

AS/NZS 13594:1998
ISO/IEC TR 13594:1995

Australian/New Zealand Standard™

**Information technology—
Lower layers security**

AS/NZS 13594

STANDARDS AUSTRALIA 

STANDARDS NEW ZEALAND



Documents

Document Sharing Hub

AS/NZS 13594:1998

This Joint Australian/New Zealand Standard was prepared by Joint Technical Committee IT/1, Information Systems—Interconnection. It was approved on behalf of the Council of Standards Australia on 18 March 1998 and on behalf of the Council of Standards New Zealand on 20 July 1998. It was published on 5 September 1998.

The following interests are represented on Committee IT/1:

Australian Bankers Association
 Australian Bureau of Statistics
 Australian Computer Society
 Australian Computer Users Association
 Australian Information Industry Association
 Australian Vice Chancellors Committee
 Department of Defence, Australia
 Department of Industry, Science and Technology, Australia
 Government Computing Service, New Zealand
 Information Exchange Steering Committee, Australia
 Institute of Information and Communication Technologies, CSIRO, Australia
 Telecom New Zealand
 Telstra Corporation, Australia

Review of Standards. To keep abreast of progress in industry, Joint Australian/New Zealand Standards are subject to periodic review and are kept up to date by the issue of amendments or new editions as necessary. It is important therefore that Standards users ensure that they are in possession of the latest edition, and any amendments thereto.

Full details of all Joint Standards and related publications will be found in the Standards Australia and Standards New Zealand Catalogue of Publications; this information is supplemented each month by the magazines 'The Australian Standard' and 'Standards New Zealand', which subscribing members receive, and which give details of new publications, new editions and amendments, and of withdrawn Standards.

Suggestions for improvements to Joint Standards, addressed to the head office of either Standards Australia or Standards New Zealand, are welcomed. Notification of any inaccuracy or ambiguity found in a Joint Australian/New Zealand Standard should be made without delay in order that the matter may be investigated and appropriate action taken.

This Standard was issued in draft form for comment as DR 97539



Documents

Document Sharing Hub

AS/NZS 13594:1998

Australian/New Zealand Standard™

**Information technology—
Lower layers security**

First published as AS/NZS 13594:1998.

Published jointly by:

Standards Australia
1 The Crescent,
Homebush NSW 2140 Australia

Standards New Zealand
Level 10, Radio New Zealand House,
155 The Terrace,
Wellington 6001 New Zealand

PREFACE

This Standard was prepared by the Joint Standards Australia/Standards New Zealand Committee IT/1, Information Systems—Interconnection. It is identical with, and has been reproduced from, ISO/IEC TR 13594:1995, *Information technology—Lower layers security*.

The objective of this Standard is to provide a description of the cross layer aspects of the provision of security services in the lower layers of the OSI Reference model (transport, network, data link and physical layers).

As this Standard is reproduced from an international Standard, the following applies:

- (a) Its number does not appear on each page of text and its identity is shown only on the cover and title page.
- (b) In the source text 'this International Standard' should read 'this Australian/New Zealand Standard'.
- (c) A full point substitutes for a comma when referring to a decimal marker.

Reference to International Standard or other Publication

Australian/New Zealand Standard

ISO/IEC

AS/NZS

7498 Information technology—
Open Systems Interconnection—
Basic Reference Model

7498-1 Part 1: The Basic Model

8473 Information technology—
Protocol for providing the OSI
connectionless-mode Network service

8473-1 Part 1: Protocol specification

8602 Information technology—
Protocol for providing the OSI
connectionless-mode Transport service

10736 Information technology—
Telecommunications and information
exchange between systems—
Transport layer security protocol

10745 Information technology—
Open Systems Interconnection—
Upper layers security model

10181 Information technology—
Open Systems Interconnection—
Security frameworks in open systems

10181-1 Part 1: Security frameworks overview

10181-3 Part 3: Access control framework

2777 Information technology—
Open Systems Interconnection—
Basic reference model

2777.1 Part 1: The basic model

—

—

AS

3627 Information processing systems—
Open Systems Interconnection—
Protocol for providing the
connectionless-mode transport service

—

—

—

—

—

AS/NZS

11577 Information technology—
Open Systems Interconnection—
Network layer security protocol

4471 Information technology—
Open Systems Interconnection—
Network layer security protocol

CONTENTS

	<i>Page</i>
1 Scope	1
2 References	1
2.1 Identical Recommendations International Standards	1
2.2 Paired Recommendations International Standards equivalent in technical content	2
2.3 Additional references	2
3 Definitions	2
3.1 OSI Reference Model definitions	2
3.2 Open System Security Frameworks definitions	3
3.3 Internal Organization of the Network Layer definitions	3
3.4 Additional definitions	3
4 Abbreviations	3
5 Security associations	3
5.1 General overview	3
5.2 Establishing a security association for the lower layers	5
5.3 Security association close	6
5.4 Modification of attributes in a connection	6
6 Influence on existing protocols	6
6.1 General principle	6
6.2 Connectionless SDU size	6
6.3 Concatenation of PDUs	6
6.4 Algorithm and mechanism independence	6
7 Common security PDU structure	7
8 Determination of security services and mechanisms	7
9 Protection QOS	7
10 Security rules	7
11 Placement of security in the lower layers	7
12 Use of (N-1)-layer(s) to enhance (N)-layer security	13
13 Security labelling	13
14 Security domains	13
15 Security of routing	13
16 Security Management	14
16.1 Security policy	14
16.2 Security association management	14
16.3 Key management	14
16.4 Security Audit	14
17 Traffic flow confidentiality	14
18 Guidelines for the definition of SA-Attributes	15
19 Error handling	15
Annex A – Illustrative example of an Agreed Set of Security Rules	16

NOTES

© Copyright STANDARDS AUSTRALIA/STANDARDS NEW ZEALAND

Users of Standards are reminded that copyright subsists in all Standards Australia and Standards New Zealand publications and software. Except where the Copyright Act allows and except where provided for below no publications or software produced by Standards Australia or Standards New Zealand may be reproduced, stored in a retrieval system in any form or transmitted by any means without prior permission in writing from Standards Australia or Standards New Zealand. Permission may be conditional on an appropriate royalty payment. Australian requests for permission and information on commercial software royalties should be directed to the head office of Standards Australia. New Zealand requests should be directed to Standards New Zealand.

