This is a preview - click here to buy the full publication

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)

This is a preview - click here to buy the full publication

Contents

		Page
1	Scope	1
2	Normative references	2
2.1	Identical Recommendations I International Standards	2
2.2	Paired Recommendations I 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	3
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	10
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	16
6.3.3.1	Unique sequence numbers	16

© ISO/IEC 1995
All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from the publisher.

ISO/IEC Copyright Office • Case postale 56 • CH-1211 Genève 20 • Switzerland

Printed in Switzerland

This is a preview - click here to buy the full publication

Page

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 ... 17
6.5.1 Purpose ... 17
6.5.2 TPDUs and parameters used ... 17
6.5.3 Procedure ... 17
6.6 Connection release ... 17
6.7 Key replacement ... 17
6.8 Unprotected TPDUs ... 17
6.9 Protocol identification ... 18
6.10 Security Association-Protocol ... 18
7 Use of elements of procedure ... 19
8 Structure and encoding of TPDUs ... 19
8.1 Structure of TPDU ... 19
8.2 Security encapsulation TPDU ... 19
8.2.1 Clear header ... 20
8.2.1.1 PDU clear header length ... 20
8.2.1.2 PDU type ... 20
8.2.1.3 SA-ID ... 20
8.2.2 Crypto sync ... 20
8.2.3 Protected contents ... 20
8.2.3.1 Structure of protected contents field ... 21
8.2.3.2 Content length ... 21
8.2.3.3 Flags ... 21
8.2.3.4 Label ... 22
8.2.3.5 Protected data ... 22
8.2.3.6 Integrity PAD ... 22
8.2.4 ICV ... 22
8.2.5 Encipherment PAD ... 23
8.3 Security Association PDU ... 23
8.3.1 LI ... 23
8.3.2 PDU Type ... 23
8.3.3 SA-ID ... 23
8.3.4 SA-P Type ... 23
8.3.5 SA PDU Contents ... 23
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 ... 24
9.4 TLSP with ITU-T Rec. X.224 | ISO/IEC 8073 static conformance requirements ... 24
9.5 Common dynamic conformance requirements ... 24
9.6 TLSP with ITU-T Rec. X.234 | ISO 8602 dynamic conformance requirements ... 24
9.7 TLSP with ITU-T Rec. X.224 | ISO/IEC 8073 dynamic conformance requirements ... 24
10 Protocol implementation conformance statement (PICS) ... 24
Annex A – PICS proforma ... 25
A.1 Introduction ... 25
A.1.1 Background ... 25
A.1.2 Approach ... 25
A.2 Implementation identification ... 26
A.3 General statement of conformance ... 26
A.4 Protocol implementation ... 26

This is a preview - click here to buy the full publication

Page

A.5 Security services supported ... 27
A.6 Supported functions ... 28
A.7 Supported Protocol Data Units (PDUs) ... 31
A.7.1 Supported Transport PDUs (TPDUs) ... 31
A.7.2 Supported parameters of issued TPDUs ... 31
A.7.3 Supported parameters of received TPDUs ... 31
A.7.4 Allowed values of issued TPDU parameters ... 32
A.8 Service, function, and protocol relationships ... 33
A.8.1 Relationship between services and functions ... 33
A.8.2 Relationship between services and protocol ... 33
A.9 Supported algorithms ... 34
A.10 Error handling ... 34
A.10.1 Security errors ... 34
A.10.2 Protocol errors ... 35
A.11 Security Association ... 35
A.11.1 SA Generic Fields ... 35
A.11.2 Content Fields Specific to Key Exchange SA-P ... 36

Annex B – Security Association Protocol Using Key Token Exchange and Digital Signatures ... 37
B.1 Overview ... 37
B.2 Key Token Exchange (KTE) ... 38
B.3 SA-Protocol Authentication ... 38
B.4 SA Attribute Negotiation ... 39
B.4.1 Service Negotiation ... 39
B.4.2 Label Set Negotiation ... 39
B.4.3 Key and ISN Selection ... 39
B.4.4 Miscellaneous SA Attribute Negotiation ... 40
B.4.5 Re-keying Overview ... 40
B.4.6 SA Abort/Release Overview ... 40
B.5 Mapping of SA-Protocol Functions to Protocol Exchanges ... 40
B.5.1 KTE (First) Exchange ... 40
B.5.1.1 Request to Initiate the SA-Protocol ... 40
B.5.1.2 Receipt of the First Exchange PDU by Recipient ... 41
B.5.2 Authentication and Security Negotiation (Second) Exchange ... 41
B.5.2.1 Receipt of First Exchange PDU by Initiator ... 41
B.5.2.2 Receipt of the Second Exchange PDU by Recipient ... 42
B.5.3 Rekey Procedure ... 42
B.5.4 SA Release / Abort Exchange ... 43
B.5.4.1 Request to Initiate SA Release / Abort ... 43
B.5.4.2 Receipt of SA Abort/Release Requests ... 43
B.6 SA PDU – SA Contents ... 44
B.6.1 Exchange ID ... 44
B.6.2 Content Length ... 44
B.6.3 Content Fields ... 44
B.6.3.1 My SA-ID ... 45
B.6.3.2 Old Your SA-ID ... 45
B.6.3.3 Key Token 1, Key Token 2, Key Token 3, and Key Token 4 ... 45
B.6.3.4 Authentication Digital Signature, Certificate ... 45
B.6.3.5 Service Selection ... 45
B.6.3.6 SA Rejection Reason ... 45
B.6.3.7 SA Abort/Release Reason ... 46
B.6.3.8 Label ... 46
B.6.3.9 Key Selection ... 46
B.6.3.10 SA Flags ... 47
B.6.3.11 ASSR ... 47

Annex C – An example of an agreed set of security rules (ASSR) ... 48

Annex D – Overview of EKE Algorithm ... 49

This is a preview - click here to buy the full publication

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.

This is a preview - click here to buy the full publication

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.

This is a preview - click here to buy the full publication

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.

 This is a preview - click here to buy the full publication

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.*