

IEEE Standards for Local and Metropolitan Area Networks:

Supplement to Standard for Interoperable LAN/MAN Security (SILS):

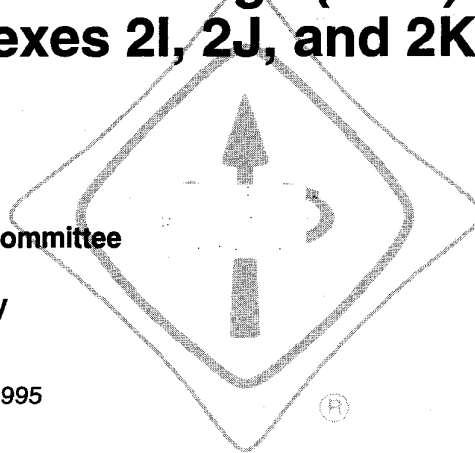
Secure Data Exchange (SDE)—Security Label (Annexes 2I, 2J, and 2K)

Sponsor

**LAN MAN Standards Committee
of the
IEEE Computer Society**

Approved September 21, 1995

IEEE Standards Board



Abstract: A security label option that can be used to implement rule-based access controls for the protection of IEEE 802 local area networks (LANs) and metropolitan area networks (MANs) is defined. Information carried by security labels can be used to control access, specify protective measures, and identify handling restrictions required by a communications security policy. This standard specifies the syntax for the label and basic processing rules. Other information, such as label semantics and additional processing requirements unique to a security policy, can be specified via registration.

Keywords: access control, local area network security, metropolitan area network security, secure data exchange, security labels

The Institute of Electrical and Electronics Engineers, Inc.
345 East 47th Street, New York, NY 10017-2394, USA

Copyright © 1996 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 1996. Printed in the United States of America.

ISBN 1-55937-562-0

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.

IEEE Standards documents are developed within the Technical Committees of the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Board. Members of the committees serve voluntarily and without compensation. They are not necessarily members of the Institute. The standards developed within IEEE represent a consensus of the broad expertise on the subject within the Institute as well as those activities outside of IEEE that have expressed an interest in participating in the development of the standard.

Use of an IEEE Standard is wholly voluntary. The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation. When a document is more than five years old and has not been reaffirmed, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of all concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason IEEE and the members of its technical committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration.

Comments on standards and requests for interpretations should be addressed to:

Secretary, IEEE Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

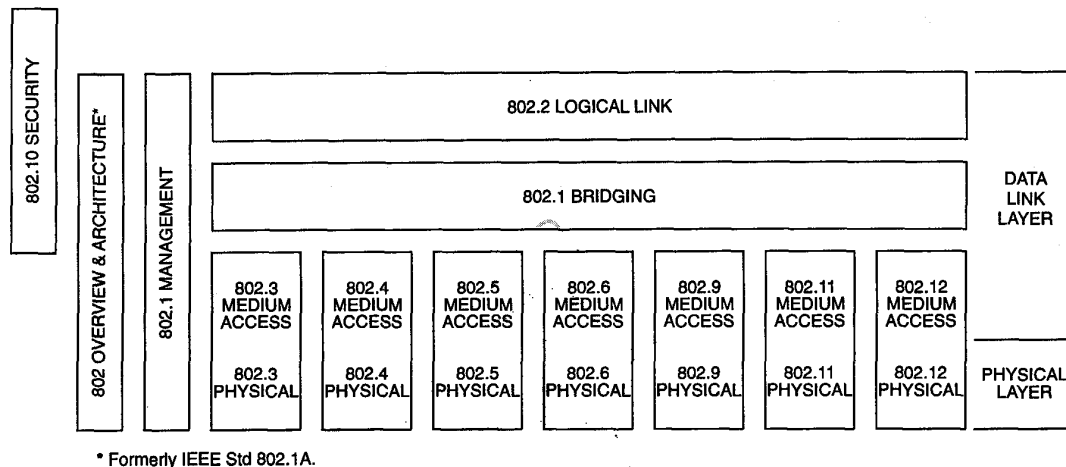
Note: Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE shall not be responsible for identifying all patents for which a license may be required by an IEEE standard or for conducting inquiries into the legal validity or scope of those patents that are brought to its attention.

