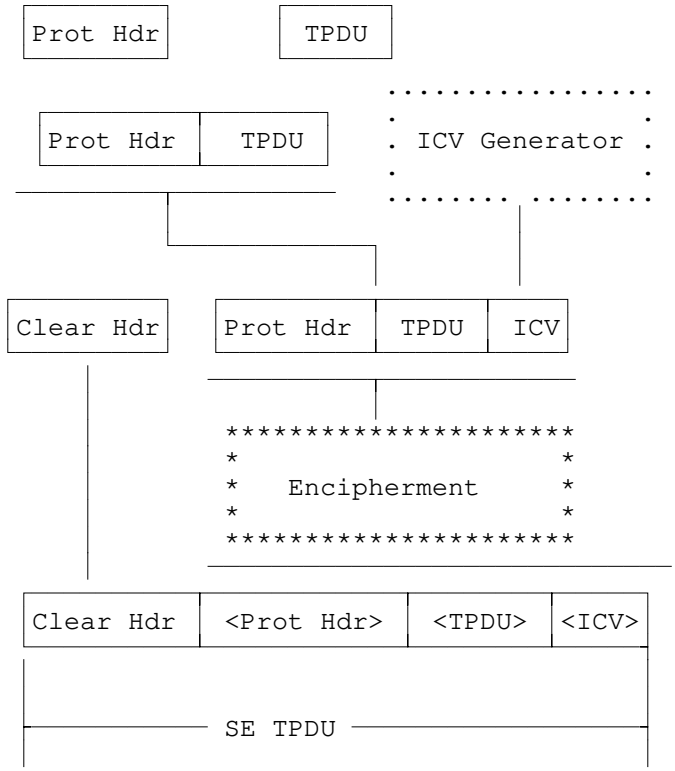


Figure 5 TLSP Encapsulation Methods. TLSP's method for encapsulation and ICV generation in support of Integrity as indicated in Clause 6.3

Processing in Support of Integrity and Confidentiality

Figure 6 depicts both integrity and confidentiality.



Note: Quantities in brackets are enciphered quantities

Figure 6 TLSP Encapsulation Method. TLSP's method for encapsulation and ICV generation in support of "Integrity and Confidentiality" as indicated in Clauses 6.2 and 6.3.

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 shall contain the direction indicator bit (FLAGS field) indicating the sender of the TPDU. When a SE TPDU is sent by the initiator of the security association, the direction indicator bit shall be set to 1. When a SE TPDU is sent by the responder of the security association, the direction indicator bit shall be 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. If a SE-TPDU is received with unsupported flags set, the SE TPDU shall be discarded.

Note

This reception of improperly protected TPDUs is a security relevant event; however further action hereon is outside the scope of this International Standard (e.g., such as filling audit reports).

6.3.3 Connection Integrity Sequence Number Processing

Replay, insertion, and deletion detection requires that each TPDU in a security 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). This procedure is not used with ISO 8602.

6.3.3.1 Unique Sequence Numbers

6.3.3.2 Purpose

Unique sequence numbers is an optional procedure to uniquely identify each DT and ED TPDU within a connection. This procedure is only applicable to ISO/IEC 8073 (Classes 2, 3, and 4)

6.3.3.3 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 Security Association. 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) may be used for transmitting any further data TPDUs. The key replacement procedure (6.8) shall be invoked. If no such key exists, the connection may 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 reception of improperly protected TPDUs is a security relevant event; however further action hereon is outside the scope of this International Standard (e.g., such as filling audit reports).

The unique sequence number is the Transport sequence number used in classes 2, 3, and 4. It is recommended that extended sequence numbers be used to avoid rekeying.

6.4 Peer Address Check Processing

6.4.1 Purpose

This procedure is to counter masquerade attacks and support data origin authentication.

6.4.2 Procedure

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 reception of improperly protected TPDUs is a security relevant event; however further action hereon is outside the scope of this international standard (e.g., such as filling audit reports).

For each type of key granularity there is a corresponding degree of peer address information that requires verification. When per end-system (Kg-esp) keying is used, the NSAP address of the peer transport entity is checked with the negotiated peer address. When per end-system and security level (Kg-esp-sr) keying is used, the security label of the SE TPDU is checked with the negotiated security level set, in addition to checking the NSAP address of the peer transport entity. Since the security label is not strictly speaking address information and may be used optionally with single level security associations, security label checking is done independently as discussed elsewhere (Section 6.5, Security Labels for Security Associations).

