

Implementation of
ISO/IEC 10736:1995

**Information
technology —
Telecommunications
and information
exchange between
systems —
Transport layer
security protocol**

Committees responsible for this British Standard

The preparation of this British Standard was entrusted to Technical Committee IST/6 Data communications, upon which the following bodies were represented:

- British Computer Society
- British Telecommunications
- CCTA (Government Centre for Information Systems)
- Digital Equipment Co. Ltd.
- IBM United Kingdom Ltd.
- Institution of Electrical Engineers
- International Computers Limited
- Logica UK Ltd.
- Nine Tiles Computer Systems Ltd.
- Rank Xerox (UK) Ltd.

This British Standard, having been prepared under the direction of the Information Systems Technology Assembly, was published under the authority of the Standards Board and comes into effect on 15 September 1995

© BSI 01-2000

The following BSI references relate to the work on this standard:
Committee reference IST/6
Draft for comment 91/69325 DC

ISBN 0 580 24459 8

Amendments issued since publication

Amd. No.	Date	Comments

Contents

	Page
Committees responsible	Inside front cover
National foreword	ii
Foreword	vii
Text of ISO/IEC 10736	1

National foreword

This British Standard reproduces verbatim ISO/IEC 10736:1995 and implements it as the UK national standard.

This British Standard is published under the direction of the Information Systems Technology Assembly whose Technical Committee IST/6, Data communications, has the responsibility to:

- aid enquirers to understand the text;
- present to the responsible international committee any enquiries on interpretation, or proposals for change, and keep UK interests informed;
- monitor related international and European developments and promulgate them in the UK.

NOTE International and European Standards, as well as overseas standards, are available from Customer Services, BSI, 389 Chiswick High Road, London W4 4AL.

A British Standard does not purport to include all the necessary provisions of a contract. Users of British Standards are responsible for their correct application.

Compliance with a British Standard does not of itself confer immunity from legal obligations.

Summary of pages

This document comprises a front cover, an inside front cover, pages i and ii, the ISO/IEC title page, pages ii to viii, pages 1 to 48 and a back cover.

This standard has been updated (see copyright date) and may have had amendments incorporated. This will be indicated in the amendment table on the inside front cover.

INTERNATIONAL STANDARD

ISO/IEC 10736

First edition
1995-04-15

Information technology — Telecommunications and information exchange between systems — Transport layer security protocol

*Technologies de l'information — Télécommunications et échange
d'information entre systèmes — Protocole de sécurité de la couche
transport*



Reference number
ISO/IEC 10736:1995(E)

Contents

	Page
Foreword	vii
Introduction	1
1 Scope	1
2 Normative references	2
2.1 Identical Recommendations International Standards	2
2.2 Paired Recommendations International Standards equivalent in technical content	2
2.3 Additional references	2
3 Definitions	3
3.1 Security reference model definitions	3
3.2 Additional definitions	3
4 Symbols and abbreviations	4
5 Overview of the Protocol	5
5.1 Introduction	5
5.2 Security Associations and attributes	6
5.2.1 Security services for connection-oriented Transport protocol	9
5.2.2 Security Service for connectionless Transport protocol	9
5.3 Service assumed of the Network Layer	9
5.4 Security management requirements	9
5.5 Minimum algorithm characteristics	10
5.6 Security encapsulation function	10
5.6.1 Data encipherment function	10
5.6.2 Integrity function	10
5.6.3 Security label function	11
5.6.4 Security padding function	11
5.6.5 Peer Entity Authentication function	11
5.6.6 SA Function using in band SA-P	11
6 Elements of procedure	11
6.1 Concatenation and separation	12
6.2 Confidentiality	12
6.2.1 Purpose	12
6.2.2 TPDUs and parameters used	12
6.2.3 Procedure	12
6.3 Integrity processing	13
6.3.1 Integrity Check Value (ICV) processing	13
6.3.1.1 Purpose	13
6.3.1.2 TPDUs and parameters used	13
6.3.1.3 Procedure	13
6.3.2 Direction indicator processing	15
6.3.2.1 Purpose	15
6.3.2.2 TPDUs and parameters used	15
6.3.2.3 Procedure	15
6.3.3 Connection integrity sequence number processing	15
6.3.3.1 Unique sequence numbers	15
6.3.3.2 Purpose	16
6.3.3.3 Procedure	16
6.4 Peer address check processing	16
6.4.1 Purpose	16
6.4.2 Procedure	16
6.5 Security labels for Security Associations	16