Authorization to photocopy portions of any individual standard for internal or personal use is granted by the Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; (508) 750-8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction

[This introduction is not part of IEEE Std 802.10g-1995, IEEE Standards for Local and Metropolitan Area Networks: Supplement to Standard for Interoperable LAN/MAN Security (SILS): Secure Data Exchange (SDE)—Security Label.]

This standard is part of a family of standards for local and metropolitan area networks. The relationship of the members of the family to each other is shown below. (The numbers in the figure refer to IEEE standard numbers.)



This family of standards deals with the Physical and Data Link Layers as defined by the International Organization for Standardization (ISO) Open Systems Interconnection Basic Reference Model (ISO 7498: 1984). The access standards define several types of medium access technologies and associated physical media, each appropriate for particular applications or system objectives. Other types are under investigation. The IEEE 802.9 ISLAN Interface Standard specifies both isochronous and packet mode services, and provides access to ISDN and other backbone networks for service provisioning.

The standards defining these technologies are as follows:

- IEEE Std 802¹: Overview and Architecture. This standard provides an overview to the family of IEEE 802 Standards. This document forms part of the 802.1 scope of work.
- ISO/IEC 15802-2 [IEEE Std 802.1B and 802.1k]: LAN/MAN Management. Defines an Open Systems Interconnection (OSI) management-compatible architecture, and services and protocol elements for use in a LAN/MAN environment for performing remote management.
- ISO/IEC 10038 [ANSI/IEEE Std 802.1D]: MAC Bridging. Specifies an architecture and protocol for the interconnection of IEEE 802 LANs below the MAC service boundary.

¹The 802 Architecture and Overview Specification, originally known as IEEE Std 802.1A, has been renumbered as IEEE Std 802. This has been done to accommodate recognition of the base standard in a family of standards. References to IEEE Std 802.1A should be considered as references to IEEE Std 802.

- ISO/IEC 15802-4 [ANSI/IEEE Std 802.1E]: System Load Protocol. Specifies a set of services and protocol for those aspects of management concerned with the loading of systems on IEEE 802 LANs.
- ISO/IEC 8802-2 [ANSI/IEEE Std 802.2]: Logical Link Control
- ISO/IEC 8802-3 [ANSI/IEEE Std 802.3]: CSMA/CD Access Method and Physical Layer Specifications
- ISO/IEC 8802-4 [ANSI/IEEE Std 802.4]: Token Bus Access Method and Physical Layer Specifications
- ISO/IEC 8802-5 [ANSI/IEEE Std 802.5]: Token Ring Access Method and Physical Layer Specifications
- ISO/IEC 8802-6 [ANSI/IEEE Std 802.6]: Distributed Queue Dual Bus Access Method and Physical Layer Specifications
- IEEE Std 802.9: Integrated Services (IS) LAN Interface at the Medium Access Control (MAC) and Physical (PHY) Layers
- IEEE Std 802.10: Interoperable LAN/MAN Security
- IEEE Std 802.12: Demand Priority Access Method, Physical Layer and Repeater Specification

In addition to the family of standards, the following is a recommended practice for a common technology:

- IEEE Std 802.7: IEEE Recommended Practice for Broadband Local Area Networks

The following additional working groups have authorized standards projects under development:

- IEEE 802.11: Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications
- IEEE 802.14: Standard Protocol for Cable-TV Based Broadband Communication Network

Conformance test methodology

An additional standards series, identified by the number 1802, has been established to identify the conformance test methodology documents for the 802 family of standards. Thus the conformance test documents for 802.3 are numbered 1802.3, the conformance test documents for 802.5 will be 1802.5, and so on. Similarly, ISO will use 18802 to number conformance test standards for 8802 standards.

IEEE Std 802.10g-1995

This supplement to IEEE Std 802.10-1992 defines a security label option that can be used to implement rule-based access controls for the protection of IEEE 802 local area networks (LANs) and metropolitan area networks (MANs). The addition of this supplement has necessitated some technical changes to the standard, such as adding label fields to several figures, changing both transmission and reception processing steps to account for the labels, converting annex 2E (Fragmentation) to normative, and changing subclause 2.8 (SDE Sublayer Management) to accommodate new managed objects related to the new security label specification.