When per connection (Kg-tc) keying is used, the procedure becomes a bit more complex since the transport connection identifiers (SRC-REF, DST-REF) conveyed within individual TPDUs must be verified, in addition to the NSAP address of the peer transport entity. The SRC-REF is checked against the remote transport reference number portion of the peer address security attribute and the DST-REF against the local reference for the connection. Note that a transport entity initiating a connection may not know the local reference used by its peer, and may be unable to verify the SRC-REF of an incoming CC TPDU. This

situation occurs when the peer dynamically determines the local reference upon processing a CR TPDU, and no value is available for the key manager to convey at the time the security attributes are established. Providing that the DST-REF field of the CC TPDU is the same as the local reference for the connection, the TPDU may be accepted and the value of SRC-REF field retained.

6.5 Security Labels for Security Associations

6.5.1 Purpose

Security labels are used 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 parameters:

- SE TPDU;
  - SA-ID
  - LABEL.

6.5.3 Procedure

When a security association 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 security association. If a SE TPDU is received with an improper LABEL, the TPDU shall be discarded.

NOTE

This reception of improperly protected TPDUs is a security relevant event; however further action hereon is outside the scope of this international standard (e.g., such as filling audit reports).

6.6 Padding

6.6.1 Purpose

Padding is used 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
  - 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 deselected 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 may also be 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 have attributes which are identical to the old key. If no such key exists, the Secure management entity shall be notified and the original cryptographic key shall be discarded.

Note

The new key should be available within the transport activity timer (for class 4) or the TWR time (class 3) otherwise the connection may be terminated by the transport protocol.

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

6.9 Unprotected TPDUs

The security policy may allow secure Transport connections and non-secure connections between communicating entities. The means by which this is achieved is a local matter.

On transmission if the SA-Attribute Unprotected is true the TPDU is passed through unprotected without the addition of PCI processing under TLSP.

On reception if the SA-Attribute Unprotected is true the received TPDU is passed through without any processing under TLSP procedures.

6.10 Protocol Identification

If this protocol is used over a network connection, it shall be explicitly identified by the explicit identification procedures defined in ISO/IEC 8073/Add 1. The identifying UN TPDU itself may be protected by the protocol specified in this International Standard. If the UN TPDU is unprotected and if it specifies this International Standard in conjunction with either ISO/IEC 8073 or ISO 8602, then the TPDUs will be protected after successful completion of network connection establishment in accordance with the SA attributes. If the UN TPDU is protected and if it specifies either ISO/IEC 8073 only or ISO 8602 only then the single specified protocol is used after successful completion of network connection establishment.

Notes

1. Whether or not unprotected communications is supported depends on the SA attributes.

2. If unprotected Tcs are supported, whether or not they are multiplexed with protected TCs over the same NC depends on SA attributes and the security policy of the entity.

The explicit identification procedure defined in ISO/IEC 8073/ADD 1 is not used if ISO/IEC 8073 (Class 4) is being run over ISO 8473 (Connectionless Network Protocol).

7 Use of Elements of Procedure

Table 1 gives an overview of which elements of procedure are included in each class of ISO/IEC 8073 and in ISO 8602.

KEY TO TABLE 1

* Procedure always included in class

NA Not applicable

o Negotiable procedure whose implementation in equipment is optional

m Negotiable procedure whose implementation in equipment is mandatory

Protocol mechanism	Reference	ISO/IEC 8073, Class 0	1	2	3	4	ISO 8602
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	NA	NA	o	o	o	NA
Peer Address Check Processing	6.4	*	*	*	*	*	*
Security Labels for Cryptographic Assoc.	6.5	o	o	o	o	o	o
Pad Parameter	6.6	*	*	*	*	*	*
Connection Release	6.7	o	o	o	o	o	NA
Key Replacement	6.8	o	o	o	o	o	o

Table 1: TLSP Elements of Procedure

Note

All negotiation is presently outside the scope of this International Standard. An Amendment to this International Standard will allow this negotiation to be done at any time before the connection as part of TLSP.

