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

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.

Annexes A and B form an integral part of this International Standard. Annexes C and 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.

INTERNATIONAL STANDARD

ITU-T RECOMMENDATION

INFORMATION TECHNOLOGY – TELECOMMUNICATIONS AND INFORMATION EXCHANGE BETWEEN SYSTEMS – TRANSPORT LAYER SECURITY PROTOCOL

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 TPDUs
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.

NOTES

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.

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.

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

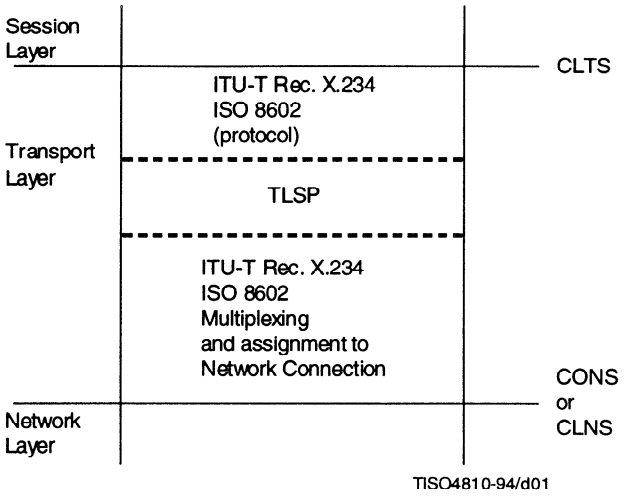

Figure 1 – TLSP with ITU-T Rec. X.234 | ISO 8602

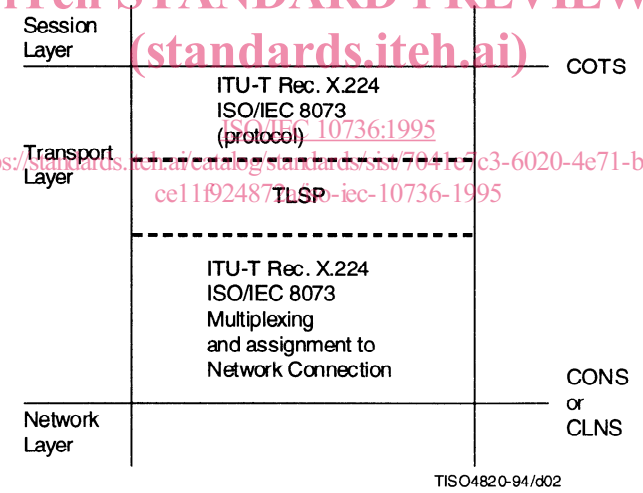

Figure 2 – TLSP with ITU-T Rec. X.224 | ISO/IEC 8073

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.

f) Mechanisms selected for the SA

– Label: Boolean – Explicit labelling TPDUs.

- Conf: Boolean – Confidentiality of a Secure Data Transfer by encipherment.
- ICV: check Boolean – Integrity of a Secure Data Transfer contents using an integrity value.
- SN: Boolean – Connection Integrity Sequence number procedure to be used.
- PE-Authentication: Boolean – Peer Entity Authentication using exchange of encapsulated Connect Request / Connect Response PDUs.
- UNProt: Boolean – Unprotected TPDUs.

g) Label mechanism attributes

The values of these attributes are set up on SA establishment or pre-established. This attribute specifies the set of allowable security labels for the security association.

Label_set: Set of {

Label_Ref: Integer
Label_Defining_Auth: Object Identifier
Label_Content: Format defined by Label_Defining_Auth

}

h) ICV mechanism attributes

- ICV_Alg: Object Identifier
- ICV_Len: Integer
- ICV_Blk: Integer Block size of padding for ICV algorithm

The following attributes are only present if the algorithm is cryptographic:

- 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 level A separate cryptographic key is used for each end system pair and security set.

The values of the above 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

i) SN Mechanism attributes

The following attributes are only relevant for TLSP used in conjunction with ITU-T Rec. X.224 | ISO/IEC 8073:

- Data_Local_SN: SN for last normal data sent
- Data_Peer_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 ITU-T Rec. X.224 | ISO/IEC 8073.

j) EXSN Mechanism attributes

The following attributes are only relevant for TLSP used in conjunction with ITU-T Rec. X.224 | ISO/IEC 8073:

- Data_Local_EXSN: EXSN for last expedited data sent
- Data_Peer_EXSN: EXSN for last expedited data received

The initial values of these attributes are set up as part of the expedited procedure. The EXSN is the sequence number used by ITU-T Rec. X.224 | ISO/IEC 8073.

k) Encipherment Mechanism Attributes

- Enc_Alg: Object identifier (e.g. allocated under ISO 9979)
- Enc_Blk: Integer Block size of padding for encipherment algorithm
- 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

NOTE – Additional mechanisms and attributes may be identified in future versions of this Recommendation | International Standard and or 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 SA-ID 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 SA-ID shall be created explicitly for the protected transport connection(s). The security services to be provided on the connection are those defined by 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 (ICV = True). 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 Recommendation | 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 an SA-ID 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 attributes associated with the SA-ID and shall place the peer identifier (SA-ID) in the SA-ID parameter of the SE TPDU. Upon receiving an SE TPDU, the key specified by 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 Recommendation | 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 Recommendation | International Standard or through the use of the SA-P.

The degree of protection achieved will depend upon proper management of security including key management. The procedures in this Recommendation | International Standard 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 are not available for both the sending and receiving TLSP entities. Either symmetric or asymmetric keying is allowed by this Recommendation | International Standard.

c) cryptographic keys are pairwise, see 3.2.4.

This Recommendation | International Standard does not define how the cryptographic keys are created, updated, or otherwise managed.