Security labels provide an indication of the sensitivity of the encapsulated data to the SDE protocol processing entity. The information provided by a label enables the SDE protocol entity to make access control decisions based on a hierarchy of classification levels and sets of information categories. This optional field may increase the size of the protocol header and may increase the number of packets that exceed the maximum allowable PDU size for a particular implementation, thereby increasing the probability of Data Link Layer fragmentation. This possibility has given greater importance to having a well defined, uniform method for handling Data Link Layer fragmentation.

Participants

At the time this standard was completed, the IEEE 802.10 Working Group had the following membership:

Kenneth G. Alonge, Chair	Noel A. Nazario, Technical Editor
Russell D. Housley, Vice Chair	Joanne Evans, Recording Secretary (1995)
James Coyle, Recording Secretary (1993-1995)	Wen-Pai Lu, Executive Secretary

Asher Altman
Kym D. Blair
Dane Elliot
Paul Lambert
Joseph A. Maley
Richard McAllister
Michael Michnikov

Barbara Patrick
Brian J. Phillips
Karen T. Randall
Amy Reiss
Robert Rosenthal
Anthony Sacco

Emile W. Soueid
Dale L. Walters
David M. Wheeler
Michael White
Peter Yee
Roberto Zamparo
James E. Zmuda

The following persons were on the balloting committee:

William B. Adams
Kenneth G. Alonge
James P. Anderson
Allen Arndt
Kit Athul
William E. Ayen
David Bagby
Thomas W. Bailey
Dixie B. Baker
Anthony L. Barnes
Kendall F. Barney
Mordechai Ben-Menachem
Greg Bergren
Justin M. Biddle
Brian Billard
Kym D. Blair
Kathleen L. Briggs
Michael J. Caldwell
J. Campbell
Paul W. Campbell
Peter K. Campbell
Frederick N. Chase
Gary G. Christoph
Alan J. Chwick
Karen J. Cooper
John Cronican
Robert S. Crowder
Michael Crumrine
Ibibia K. Dabipi
Connie W. Delaney

Huijie Deng
Robert Donnan
Edward A. Dunlop
Sourav K. Dutta
Gregory Elkmann
John E. Emrich
Philip H. Enslow
John W. Fendrich
Michael Fischer
Robert J. Gagliano
Carlos Gallegos
Rob Goode
Jon Graff
Daniel Guinier
Karunakar Gulukota
J. Thomas Haigh
Sandor V. Halasz
William S. Harbison
J. Scott Haugdahl
Clark M. Hay
Russell D. Housley
Nai-Kuan Huang
Cynthia E. Irvine
Shang-Sheng Jeng
Henry D. Keen
Peter M. Kelly
Gary C. Kessler
Lathia Kiritkumar
Peter Kraaibeek
Stephen B. Kruger

Kenneth C. Kung
Lanse M. Leach
Pil Joong Lee
Randolph S. Little
Joseph C. J. Loo
Robert D. Love
Jonathan Low
Wen-Pai Lu
Peter Martini
John McDermott
Chris McDonald
Robert J. Melford
Bennett Meyer
Ann Miller
Dale W. Miller
David S. Millman
Stig Frode Mjolsnes
W. Melody Moh
Refik Molva
Warren Monroe
Kinji Mori
David J. Morris
James R. Moulton
Wayne D. Moyers
Kevin V. Murphy
Michael John Nash
Bongnam Noh
Richard O'Brien
Robert O'Hara
D. O'Mahony

Lalit Mohan Patnaik
 Lucy W. Person
 Andreas Pfitzmann
 Brian J. Phillips
 Thomas L. Phinney
 Art Pina
 Rafat Pirzada
 Kirk Preiss
 Vikram Punj
 Yang Qianli
 Karen T. Randall
 Eugene J. Reilly
 John P. Riganati
 Edouard Y. Rocher
 Kris Rogers
 James W. Romlein
 Daniel Rosich
 Floyd E. Ross