8 Structure and Encoding of TPDUs

8.1 Structure

The structure of the TPDU, or concatenated TPDUs, before encapsulation (i.e. placed in "protected data" field of a TPDU see 8.2) is as defined in Section 13.2 of ISO/IEC 8073.

8.2 Security Encapsulation TPDU

All the transport protocol data units (SE TPDUs) shall contain an integral number of octets. The octets in a SE 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 within the SE TPDU are used to represent a binary number, the lower octet number has the most significant value.

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

The structure of the TPDU shall be as follows:

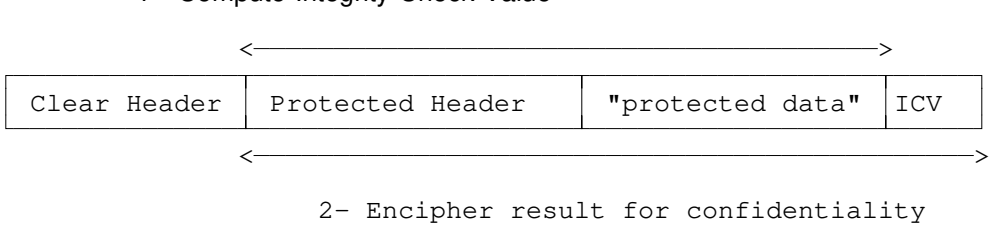


Figure 8.1 Structure of the TPDU

8.2.1 Clear Header

Protocol ID	LI	PDU Type	SA-ID	Crypo Synch
*	1	1	var	var

Figure 8.2 Format of the clear header

8.2.1.1 Protocol ID

This octet contains the TLSP protocol identifier which has been identified by NCMS.

* This field is not used if ISO/IEC 8073 and TLSP is running over ISO 8473.

8.2.1.2 PDU Clear Header Length

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

8.2.1.3 PDU Type

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

8.2.1.4 SA-ID

The Security Association identifier field (SA-ID) contains the remote identifier of the cryptographic key used to protect the TPDU.

8.2.1.5 Crypto Sync

This is an optional field which may contain synchronization data for specific encipherment algorithm identifier contained in the Security Association attributes.

Note: The size of the field would be known by the participating entities and part of the Security Association attributes.

8.2.2 Protected Contents

Content Length	Flag/type	Label	Data	PAD	ICV
2	1	var(tlv)	var(tlv)	var	var

Figure 8.3 Protected Contents

Figure 8.3 shows the protected contents format for the Secure PDU.

8.2.2.1 Content Length

The length field contains the length of the Protected Contents in octets, excluding the content length field. It has a maximum value of 65535 (2^{16}-1).

8.2.2.2 Flags

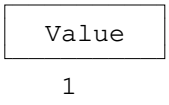


Figure 8.4 Flags field

The currently defined bits in this field are:

o bit 1 direction indicator

0 = responder to initiator

1 = initiator to responder

bit 2 = 1 SCI Exchange Se TPDU

bits 3 to 8 Unused flag bits are set to zero on transmission

8.2.2.3 Label

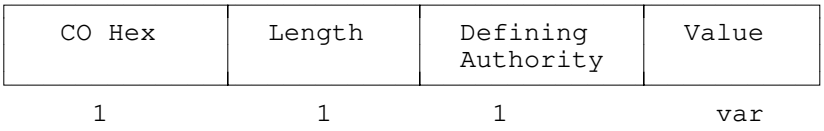


Figure 8.5 Format of the label field.

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

8.2.2.4 Protected Data

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

8.2.2.5 Pad

The Value field contains arbitrary data required for integrity and block encipherment mechanisms.

The length of padding is defined by:

a. the padding required by the integrity mechanism;

The integrity mechanism being used has known characteristics which will include block length defined for the use in the security association (if mechanism used in block mode. The starting point of the integrity process to the end of the integrity pad must be an integral multiple of the block length.

b. the padding required by the block encipherment mechanism to bring the end of the ICV up to the end of the block size.

The block size for encipherment is a known characteristic of the encipherment algorithm. The starting point of the confidentiality process to the end of the ICV must be an integral multiple of the block length.

8.2.2.6 ICV

The ICV field contains the Integrity Check Value. The length of this field is implied by the ICV algorithm identifier contained in the Security Association attributes.