Up to 10 percent of the technical content pages of a Standard may be copied for use exclusively in-house by purchasers of the Standard without payment of a royalty or advice to Standards Australia or Standards New Zealand.

Inclusion of copyright material in computer software programs is also permitted without royalty payment provided such programs are used exclusively in-house by the creators of the programs.

Care should be taken to ensure that material used is from the current edition of the Standard and that it is updated whenever the Standard is amended or revised. The number and date of the Standard should therefore be clearly identified.

The use of material in print form or in computer software programs to be used commercially, with or without payment, or in commercial contracts is subject to the payment of a royalty. This policy may be varied by Standards Australia or Standards New Zealand at any time.

AUSTRALIAN/NEW ZEALAND STANDARD

INFORMATION TECHNOLOGY – LOWER LAYERS SECURITY

1 Scope

This Recommendation | Technical Report describes the cross layer aspects of the provision of security services in the lower layers of the OSI Reference Model (Transport, Network, Data Link and Physical layers).

This Recommendation | Technical Report describes:

- a) architectural concepts common to the lower layers based on those defined in CCITT Rec. X.800 | ISO 7498-2;
- b) the basis for interactions relating to security between protocols in the lower layers;
- c) the basis for any interactions relating to security between the lower layers and upper layers of OSI;
- d) the placement of security protocols in relation to other lower layer security protocols and the relative role of such placements.

There should be no conflict between the security protocols for the lower layers and the model described in this Recommendation | Technical Report.

CCITT Rec. X.500 | ISO/IEC 9594-1 identifies the security services relevant to each of the lower layers of the OSI Reference Model.

2 References

The following Recommendations and International Standards contain provisions which, through reference in this text, constitute provisions of this Recommendation | Technical Report. At time of publication, the editions indicated were valid. All Recommendations and Standards are subject to revision, and parties to agreements based on this Recommendation | Technical Report are encouraged to investigate the possibility of applying the most recent edition of the Recommendations and 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.200 (1994) | ISO/IEC 7498-1:1994, *Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model*.
- ITU-T Recommendation X.233 (1993) | ISO/IEC 8473-1:1994, *Information technology – Protocol for providing the OSI connectionless-mode Network service: Protocol specification*.
- ITU-T Recommendation X.234 (1994) | ISO/IEC 8602:1995, *Information technology – Protocol for providing the OSI connectionless-mode Transport service*.
- ITU-T Recommendation X.273 (1994) | ISO/IEC 11577:1995, *Information technology – Open Systems Interconnection – Network layer security protocol*.
- ITU-T Recommendation X.274 (1994) | ISO/IEC 10736:1995, *Information technology – Telecommunications and information exchange between systems – Transport layer security protocol*.
- ITU-T Recommendation X.803 (1994) | ISO/IEC 10745:1995, *Information technology – Open Systems Interconnection – Upper layers security model*.

- ITU-T Recommendation X.810¹⁾ | ISO/IEC 10181-1...¹⁾, *Information technology – Open Systems Interconnection – Security frameworks in open systems: Security frameworks overview.*
- ITU-T Recommendation X.812¹⁾ | ISO/IEC 10181-3...¹⁾, *Information technology – Open Systems Interconnection – Security frameworks in open systems: Access control framework.*

2.2 Paired Recommendations | International Standards equivalent in technical content

- 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/IEC 8825:1990, *Information technology – Open Systems Interconnection – Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1).*

2.3 Additional references

- ISO/IEC 8208:1995, *Information technology – Data communications – X.25 Packet Layer Protocol For Data Terminal Equipment.*
- ITU-T Recommendation X.25 (1993), *Interface between Data Terminal Equipment (DTE) and Data Circuit-Terminating Equipment (DCE) for terminals operating in packet mode and connected to public data networks by dedicated circuits.*
- ISO 8648:1988, *Information processing systems – Open Systems Interconnection – Internal organization of the Network Layer.*
- ISO 9542:1988²⁾, *Information processing systems – Telecommunications and information exchange between systems – End system to intermediate system routing exchange protocol for use in conjunction with the Protocol for providing the connectionless-mode network service (ISO 8473).*
- ISO/IEC 10589:1992, *Information technology – Telecommunications and information exchange between systems – Intermediate system to intermediate system intra-domain-routing routine information exchange protocol for use in conjunction with the protocol for providing the connectionless-mode Network service (ISO 8473).*
- ISO/IEC 10747:1994, *Information technology – Telecommunications and information exchange between systems – Protocol for exchange of inter-domain routing information among intermediate systems to support forwarding of ISO 8473 PDUs.*

3 Definitions

3.1 OSI Reference Model definitions

This Recommendation | Technical Report makes use of the following terms as defined in ITU-T Rec. X.200 | ISO/IEC 7498-1:

- Quality of Service

¹⁾ Presently at the stage of draft.

²⁾ Currently under revision.