R. Waldo Roth
 Rainer A. Rueppel
 Frederick E. Sauer
 Sanjay K. Saxena
 Roger R. Schell
 Gregory D. Schumacher
 Moe Shahdad
 Leo Sintonen
 Stephen E. Smaha
 Gary W. Smith
 William R. Smith
 David Snow
 Harry P. Solomon
 Joseph Stevenson
 Stuart G. Stubblebine
 Michael L. Sutherland
 E. D. Syhas
 Efsthiois D. Sykas
 Daniel Sze

Geoffrey O. Thompson
 Harold Tremblay
 Robert C. Tripi
 Mark-Rene Uchida
 J. Vandewalle
 Raymond VanHoutte
 Rammchan Varadarajan
 James T. Vorhies
 Barry M. Vornbrock
 Frank J. Weisser
 Clark Weissman
 Raymond Wenig
 D. J. Whitley
 Harold M. Wilensky
 James Williams
 Jerry A. Wyatt
 Peter Yee
 Oren Yuen

When the IEEE Standards Board approved this standard on September 21, 1995, it had the following membership:

E. G. "Al" Kiener, *Chair*

Donald C. Loughry, *Vice Chair*

Andrew G. Salem, *Secretary*

Gilles A. Baril
 Clyde R. Camp
 Joseph A. Cannatelli
 Stephen L. Diamond
 Harold E. Epstein
 Donald C. Fleckenstein
 Jay Forster*
 Donald N. Heirman
 Richard J. Holleman

Jim Isaak
 Ben C. Johnson
 Sonny Kasturi
 Lorraine C. Kevra
 Ivor N. Knight
 Joseph L. Koepfinger*
 D. N. "Jim" Logothetis
 L. Bruce McClung

Marco W. Migliaro
 Mary Lou Padgett
 John W. Pope
 Arthur K. Reilly
 Gary S. Robinson
 Ingo Rüschi
 Chee Kiow Tan
 Leonard L. Tripp
 Howard L. Wolfman

*Member Emeritus

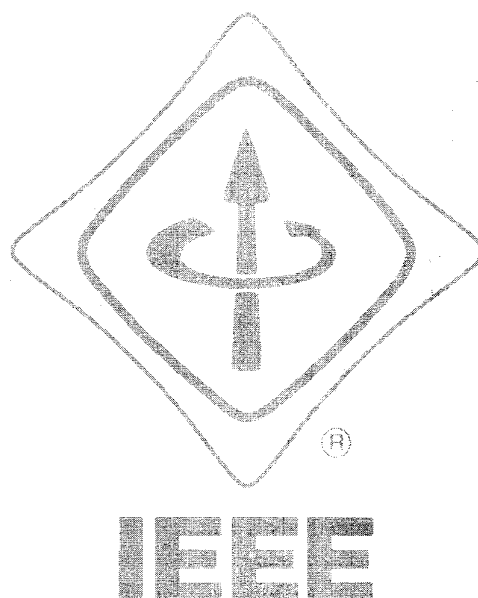
Also included are the following nonvoting IEEE Standards Board liaisons:

Satish K. Aggarwal
 Richard B. Engelman
 Robert E. Hebner
 Chester C. Taylor

Valerie E. Zelenty
IEEE Standards Project Editor

Contents

CLAUSE	PAGE
Revisions to IEEE Std 802.10-1992	1
Revisions to IEEE Std 802.10f-1993	9
ANNEX	
Annex 2I (normative) Secure data exchange security label.....	13
2I.1 Introduction.....	13
2I.2 Overview	13
2I.3 SDE security label option	14
2I.4 Security label length	14
2I.5 Security tags.....	15
2I.6 Security Tag Type 1.....	15
2I.7 Security Tag Type 2.....	16
2I.8 Security Tag Type 5.....	17
2I.9 Security Tag Type 6.....	17
2I.10 Security Tag Type 7.....	18
2I.11 Additional station objects	18
2I.12 Additional association objects	18
2I.13 Additional Protected Header field	19
2I.14 Detailed functional specification	20
Annex 2J (informative) Security label set registration service	21
Annex 2K (informative) Basic processing rules for security labels.....	22
2K.1 Introduction.....	22
2K.2 Trustworthiness of transmitted labels	22
2K.3 Originator requirements	22
2K.4 Receiver requirements	23
2K.5 Error reports	23
2K.6 Policy-based processing rules	23
2K.7 Bibliography	24