9 Conformance

9.1 General

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

9.2 Common Static Conformance Requirements

a) A conformant implementation shall support at least TLSP with either ISO/IEC 8073 or ISO 8602.

b) A conformant implementation shall support implementation in an end system.

c) Each system claiming conformance to TLSP shall be capable of encapsulation and extraction of Userdata within a Secure Data Transfer PDU.

d) Each system claiming to provide confidentiality security services shall support at least the encipherment mechanism.

e) Each system claiming to provide integrity security services shall support at least the ICV mechanism.

9.3 TLSP with ISO 8602 Static Conformance Requirements

a) Each system claiming conformance to the TLSP protocol shall provide at least one of the following security services:

I) Connectionless confidentiality
II) Connectionless integrity

9.4 TLSP with ISO/IEC 8073 Static Conformance Requirements

a) Each system claiming conformance to TLSP shall provide at least one of the following security services:

I) Connection confidentiality
II) Connection integrity without recovery
III) Peer entity authentication.

9.5 Common Dynamic Conformance Requirements

Each system claiming to be conformant to this International Standard shall have the following behavior:-

a) Detection of all mandatory and optional fields within a Secure Data Transfer PDU in an sequence.

b) Unrecognized fields within a Secure Data Transfer PDU shall be treated as an error as described in sections 6.

c) If the ICV algorithm used is not cryptographically based then the encipherment mechanism may be used to protect the ICV.

9.6 TLSP with ISO 8602 Dynamic Conformance Requirements

Each system claiming to be conformant to the TLSP protocol shall have the following behavior:-

a) When peer data origin authentication is provided then either the encipherment mechanism or a cryptographic ICV mechanism shall be invoked.

9.7 TLSP with ISO/IEC 8073 Dynamic Conformance Requirements

Each system claiming to be conformant to the TLSP protocol shall have the following behavior:-

a) When peer entity origin authentication is provided then either the encipherment mechanism or a cryptographic ICV mechanism shall be invoked.

b) Detection and valid response to received Connection Authentication PDUs as defined in sections 6.

10 Protocol Implementation Conformance Statement (PICS)

The supplier of a protocol implementation which is claimed to conform to this International Standard shall complete a copy of the PICS proforma provided in annex A, including the information necessary to identify fully both the supplier and the implementation.

Annex A (normative)

PICS proforma

A.1 Introduction

A.1.1 Background

The supplier of a protocol implementation which is claimed to conform to International Standard 10736 shall complete the Transport Layer Security Protocol (TLSP), Protocol Implementation Conformance Statement (PICS) proforma. A completed PICS proforma becomes the PICS for the implementation in question. The PICS is a statement identifying the capabilities and options of the protocol that have been implemented. The PICS can have a number of uses, including:

A.1.1.0.1 use by the protocol implementer, as a check list to reduce the risk of failure to conform to the standard through oversight;

A.1.1.0.2 use by the supplier and receiver of the implementation, as a detailed indication its capabilities, stated relative to the common basis of understanding provided by the standard PICS proforma;

A.1.1.0.3 use by the user of the implementation, as a basis for checking the possibility of interworking with another implementation;

A.1.1.0.4 use by a protocol tester, as the basis for selecting appropriate tests against which to assess the claim for conformance of the implementation.

A.1.2 Approach

The first part of the PICS proforma, the Implementation 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 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. Therefore, all relevant choices are to be marked.

---

*) Copyright release for PICS proforma

Users of this International Standard may freely reproduce the PICS proforma in this annex so that it can be used for the intended purpose and may further publish the completed PICS."

Each item is identified by an reference index in the first column; the second column contains the item to be addressed; the third column contains the reference(s) to the location of the item in the main body of the standard. For optional items, additional columns indicate the status of the item (i.e., whether support is mandatory, optional, or conditional), and provide space or a choice or items for the implementation support response.

