

IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS)

Currently Contains **Secure Data Exchange (SDE) (Clause 2)**

Sponsor

**Technical Committee on Security and Privacy and
Technical Committee on Computer Communications
of the IEEE Computer Society**

Approved September 17, 1992

IEEE Standards Board

Approved March 22, 1993

American National Standards Institute

Abstract: A security protocol that can be used to protect IEEE 802 Local Area Networks (LANs) and Metropolitan Area Networks (MANs) is described. This Open Systems Interconnection (OSI) Layer 2 security protocol can be used to provide the security services of confidentiality and connectionless integrity. In conjunction with key management or system management, the security services of data origin authentication and access control may also be provided.

Keywords: decipherment; encipherment; local area networks, security; metropolitan area networks, secure data exchange; security; security association

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

Copyright © 1993 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 1993. Printed in the United States of America

ISBN 1-55937-254-0

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:

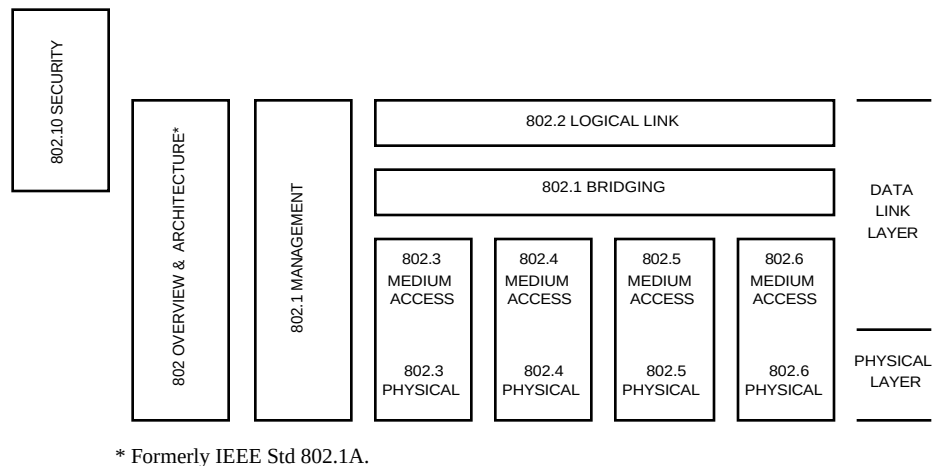
Secretary, IEEE Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

IEEE standards documents may involve the use of patented technology. Their approval by the Institute of Electrical and Electronics Engineers does not mean that using such technology for the purpose of conforming to such standards is authorized by the patent owner. It is the obligation of the user of such technology to obtain all necessary permissions.

Introduction

[This introduction is not a part of IEEE Std 802.10-1992, IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS) (ANSI).]

This standard is part of a family of standards for local and metropolitan area networks. The relationship between the standard and other members of the family 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 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 standards defining these technologies are as follows:

- IEEE Std 802*: 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.
- IEEE Std 802.1D: MAC Bridging. Specifies an architecture and protocol for the interconnection of IEEE 802 LANs below the MAC service boundary.
- 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 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

*The 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 8802-5 [ANSI/IEEE Std 802.5]: Token Ring Access Method and Physical Layer Specifications
- IEEE Std 802.6: Metropolitan Area Network Access Method and Physical Layer Specifications
- IEEE Std 802.10: Interoperable LAN/MAN Security (SILS)—Secure Data Exchange (SDE) [*Currently contains* Secure Data Exchange (Clause 2)]

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

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. This makes the correspondence between the various 802 standards and their applicable conformance test requirements readily apparent. 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.

802.10-1992

The IEEE 802.10 LAN Security Working Group was formed in May of 1988 to address the security of Local Area Networks (LANs) and Metropolitan Area Networks (MANs). It is co-sponsored by IEEE 802 and by the IEEE Technical Committee on Security and Privacy. The committee has representation from vendors, government, and users. IEEE Std 802.10 is intended to provide a standard to address security for LANs and MANs. The standard is an interoperability standard that is compatible with the existing IEEE 802 and OSI architectures. This volume, which includes Secure Data Exchange (SDE), is the first clause to be completed. Additional clauses and subclauses will be published as supplements and folded into the base document (IEEE Std 802.10) at the appropriate time.

Data networks, especially LANs and MANs, have become widespread. LANs and MANs are used by both industry and government for transferring vast amounts of information in the course of daily operations. Because of their ever-increasing use in the private and public sectors, the capabilities of these networks are being expanded to encompass more and more performance requirements. As a result, there is the growing need to standardize network protocols wherever feasible, to ensure that data networks will interoperate effectively.