IEEE Standards for Local and Metropolitan Area Networks:

Supplement to Standard for Interoperable LAN/MAN Security (SILS):

Secure Data Exchange (SDE)— Security Label (Annexes 2I, 2J, and 2K)

Revisions to IEEE Std 802.10-1992 and IEEE Std 802.10f-1993

This supplement to IEEE Std 802.10-1992 defines a security label option that can be used to implement rule-based access controls for the protection of IEEE 802 local area networks (LANs) and metropolitan area networks (MANs). The addition of this supplement has necessitated several changes to IEEE Std 802.10-1992 and to IEEE Std 802.10f-1993 to accommodate the new security label specification. The security label is optional for SDE.

The contents of this document will be incorporated into IEEE Std 802.10 in a future edition. The clauses of this document are ordered to parallel the order of clauses in the base standard. This supplement is intended to be used in conjunction with IEEE Std 802.10-1992, IEEE Std 802.10e-1993, and IEEE Std 802.10f-1993. Editing instructions necessary to incorporate this supplement into IEEE Std 802.10 are provided in *bold italics*.

Revisions to IEEE Std 802.10-1992

1.2.1 Acronyms

Add the following text to subclause 1.2.1:

CSOR	Computer Security Objects Register
SSL	Standard Security Label

1.2.2 Definitions

Add the following text to subclause 1.2.2:

1.2.2.1 computer security object: An information object used to maintain a condition of security in computerized environments. Examples include: representations of computer or communications systems resources, security label semantics, modes of operation for cryptographic algorithms, and one-way hashing functions (NISTIR 5308: 1993).¹

1.2.2.2 entity: An active element in an open system (ISO/IEC 7498-1: 1994).

1.2.2.3 hierarchical level: A member of a linearly ordered set (i.e., hierarchy) of levels, e.g., a number in the range from 0 to 255.

1.2.2.4 information object: A well-defined piece of information, definition, or specification that requires a name to identify its use in an instance of communication (ISO/IEC 8824).

1.2.2.5 Named Tag Set: A field containing a Tag Set Name and its associated set of security tags (FIPS PUB 188: 1994).

1.2.2.6 permissive [security] attribute: A security attribute that identifies an active entity or a resource as member of a group. An entity is granted access to all resources in the groups it is a member of. Permissive attributes could be used alone or in combination with restrictive attributes. Commonly, when used in combination with restrictive attributes, they are secondary in the determination of access privilege.

1.2.2.7 policy: See **security policy**.

1.2.2.8 protocol data unit: A unit of data specified in a protocol and consisting of protocol information and, possibly, user data (ISO/IEC 7498-1: 1994).

1.2.2.9 protocol entity: An entity that follows a set of rules and formats (semantic and syntactic) that determines the communication behavior of other entities (ISO/IEC 7498: 1984).

1.2.2.10 register: A set of records (paper, electronic, or a combination) maintained by a Registration Authority containing assigned names and the associated information (NISTIR 5308: 1993).

1.2.2.11 restrictive [security] attribute: A security attribute that indicates the minimum level of privilege required by an active entity (i.e., subject) in order to gain access to a resource (i.e., object). Commonly a set of restrictive security attributes are associated with each resource. An active entity may only gain access to a resource if its set of privileges is higher than, or a superset of (i.e., dominates), the attribute set for the resource.

1.2.2.12 security attribute: A security-related quality of an object. Security attributes may be represented as hierarchical levels, bits in a bit map, or numbers. Compartments, caveats, and release markings are examples of security attributes.

1.2.2.13 security label: A marking bound to a resource (which may be a data unit) that names or designates the security attributes of that resource (ISO 7498-2: 1989).

1.2.2.14 security level: A hierarchical level whose purpose is to indicate degree of sensitivity to a designated security threat. It indicates a specific level of protection as specified by the security policy being enforced.

1.2.2.15 security policy: A set of criteria for the provision of security services (ISO/IEC 7498-2: 1989).

1.2.2.16 security tag: An information unit containing a representation of certain security-related information (e.g., a restrictive attribute bit map).

¹Information on references can be found in 1.3.