The following status column notations described in ISO/IEC JTC1/ SC6 N6233, Catalogue of PICS Proforma Notations, are used for this PICS proforma:

Symbol	Meaning
m	mandatory
o	optional
-	not applicable (N/A)
o.<n>	optional, but support of at least one of the group of options labelled by the same numeral <n> is required
<cid>:	conditional requirement, according to the condition or item index identified by <cid>
<item>::	simple predicate condition, dependent on the support marked for <item>

A.2 Implementation Identification

Table 1: TLSP Implementation Identification

Item	Information
Supplier	_____
Contact point for queries about this PICS	_____ _____
Implementation Name(s) and Version(s)	_____ _____
Other information necessary for full identification (e.g., Name's and Version(s) for machines and operating systems, System Name(s))	_____ _____ _____ _____

Notes:

a) Only the first three items are required for each implementation. Other information may be completed as appropriate in meeting the requirements for full identification.

b) The terms "Name" and "Version" should be interpreted appropriately to correspond with a supplier's terminology (e.g., using Type, Series, Model).

A.3 General Statement of Conformance

Table 2 below codifies the general statement of conformance for the implementation.

Table 2: General Conformance Statement

Index	Item	Support	
COTP	Does the implementation claim conformance with ISO/IEC 8073?	Y	N
COMAN	Are all mandatory features of ISO/IEC 8073 implemented?	Y	N
CLTP	Does the implementation claim conformance with ISO 8602?	Y	N
CLMAN	Are all mandatory features of ISO 8602 implemented?	Y	N
SP	Does the implementation claim conformance with ISO/IEC 10736?	Y	N
SPMAN	Are all mandatory features of ISO/IEC 10736 implemented?	Y	N

A.4 Protocol Implementation

Table 3 identifies the classes of the connection oriented Transport Protocol (COTP::) supported by the implementation.

Table 3: COTP Classes Implemented

Index	Transport Class	Support	
C0	class 0 TLSP-cons	Y	N
C1	class 1 TLSP-cons	Y	N
C2	class 2 TLSP-cons	Y	N
C3	class 3 TLSP-cons	Y	N
C4	class 4 TLSP-cons	Y	N
C4L	class 4 TLSP-clns	Y	N

A.5 Security Services Supported

The following set of tables identify for each class of Transport (COTP::), the security services available through the TLSP and their level of support within the implementation. The security service definitions are taken from ISO\IEC 7498-2.

Table 4: Service Element Proforma for C0

Index	Service Element	Status	Support	
SE0	Confidentiality	o.1	Y	N
SE1	Connection Confidentiality	SE0:m	Y	N
SE2	Connectionless Confidentiality	-		
SE3	Integrity	o.1	Y	N
SE4	Connection Integrity w Recovery	-		
SE5	Connection Integrity wo Recovery	SE3:m	Y	N
SE6	Connectionless Integrity			
SE7	Data Origination Authentication	o	Y	N
SE8	Access Control	o	Y	N

Table 5: Service Element Proforma for C1, C2, C3

Index	Service Element	Status	Support	
SE0	Confidentiality	o.1	Y	N
SE1	Connection Confidentiality	SE0:m	Y	N
SE2	Connectionless Confidentiality	-		
SE3	Integrity	o.1	Y	N
SE4	Connection Integrity w Recovery	-		
SE5	Connection Integrity wo Recovery	SE3:o.2	Y	N
SE6	Connectionless Integrity	SE3:o.2	Y	N
SE7	Data Origination Authentication	o	Y	N
SE8	Access Control	o	Y	N

Table 6: Service Element Proforma for C4

Index	Service Element	Status	Support	
SE0	Confidentiality	o.1	Y	N
SE1	Connection Confidentiality	SE0:m	Y	N
SE2	Connectionless Confidentiality	-		
SE3	Integrity	o.1	Y	N
SE4	Connection Integrity w Recovery	SE3:o.2	Y	N
SE5	Connection Integrity wo Recovery	-		
SE6	Connectionless Integrity	SE3:o.2	Y	N
SE7	Data Origination Authentication	o	Y	N
SE8	Access Control	o	Y	N

Table 7: Service Element Proforma for C4L

Index	Service Element	Status	Support	
SE0	Confidentiality	o.1	Y	N
SE2	Connectionless Confidentiality	SE0:m	Y	N
SE1	Connection Confidentiality	–		
SE3	Integrity	o.1	Y	N
SE4	Connection Integrity w Recovery	–		
SE5	Connection Integrity wo Recovery	–		
SE6	Connectionless Integrity	SE3:m	Y	N
SE7	Data Origination Authentication	o	Y	N
SE8	Access Control	o	Y	N

The following table identifies for connectionless Transport (CLTP::), the security services available through the TLSP and their level of support within the implementation.