As standardization practices evolve, several key areas will become critically important. One of these areas is network security. Many LANs and MANs require the capability to exchange data in a secure manner. This is especially important in cases where disclosure of operational information to unauthorized parties would severely undermine an organization's effectiveness. It is often as critical to protect the integrity of the data as it is to prevent disclosure of operating information.

Financial and government institutions have traditionally been most aware of the importance of security. However, recent widely publicized cases of computer fraud and related crimes have made security a goal for many other industries as well. As the need for security on LANs and MANs gains recognition, the need for a standardized approach to providing such a capability also becomes a priority. Much security standardization has already been started. Where applicable, this standard attempts to incorporate this work.

Participants

At the time this standard was completed, the 802.10 LAN/MAN Security Working Group had the following membership:

Kenneth G. Alonge, *Chair (1991 to present)*

Kimberly Kirkpatrick, *Chair (1988–1991)*

Russell Housley, *Vice Chair*

L. Kirk Barker, *Technical Editor* **Peter Yee**, *Recording Secretary*

Alan Arndt	Paul Lambert	James Pyles
Kurt Augustine	Warren Loper	James Randall
Bill Birnbaum	Wen-Pai Lu	Eugene Reilly
Ben Bratcher	Marc Mandel	Brian Schanning
Ronald Gibson	Ken McCoy	James Sutherland
Jon Graff	Esther Murphy	Kenta Takumi
Tom Hunwick	Richard Parker	Lloyd Taylor
Robert Kolacki	Brian Phillips	Joseph Williamson

The following individuals also contributed review and comments:

Morrie Gasser	John Kimmins	C.E. Reaver
B.J. Herbison	Scott Lawrence	Jim Sanders
Lawrence Kilgallen	Larry Lunsford	Mitch Tannenbaum

The following persons were on the balloting committee that approved this document for submission to the IEEE Standards Board:

W. B. Adams	H. K. Gorowara	A. J. Luque
I. F. Akyildiz	J. Graff	G. Q. Maguire
P. Angarano	M. Greer	E. G. Marmol
Y. M. Baeg	R. M. Gross	P. Martini
M. R. Balomiri	A. Grund	C. McDonald
T. Batten	D. Hardie	W. C. McDonald
J. O. Bondi	C. M. Hay	G. McWilliams
C. E. Bouldin	L. A. Hollaar	R. J. Melford
M. A. Branstad	G. L. Hollander	A. Miller
A. L. Bridges	R. D. Housley	R. H. Miller
D. W. Browne	G. J. Huey	D. S. Millman
R. Caasi	W. J. Huntman	R. R. Moeller
A. L. Carrato	T. R. Hunwick	T. Mookken
A. Castaldo	B. Igglan	D. J. Morris
K. J. Cooper	T. J. Jasinski	C. E. Neblock
S. J. Covington	R. Juvonen	R. Nelson
R. S. Crowder	K. C. Kelley	D. M. Nessett
E. A. Czarcinski	G. C. Kessler	C. Neuman
A. M. De Alvaré	F. Khatibi	D. O'Mahony
R. Diaz	K. Kirkpatrick	E. Okamoto
W. C. Dube	T. Korelsky	S. A. Orrell
A. M. Dunn	P. Kornerup	A. Pfizmann
S. K. Dutta	M. D. Krenzin	T. E. Phillips
T. Dzik	K. Kung	T. L. Phinney
J. Ellis	C. A. LaBarge	R. L. Phipps
P. H. Enslow, Jr.	L. M. Lam	A. J. Pina
S. A. Faviell	L. M. Leach	U. W. Pooch
J. W. Fendrich	M. E. Lee	V. Prabhu
C. A. Finseth	E. V. Leighninger	Y. Qianli
H. A. Freeman	W. A. Levy	R. Ramaswamy
G. Fullerton	E. Liebman	E. J. Reilly
R. Gagliano	P. Lin	T. E. Revello
M. Gasser	J. Litchfield	A. B. Richstein
C. G. Girling	W. E. Loper	C. J. Riddick
P. Gonia	W. Lu	R. Rosenthal

V. Rozentouler
J. W. Rub
R. A. Rueppel
C. Ruland
D. J. Rypka
E. R. Schallennmuller
B. P. Schanning
R. R. Schell
N. Schneidewind
J. R. Schwab
B. Sklar
D. Snow
H. P. Solomon