	Page
6.5.1 Purpose	16
6.5.2 TPDUs and parameters used	16
6.5.3 Procedure	17
6.6 Connection release	17
6.7 Key replacement	17
6.8 Unprotected TPDUs	17
6.9 Protocol identification	17
6.10 Security Association-Protocol	17
7 Use of elements of procedure	18
8 Structure and encoding of TPDUs	18
8.1 Structure of TPDU	18
8.2 Security encapsulation TPDU	19
8.2.1 Clear header	19
8.2.1.1 PDU clear header length	19
8.2.1.2 PDU type	19
8.2.1.3 SA-ID	19
8.2.2 Crypto sync	19
8.2.3 Protected contents	20
8.2.3.1 Structure of protected contents field	20
8.2.3.2 Content length	20
8.2.3.3 Flags	21
8.2.3.4 Label	21
8.2.3.5 Protected data	21
8.2.3.6 Integrity PAD	21
8.2.4 ICV	22
8.2.5 Encipherment PAD	22
8.3 Security Association PDU	22
8.3.1 LI	22
8.3.2 PDU Type	22
8.3.3 SA-ID	22
8.3.4 SA-P Type	22
8.3.5 SA PDU Contents	22
9 Conformance	23
9.1 General	23
9.2 Common static conformance requirements	23
9.3 TLSP with ITU-T Rec. X.234 ISO 8602 static conformance requirements	23
9.4 TLSP with ITU-T Rec. X.224 ISO/IEC 8073 static conformance requirements	23
9.5 Common dynamic conformance requirements	23
9.6 TLSP with ITU-T Rec. X.234 ISO 8602 dynamic conformance requirements	23
9.7 TLSP with ITU-T Rec. X.224 ISO/IEC 8073 dynamic conformance requirements	23
10 Protocol implementation conformance statement (PICS)	23
Annex A PICS proforma	24
A.1 Introduction	24
A.1.1 Background	24
A.1.2 Approach	24

	Page
A.2	Implementation identification
A.3	General statement of conformance
A.4	Protocol implementation
A.5	Security services supported
A.6	Supported functions
A.7	Supported Protocol Data Units (PDUs)
A.7.1	Supported Transport PDUs (TPDUs)
A.7.2	Supported parameters of issued TPDUs
A.7.3	Supported parameters of received TPDUs
A.7.4	Allowed values of issued TPDU parameters
A.8	Service, function, and protocol relationships
A.8.1	Relationship between services and functions
A.8.2	Relationship between services and protocol
A.9	Supported algorithms
A.10	Error handling
A.10.1	Security errors
A.10.2	Protocol errors
A.11	Security Association
A.11.1	SA Generic Fields
A.11.2	Content Fields Specific to Key Exchange SA-P
Annex B	Security Association Protocol Using Key Token Exchange and Digital Signatures
B.1	Overview
B.2	Key Token Exchange (KTE)
B.3	SA-Protocol Authentication
B.4	SA Attribute Negotiation
B.4.1	Service Negotiation
B.4.2	Label Set Negotiation
B.4.3	Key and ISN Selection
B.4.4	Miscellaneous SA Attribute Negotiation
B.4.5	Re-keying Overview
B.4.6	SA Abort/Release Overview
B.5	Mapping of SA-Protocol Functions to Protocol Exchanges
B.5.1	KTE (First) Exchange
B.5.1.1	Request to Initiate the SA-Protocol
B.5.1.2	Receipt of the First Exchange PDU by Recipient
B.5.2	Authentication and Security Negotiation (Second) Exchange
B.5.2.1	Receipt of First Exchange PDU by Initiator
B.5.2.2	Receipt of the Second Exchange PDU by Recipient
B.5.3	Rekey Procedure
B.5.4	SA Release/Abort Exchange
B.5.4.1	Request to Initiate SA Release/Abort
B.5.4.2	Receipt of SA Abort/Release Requests
B.6	SA PDU — SA Contents
B.6.1	Exchange ID
B.6.2	Content Length
B.6.3	Content Fields
B.6.3.1	My SA-ID

