

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

	<i>Page</i>
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	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