J. Stevenson
B. J. Stoppe
E. Sullivan
E. D. Sykas
H. Tang
B. J. Tarbox
L. W. Taylor
P. Thaler
J. C. Thomas
D. M. Topkis
B. Tretick
R. C. Tripi
G. Tsudik
D. B. Turner

R. Van Houtte
J. Vandewalle
J. T. Vorhies
B. Vornbrock
S. T. Walker
R. K. Walker
R. Wenig
W. J. Wenker
J. A. West
G. B. Wright
J. Yang
P. Yee
O. Yuen

When the IEEE Standards Board approved this standard on September 17, 1992, it had the following membership:

Marco W. Migliaro, *Chair*

Donald C. Loughry, *Vice Chair*

Andrew G. Salem, *Secretary*

Dennis Bodson
Paul L. Borrill
Clyde Camp
Donald C. Fleckenstein
Jay Forster*
David F. Franklin
Ramiro Garcia
Thomas L. Hannan

Donald N. Heirman
Ben C. Johnson
Walter J. Karplus
Ivor N. Knight
Joseph Koepfinger*
Irving Kolodny
D. N. "Jim" Logothetis
Lawrence V. McCall

T. Don Michael*
John L. Rankine
Wallace S. Read
Ronald H. Reimer
Gary S. Robinson
Martin V. Schneider
Terrance R. Whittemore
Donald W. Zipse

*Member Emeritus

Also included are the following IEEE Standards Board liaisons:

Satish K. Aggarwal
James Beall
Richard B. Engelman
David E. Soffrin
Stanley Warshaw

Kristin M. Dittmann
IEEE Standards Project Editor

IEEE Standards for Local and Metropolitan Area Networks: Interoperable LAN/MAN Security (SILS)

Currently Contains Secure Data Exchange (SDE) (Clause 2)

1. Overview and model

1.1 Scope and purpose

This standard was developed to provide security in IEEE 802 Local Area Networks (LANs) and Metropolitan Area Networks (MANs).

The model for providing security services is described in clause 1. A Secure Data Exchange (SDE) protocol for IEEE 802 LANs and MANs is defined in clause 2. Key management and system/security management in IEEE 802 LANs and MANs are described in clauses 3 and 4. While SDE is independent of any key management or system management implementation, the security services described in this standard depend on management information provided by management entities.

1.2 Acronyms and definitions

1.2.1 Acronyms

This subclause contains acronyms that are applicable to all clauses of the standard.

CMIP	Common Management Information Protocol
DA	Destination Address
DEA	Data Encryption Algorithm
DSAP	Destination Service Access Point
ICV	Integrity Check Value
IV	Initialization Vector
LAN	Local Area Network
LM	Layer Manager
LLC	Logical Link Control
LSAP	Link Service Access Point
MAC	Medium Access Control
MAN	Metropolitan Area Network
MDF	Management-Defined Field
MER	Minimum Essential Requirements
MIB	Management Information Base
MSDU	MAC Service Data Unit
OSI	Open Systems Interconnection
PDU	Protocol Data Unit

SA	Source Address
SAID	Security Association Identifier
SAP	Service Access Point
SDE	Secure Data Exchange
SDU	Service Data Unit
SILS	Standard for Interoperable LAN Security
SMAE	System Management Application Entity
SMIB	Security Management Information Base
SSAP	Source Service Access Point
TCB	Trusted Computing Base

1.2.2 Definitions

This subclause contains the definitions that are applicable to all clauses of this standard. Sources for the definitions are indicated. When no source is indicated, this standard is the source.

1.2.2.1 access control: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. (ISO 7498-2 : 1989¹)

1.2.2.2 attribute: A property of a managed object or a property of an association among OSI entities. An attribute has an associated value, which may have a simple or complex structure. (ISO/IEC 10040 : 1992)

1.2.2.3 authentication: *See: data origin authentication; peer entity authentication.* *Note:* In this standard, the term “authentication” is not used in connection with data integrity; the term “data integrity” is used instead.

1.2.2.4 bootstrap SAID. Four SAID values are reserved for the purpose of establishing initial communication with key management or system management when an SAID has not already been negotiated. These SAID values are called “bootstrap” SAIDs and have a preestablished security association.

1.2.2.5 ciphertext: Data produced through the use of encipherment, the semantic content of which is not available. *Note:* Ciphertext may itself be input to encipherment, producing superenciphered data.