	Page
B.6.3.2 Old Your SA-ID	44
B.6.3.3 Key Token 1, Key Token 2, Key Token 3, and Key Token 4	44
B.6.3.4 Authentication Digital Signature, Certificate	44
B.6.3.5 Service Selection	44
B.6.3.6 SA Rejection Reason	44
B.6.3.7 SA Abort/Release Reason	45
B.6.3.8 Label	45
B.6.3.9 Key Selection	45
B.6.3.10 SA Flags	46
B.6.3.11 ASSR	46
Annex C An example of an agreed set of security rules (ASSR)	46
Annex D Overview of EKE Algorithm	47
Figure 1 — TLSP with ITU-T Rec. X.234 ISO 8602	6
Figure 2 — TLSP with ITU-T Rec. X.224 ISO/IEC 8073	6
Figure 3 — Illustration of exchanges to support peer entity authentication	11
Figure 4 — TLSP Encapsulation Methods (TLSP's method for encapsulation and encipherment in support of Confidentiality as indicated in 6.2)	13
Figure 5 — TLSP Encapsulation Methods (TLSP's method for encapsulation and ICV generation in support of integrity as indicated in 6.3)	14
Figure 6 — TLSP Encapsulation Method (TLSP's method for encapsulation and ICV generation in support of "Integrity and Confidentiality" as indicated in 6.2 and 6.3)	15
Figure 7 — Structure of the TPDU	19
Figure 8 — Format of the clear header	19
Figure 9 — Protected contents	20
Figure 10 — Flags field	21
Figure 11 — Format of the label field	21
Figure 12 — Format of the protected data field	21
Figure 13 — SA PDU Structure	22
Figure B.2 — SA Contents	43
Figure D.1 — Illustration of On-Line Key Derivation and Digital Signature using EKE	48
Table 1 — TLSP elements of procedure	18
Table A.1 — TLSP Implementation Identification	25
Table A.2 — General Conformance Statement	25
Table A.3 — CO and CL Transport Implemented	25
Table A.4 — Service Element Proforma for CO	26
Table A.5 — Service Element Proforma for C1, C2, C3	26
Table A.6 — Service Element Proforma for C4	26
Table A.7 — Service Element Proforma for C4L	27
Table A.8 — Service Element Proforma for CLTP	27
Table A.9 — Mandatory Functions for C0	27
Table A.10 — Optional Functions for C0	27
Table A.11 — Mandatory Functions for C1	28
Table A.12 — Optional Functions for C1	28
Table A.13 — Mandatory Functions for C2, C3	28

	Page
Table A.14 — Optional Functions for C2, C3	28
Table A.15 — Mandatory Functions for C4, C4L	29
Table A.16 — Optional Functions for C4, C4L	29
Table A.17 — Mandatory Functions for CLTP	29
Table A.18 — Optional Functions for CLTP	29
Table A.19 — TPDUs Supported	30
Table A.20 — Mandatory Parameters for COTP, CLTP	30
Table A.21 — Optional Parameters for COTP, CLTP	30
Table A.22 — Mandatory parameters for COTP, CLTP	30
Table A.23 — Values for Parameters of issued TPDUs for COTP, CLTP	31
Table A.24 — Values for parameters of received TPDUs for COTP, CLTP	31
Table A.25 — Mapping of security services to supported functions	32
Table A.26 — Mapping of security services to SE TPDU parameters	32
Table A.27 — Supported algorithms	33
Table A.28 — Mandatory security error actions for COTP, CLTP	33
Table A.29 — Protocol error actions for COTP, CLTP	33
Table A.30	34
Table A.31	35

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work.