Table 8: Service Element Proforma for CLTP

Index	Service Element	Status	Support	
SE0	Confidentiality	o.1	Y	N
SE1	Connection Confidentiality	–		
SE2	Connectionless Confidentiality	SE0:m	Y	N
SE3	Integrity	o.1	Y	N
SE4	Connection Integrity w Recovery	–		
SE5	Connection Integrity wo Recovery	–		
SE6	Connectionless Integrity	SE3:m	Y	N
SE7	Data Origination Authentication	o	Y	N
SE8	Access Control	o	Y	N

A.6 Supported Functions

The following set of tables identify the mandatory and optional functions implemented for each class of Transport (COTP::) supported.

Table 9: Mandatory Functions for C0

Index	Function	Ref
T0F1	verification of peer address	5.6.2,6.4
T0F2	reflection detection	5.6.2,6.3.2
T0F3	security encapsulation	5.6
T0F4	reporting of security events	Notes

Table 10: Optional Functions for C0

Index	Function	Ref	Status	Support	
T0F5	data encipherment	6.2	o.1	Y	N
T0F6	integrity protection	6.3	o.1	Y	N
T0F7	padding	6.6	o	Y	N
T0F8	explicit security labeling	6.5	o	Y	N

Table 11: Mandatory Functions for C1

Function	Ref
verification of peer address	5.6.2,6.4
reflection detection	5.6.2,6.3.2
separation after decapsulation	6.1
security encapsulation	5.6
reporting of security events	Notes

Table 12: Optional Functions for C1

Function	Ref	Status	Support	
data encipherment	6.2	o.1	Y	N
integrity protection	6.3	o.1	Y	N
integrity sequence number space	6.3.3	o	Y	N
pre-encapsulation concatenation	6.1	o	Y	N
data encipherment padding	6.6	o	Y	N
explicit security labeling	6.5	o	Y	N

Table 13: Mandatory Functions for C2, C3

Function	Ref
verification of peer address	5.6.2,6.4
reflection detection	5.6.2,6.3.2
separation after decapsulation	6.1
secure multiplexing	Implicit
security encapsulation	5.6
reporting of security events	Notes

Table 14: Optional Functions for C2, C3

Function	Ref	Status	Support	
data encipherment	6.2	o.1	Y	N
integrity protection	6.3	o.1	Y	N
integrity sequence number space	6.3.3	o	Y	N
pre-encapsulation concatenation	6.1	o	Y	N
data encipherment padding	6.6	o	Y	N
explicit security labeling	6.5	o	Y	N

Table 15: Mandatory Functions for C4, C4L

Function	Ref
verification of peer address	5.6.2,6.4
reflection detection	5.6.2,6.3.2
integrity sequence number space	5.6.2,6.3.3
separation after decapsulation	6.1
secure multiplexing	Implicit
security encapsulation	5.6
reporting of security events	Notes

Table 16: Optional Functions for C4, C4L

Function	Ref	Status	Support	
data encipherment	5.6.1,6.2	o.1	Y	N
integrity protection	5.6.2,6.3	o.1	Y	N
pre-encapsulation concatenation	6.1	o	Y	N
padding	5.6.4,6.6	o	Y	N
explicit security labeling	5.6.3,6.5	o	Y	N

The following table identifies the mandatory and optional functions implemented for connectionless Transport (CLTP::).

Table 17: Mandatory Functions for CLTP

Index	Function	Ref
T0F1	verification of peer address	5.6.2,6.4
T0F2	reflection detection	5.6.2,6.3.2
T0F3	security encapsulation	5.6
T0F4	reporting of security events	Notes

Table 18: Optional Functions for CLTP

Index	Function	Ref	Status	Support	
T0F5	data encipherment	6.2	o.1	Y	N
T0F6	integrity protection	6.3	o.1	Y	N
T0F7	padding	6.6	o	Y	N
T0F8	explicit security labeling	6.5	o	Y	N

A.7 Supported Protocol Data Units (PDUs)

A.7.1 Supported Transport PDUs (TPDUs)

As indicated in Table 19 below the SE TPDU is supported for both transmission and receipt, for both the connection oriented (COTP::) and connectionless Transport Protocol (CLTP::).