1.2.2.6 cleartext: Intelligible data, the semantic content of which is available. (ISO 7498-2 : 1989)

1.2.2.7 compromise: A violation of the security of a system such that an unauthorized disclosure of sensitive information may have occurred. (NCSG-TG-005 Version-1 [B3]²)

1.2.2.8 confidentiality: The property of information that is not made available or disclosed to unauthorized individuals, entities, or processes. (ISO 7498-2 : 1989)

1.2.2.9 connection-oriented confidentiality: The protection of all (N)-service data units from unauthorized disclosure during communications from one (N+1)-entity to one or more (N+1)-entities for which a security association is established for the transfer of data and for the application of confidentiality service between the entities themselves and between each entity and the physical layer.

1.2.2.10 connection-oriented integrity: A service providing for the integrity of all (N)-service data on a security association and detecting any modification, insertion, deletion, or replay of any data within an entire SDU sequence.

¹Information on references can be found in 1.3.

²The numbers in brackets preceded by the letter B correspond to those of the bibliography in clause 5.

1.2.2.11 connectionless confidentiality: The protection of (N)-service data units from unauthorized disclosure during transmission from one (N+1)-entity to one or more (N+1)-entities, where each entity has an association with the physical layer, and no association is established for the transmission of data or for the application of the confidentiality service between the layer peer-entities themselves.

1.2.2.12 connectionless integrity: A service providing for the integrity of a single SDU. It may take the form of determining whether or not the received SDU has been modified.

1.2.2.13 cryptographic checkvalue: Information that is derived by performing a cryptographic transformation on the data unit. *See: cryptography.* (ISO 7498-2 : 1989)

1.2.2.14 cryptography: The discipline embodying principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification, and/or prevent its unauthorized use. (ISO 7498-2 : 1989)

1.2.2.15 data deciphering key: A key used for the decipherment of an (N)-layer SDU. (It is not used to decipher other keys.)

1.2.2.16 data enciphering key: A key used for the encipherment of an (N)-layer SDU. (It is not used to encipher other keys.)

1.2.2.17 data integrity: The condition or state in which data has not been altered or destroyed in an unauthorized manner. (ISO 7498-2 : 1989)

1.2.2.18 data origin authentication: The corroboration that the source of data received is as claimed. This service, when provided by the (N)-layer, provides the corroboration to an (N+1)-entity that the source of the data is the claimed peer (N+1)-entity. (ISO 7498-2 : 1989)

1.2.2.19 decipherment: The reversal of a corresponding reversible encipherment. ISO 7498-2 : 1989)

1.2.2.20 encipherment: The cryptographic transformation of data to produce ciphertext. *See: cryptography.* (ISO 7498-2 : 1989)

1.2.2.21 Initialization Vector (IV): A binary vector used at the beginning of a cryptographic operation to allow cryptographic chaining. (ANSI X9.17-1985)

1.2.2.22 Integrity Check Value (ICV): A value that is derived by performing an algorithmic transformation on the data unit for which data integrity services are provided. The ICV is sent with the protected data unit and is recalculated and compared by the receiver to detect data modification. *See: cryptographic check-value.*

1.2.2.23 key: A sequence of symbols that controls the operations of encipherment and decipherment. (ISO 7498-2 : 1989)

1.2.2.24 key management: The generation, storage, distribution, deletion, archiving, and application of keys in accordance with a security policy. (ISO 7498-2 : 1989)

1.2.2.25 Key Management Stack: The protocols residing above SDE that request services via an SDE SAP that is supported by the use of a bootstrap SAID with either of the two values reserved for key management.

1.2.2.26 layer management: Functions related to the management of the (N)-layer partly performed in the (N)-layer itself according to the (N)-protocol of the layer, and partly performed as a subset of systems management. (ISO 7498 : 1984)

1.2.2.27 Layer Manager (LM): A systems management service application for which a particular exchange of systems management information has taken a manager role of the (N)-layer. (ISO/IEC 10040 : 1992)

1.2.2.28 managed object: The OSI structure of management information (ISO/IEC 10165-2 : 1992) term used as an abstract representation of a resource. This managed object has a set of attributes. These attributes are equivalent to data objects.