In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

International Standard ISO/IEC 10736 was prepared by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*, in collaboration with ITU-T. The identical text is published as ITU-T Recommendation X.274.

Annex A and Annex B form an integral part of this International Standard. Annex C and Annex D are for information only.

Introduction

The transport protocol specified in ITU-T Rec. X.224 | ISO/IEC 8073 provides the connection oriented transport service described in ITU-T Rec. 234 | ISO/IEC 8072. The transport protocol specified in ITU-T Rec. 234 | ISO/IEC 8602 provides the connectionless-mode transport service described in ISO/IEC 8072. This Recommendation | International Standard specifies optional additional functions to ITU-T Rec. X.224 | ISO/IEC 8073 and ITU-T Rec. X.234 | ISO/IEC 8602 permitting the use of cryptographic techniques to provide data protection for transport connections or for connectionless-mode TPDU transmission.

1 Scope

The procedures specified in this Recommendation | International Standard operate as extensions to those defined in ITU-T Rec. X.224 | ISO/IEC 8073 and ITU-T Rec. X.234 | ISO/IEC 8602 and do not preclude unprotected communication between transport entities implementing ITU-T Rec. X.224 | ISO/IEC 8073 or ITU-T Rec. X.234 | ISO 8602.

The protection achieved by the security protocol defined in this Recommendation | International Standard depends on the proper operation of security management including key management. However, this Recommendation | International 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 CCITT Rec. X.800 | 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 or established through the use of the Security Association — Protocol (SA-P).

Protection can be provided only within the context of a security policy.

This protocol supports peer-entity authentication at the time of connection establishment. In addition, rekeying is supported within the protocol through the use of SA-P or through means outside the protocol. Security associations can only be established within the context of a security policy. It is a matter for the users to establish their own security policy, which may be constrained by the procedures specified in this Recommendation | International Standard.

The following items could be included in a Security Policy:

- a) the method of SA establishment/release, the lifetime of SA;
- b) Authentication/Access Control mechanisms;
- c) Label mechanism;
- d) the procedure of the receiving an invalid TPDU during SA establishment procedure or transmission of protected PDU;
- e) the lifetime of Key;
- f) the interval of the rekey procedure in order to update key and security control information (SCI) exchange procedure;
- g) the time out of SCI exchange and rekey procedure;
- h) the number of retries of sci exchange and rekey procedure.

This Recommendation | International Standard defines a protocol which may be used for Security Association establishment. Entities wishing to establish an SA must share common mechanisms for authentication and key distribution. This Recommendation | International Standard specifies one algorithm for authentication and key distribution which is based on public key crypto systems. The implementation of this algorithm is not mandatory; however, when an alternative mechanism is used, it shall satisfy the following conditions:

- a) All SA attributes defined in 5.2 are derived.
- b) Derived keys are authenticated.

2 Normative references

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | International Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this Recommendation | International Standard are encouraged to investigate the possibility of applying the most recent editions of the standards listed below. Members of IEC and ISO maintain registers of currently valid International Standards. The Telecommunication Standardization Bureau of the ITU maintains a list of currently valid ITU-T Recommendations.

2.1 Identical Recommendations | International Standards

- ITU-T Recommendation X.214:1993 | ISO 8072:1994, *Information technology — Open Systems Interconnection — Transport service definition*.
- ITU-T Recommendation X.234:1993 | ISO/IEC 8602:1995, *Information technology — Protocol for providing the OSI connectionless-mode transport service*.