Table 19: TPDUs Supported

TPDU	Item	Status
SE	transmission	C1-4, C4L, or CLTP:m
SE	receipt	C1-4, C4L, or CLTP:m

A.7.2 Supported Parameters of Issued TPDUs

The following tables indicate which parameters are mandatory or optional when a SE TPDU is issued by Transport (COTP:: or CLTP::).

Table 20: Mandatory Parameters for C0-4, CL4, CLTP

Parameter	Ref
Key Identifier must be present.	6.2,6.3
Bit one of Protected Header Flag must be set as direction indicator.	8.2.2.1

Table 21: Optional Parameters for C0-4, CL4, CLTP

Parameter	Ref	Status	Support	
Label	8.2.2	o	Y	N
Pad	8.2.2	o	Y	N
ICV	8.2.4	o	Y	N

A.7.3 Supported Parameters of Received TPDUs

Implementations shall be capable of receiving and processing all possible parameters of the SE TPDU as indicated in table 22 below.

Table 22: Mandatory Parameters for C0-4, CL4, CLTP

Parameter	Ref
Key Identifier must be present.	6.2,6.3
Bit one of Protected Header Flag must be set as direction indicator.	8.2.2.1
Label	8.2.2
Pad	8.2.2
ICV	8.2.4

A.7.4 Allowed Values of Issued TPDU Parameters

Table 23: Values for Parameters of Issued TPDUs for C0-4, C4L, CLTP

Parameter	Values	
	Allowed	Supported
SA-ID	2-126 octets	
Prot Header Flags	0 or 1	
Label		
Defining Authority	1-n octets	
Value	1-m octets	
Padding		
Length	1-254	
Value	1-254 octets	
ICV	1-indef octets	

Note: Field sizes must meet the following length restrictions (n-2) + (m-2) + (Length-1) <= 254

A.7.5 Allowed Values of Received TPDU Parameters

Table 24: Values for Parameters of Issued TPDUs for C0-4, C4L, CLTP

Parameter	Values	
	Allowed	Supported
Key Identifier	1-254 octets	
Prot Header Flags	0 or 1	
Label		
Defining Authority	1-n octets	
Value	1-m octets	
Padding		
Length	1-254	
Value	1-254 octets	
ICV	1-indef octets	

Note: Field sizes must meet the following length restrictions (n-2) + (m-2) + (Length-1) <= 254

A.8 Service, Function, AND Protocol Relationships

A.8.1 Relationship Between Services and Functions

Table 25 below gives a mapping between OSI security services provided by TLSP and the associated functions needed in an implementation. The consistency between supported functions and security services shall be maintained accordingly.

Table 25: Mapping of Security Services to Supported Functions

Security Service	Functions
Confidentiality	data encipherment padding
Connection Integrity	integrity sequence number space integrity protection reflection detection padding
Connectionless Integrity	integrity protection reflection detection padding
Data Orig. Authentication	verification of peer address security encapsulation use of either: integrity protection or data encipherment
Access Control	explicit security labeling secure multiplexing security encapsulation

A.8.2 Relationship Between Services and Protocol

Table 26 below gives a mapping between OSI security services provided by TLSP and the SE TPDU protocol control information (PCI) and parameter fields employed by the underlying security mechanisms. The consistency between supported security parameters and SE TPDU parameter fields shall be maintained accordingly.

Table 26: Mapping of Security Services to SE TPDU Parameters

Security Service	TPDU Parameters/PCI
Confidentiality	encrypted data confidentiality padding
Connectionless Integrity	integrity check value direction indicator integrity padding
Connection Integrity	integrity check value direction indicator integrity padding DT/ED send sequence number (final sequence number)
Data Orig. Authentication	peer address key identifier key identifier employed in: integrity check value or encrypted data
Access Control	security labels key identifier key identifier employed in: integrity check value or encrypted data

A.9 Allowed Algorithms

Table 27 identifies the set of confidentiality and integrity algorithms supported by the implementation.

Table 27: Supported Algorithms

Item	Algorithm Identifier	
List of algorithms supported under the registration scheme defined in ISO/IEC 9979.		
	Note:	
The following three are examples of algorithms that could be used.		
	Allowed	Supported
Data Encryption	DES CBC mode	_____
MAC ICV	ANSI 9.9 (FIPS 113)	_____
MDC ICV	_____	_____