2.2 Paired Recommendations | International Standards equivalent in technical content

- CCITT Recommendation X.200:1988, *Reference Model of Open Systems Interconnection for CCITT applications*.
- ISO/IEC 7498-1:1994, *Information technology — Open Systems Interconnection — Basic Reference Model — Part 1: The Basic Model*.
- CCITT Recommendation X.800:1991, *Security architecture for Open Systems Interconnection for CCITT applications*.
- ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*.
- ITU-T Recommendation X.224:1993, *Protocol for providing the OSI connection-mode transport service*.
- ISO/IEC 8073:1992, *Information technology — Telecommunications and information exchange between systems — Open Systems Interconnection — Protocol for providing the connection-mode transport service*.
- CCITT Recommendation X.208:1988, *Specification of Abstract Syntax Notation One (ASN.1)*.
- ISO/IEC 8824:1990, *Information technology — Open Systems Interconnection — Specification of Abstract Syntax Notation One (ASN.1)*.
- CCITT Recommendation X.209:1988, *Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)*.
- ISO 8825:1990, *Information technology — Open Systems Interconnection — Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)*.
- ITU-T Recommendation X.264:1993, *Transport protocol identification mechanism*.
- ISO/IEC 11570:1992, *Information technology — Telecommunications and information exchange between systems — Open Systems Interconnection — Transport protocol identification mechanism*.

2.3 Additional references

- ISO/IEC 9834-1:1993, *Information technology — Open Systems Interconnection — Procedures for the operation of OSI Registration Authorities: General Procedures*.
- ISO/IEC 9834-3:1990, *Information technology — Open Systems Interconnection — Procedures for the operation of OSI Registration Authorities — Part 3: Registration of object identifier component values for joint ISO-CCITT use*.

3 Definitions

This Recommendation | International Standard is based on the concepts developed in the Reference Model for Open Systems Interconnection (CCITT Rec. X.200 | ISO 7498-1) as well as CCITT Rec. X.800 | ISO 7498-2 on Security Architecture.

3.1 Security reference model definitions

This Recommendation | International Standard makes use of the following terms as defined in CCITT Rec. X.800 | 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) security policy;
- m) symmetric.

3.2 Additional definitions

For the purposes of this Recommendation | International Standard, the following definitions apply:

3.2.1

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

3.2.2

in-band protocol mechanism

a protocol mechanism defined in this recommendation | International Standard

3.2.3

out-of-band protocol mechanism

a protocol mechanism not defined in this Recommendation | International Standard

3.2.4

pairwise key

a pair of related (Public Key) or identical key (Secret Key) values generated for use between two particular parties

3.2.5

reflection protection

a protection mechanism to detect when a protocol data unit has been sent back to the originator

3.2.6

security association

the relationship between communicating entities for which there exists corresponding SA-Attributes

3.2.7

security association attributes

the collection of information required to control the security of communications between an entity and its remote peer(s)

3.2.8

SE TPDU

the encapsulated TPDU for security in order to send the TPDU defined in ITU-T Rec. X.224 | ISO/IEC 8073 or ITU-T Rec. X.234 | ISO 8602 after securing it

4 Symbols and abbreviations

This Recommendation | International Standard makes use of the following abbreviations from clause 4 of ITU-T Rec X.224 | ISO/IEC 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	Expedited Data TPDU number (field)
ER TPDU	Error TPDU
LI	Length indicator (field)
NC	Network Connection
SN	Sequence Number
SRC-REF	Source Reference (field)
TC	Transport Connection
TPDU	Transport protocol data unit
TPDU-NR	DT TPDU number (field)

Additionally, the following abbreviations are used in this Recommendation | International Standard:

CBTSS	Connection Based Transport Security Service
Conf_no	Confidentiality is not to be provided
Conf_yes	Confidentiality is to be provided
DEK	Data Encipherment Key
GTSS	General Transport Security Service
ICV	Integrity Check Value
Integ_no	Integrity is not to be provided
Integ_yes	Integrity is to be provided
KEK	Key Encipherment Key
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
MAC	Message Authentication Code
MDC	Manipulation Detection Code
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 TPDU's
Ppl_pres	Security Label used on every TPDU
SA-P	Security Association — Protocol
SE TPDU	Security Encapsulation TPDU
TLSP	Transport Layer Security Protocol

5 Overview of the Protocol

5.1 Introduction

CCITT Rec. X.800 | 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 ITU-T Rec. X.214 | 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.

CCITT Rec. X.800 | 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.

A Defect Report has been raised on ITU-T Rec. X.214 | ISO 8072 to allow these and possibly other forms of protection.

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

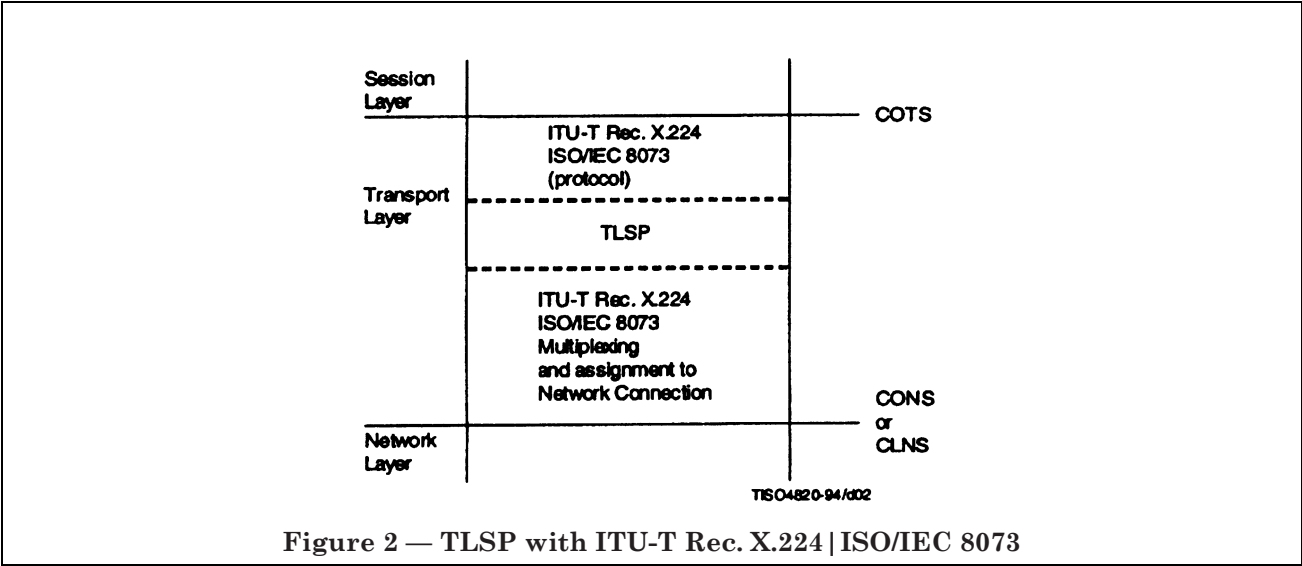
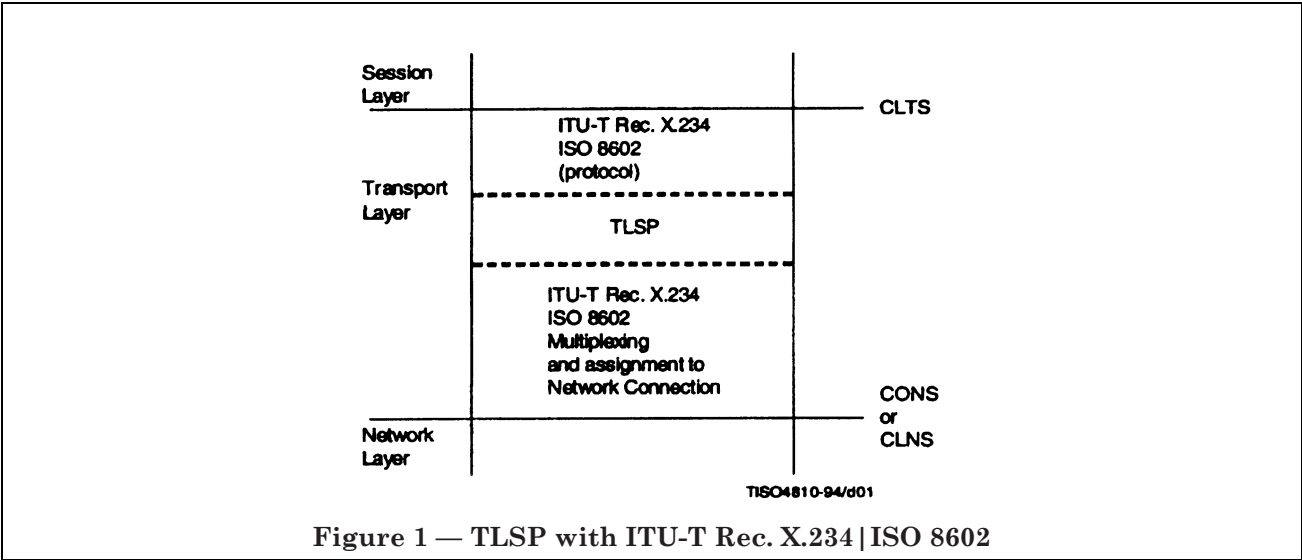
TLSP used with ITU-T Rec. X.224 | ISO/IEC 8073 can support connection integrity with and without recovery, connection confidentiality, access control service and peer entity authentication with each connection individually protected. However, a key may be shared between several connections.

TLSP used with ITU-T Rec. X.234 | ISO 8602 can support connectionless integrity, connectionless confidentiality, access control service and data origin authentication.

This Recommendation | International Standard 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.

Figure 1 and Figure 2 show the location of TLSP in the seven layer ISO model.



5.2 Security Associations and attributes

The specific TLSP processing options used in an instance of communications are determined by the set of security attributes including pairwise protection keys. TLSP assumes that two transport entities share a set of corresponding attributes. The Security Association identifier SA-ID, identifies a set of attributes which may be used to protect an instance of communication.

Each security association is defined by a set of attributes at each end system. The means of establishing all of the attributes which are to be used in an association is currently outside the scope of this Specification. Some could be established by manual exchange of attributes and some of these could be established through use of an Agreed Set of Security Rules (ASSR). An ASSR is a common set of rules which specify the security mechanisms to be used, including all parameters needed to define the operation of the mechanism for a given protection service(s). Security rules and their identifiers may be registered by third parties. See Annex B for an illustrative example of an ASSR.

Other attributes such as lifetime and timeout of rekey procedure may be defined under the security policy. 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 set of attributes appropriate for two communicating end systems is dependant on mechanisms used and the security policy.

a) SA Identification

- | | | |
|----------------|--------------|--|
| 1) Local_SAID: | Octet String | The local identifier of the SA. |
| 2) Peer_SAID: | Octet String | The remote peer identifier of the SA. |
| 3) SAID_Len: | Integer | Length of the SAID defined by the ASSR
Integer of range 2 to 126. |

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

When a TLSP entity determines that a particular SA is discontinued, it shall place the SA-ID which it has allocated in a frozen state. While frozen, the SA-ID shall not be re-used. The period in which the SA-ID is frozen shall be greater than the lifetime of the PDU(s) of the underlying network.

b) Indicator of which TLSP entity takes on the role of “initiator” and which entity takes on the role of “responder”. This attribute indicates how the direction indicator should be set to detect reflected TPDUs.

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 identifier via the local and remote transport reference numbers, 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 CCITT Rec. X.208 | 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 ITU-T Rec. X.234 | 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 ITU-T Rec. X.224 | ISO/IEC 8073:

- 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.
- CLConf: (Connectionless Confidentiality level) Integer of range defined by ASSR.
- CLInt: (Connectionless Integrity level) Integer of range defined by ASSR.

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