1.2.2.29 manipulation detection: A mechanism used to detect whether a data unit has been modified (either accidentally or intentionally). (ISO 7498-2 : 1989)

1.2.2.30 masquerade: The pretense by an entity to be a different entity. (ISO 7498-2 : 1989)

1.2.2.31 Management Information Base (MIB): A conceptual database of information contained in the collection of all the managed object classes and their instances. (ISO/IEC 7498-4 : 1989)

1.2.2.32 misordering data: A form of unauthorized data modification in which the reception sequence of data units is altered from the original transmission sequence in an unauthorized manner. This can be attempted by a combination of techniques involving deleting, delaying, and reinserting data; or modifying sequence control information; or both.

1.2.2.33 object: A data object that has an identifier (name) and a value.

1.2.2.34 Open Systems Interconnection (OSI) (N)-service: A capability of the (N)-layer, and the layers beneath it, that is provided to the (N)-entities at the boundary between the (N)-layer and the (N+1)-layer. (ISO 7498 : 1984)

1.2.2.35 peer-entity authentication: The corroboration that a peer entity in an association is the one claimed. This service, when provided by the (N)-layer, provides corroboration to the (N+1)-entity that the peer entity is the claimed (N+1)-entity. (ISO 7498-2 : 1989) This is primarily intended for, although not limited to, connection-oriented service and may be either unilateral or mutual.

1.2.2.36 reflection: A form of data modification in which PDUs sent by an entity are returned in an unauthorized manner. This can be attempted by a combination of techniques involving deleting, delaying, and reinserting data; and/or modifying address or sequence control information.

1.2.2.37 secret key: The traditional cryptographic key known only to the communicating parties and used for both encipherment and decipherment.

1.2.2.38 security association: A cooperative relationship between entities formed by the sharing of cryptographic keying information and security management objects. This shared information need not be identical, but it must be compatible.

1.2.2.39 Security Association Identifier (SAID): A value placed in the clear header of the SDE PDU that is used to identify the security association.

1.2.2.40 Security Management Information Base (SMIB): An MIB that stores security-relevant objects.

1.2.2.41 security service: A service, provided by a layer of communicating open systems, that ensures adequate security of the systems or of data transfers. (ISO 7498-2 : 1989) Note that these security services need not be directly requested at the (N)- and (N+1)-layer boundary as is required for an OSI (N)-service.

1.2.2.42 systems management: Functions in the Application Layer related to the management of various OSI resources and their status across all layers of the OSI architecture. (ISO 7498 : 1984)

1.2.2.43 System Management Stack: The protocols residing above SDE that request services via an SDE SAP that is supported by the use of a bootstrap SAID with either of the two values reserved for system management.

1.2.2.44 threat: A potential violation of security. (ISO 7498-2 : 1989)

1.2.2.45 trusted functionality: That which is perceived to be correct with respect to some criteria, e.g., as established by a security policy. (ISO 7498-2 : 1989)

1.2.2.46 unauthorized disclosure: The process of making information available to unauthorized individuals, entities, or processes. (ISO 7498-2 : 1989)

1.2.2.47 unauthorized data modification: Alteration of data not consistent with the defined security policy.

1.2.2.48 unauthorized resource use: Use of a resource not consistent with the defined security policy. (ISO 7498-2 : 1989)

1.2.2.49 User Stack: The protocols residing above SDE that request services from any SDE SAP except those supported by the use of a bootstrap SAID.

1.3 References

This standard shall be used in conjunction with the following references:

ANSI X9.17-1985 (R1991), Financial Institution Key Management (Wholesale).³

IEEE Std 802-1990, IEEE Standards for Local Area Networks: Overview and Architecture (ANSI).⁴

ISO 7498 : 1984, Information processing systems—Open Systems Interconnection—Basic Reference Model.⁵

ISO 7498-2 : 1989, Information processing systems—Open Systems Interconnection—Basic Reference Model—Part 2: Security Architecture.

ISO 8802-2 : 1989 [ANSI/IEEE Std 802.2-1989], Information processing systems—Local area networks—Part 2: Logical Link Control.⁶

ISO/IEC 7498-4 : 1989, Information processing systems—Open Systems Interconnection—Basic Reference Model—Part 4: Management framework.⁷

ISO/IEC 10039 : 1991, Information technology—Open Systems Interconnection—Local area networks—Medium Access Control (MAC) service definition.

³ANSI publications are available from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA.

⁴IEEE publications are available from the Institute of Electrical and Electronics Engineers, Service Center, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA.

⁵ISO publications are available from ISO, Case Postale 56, 1 rue de Varembe, CH-1211, Genève 20, Switzerland/Suisse. ISO publications are also available in the United States from ANSI.

⁶ISO [ANSI/IEEE] publications are available from the ISO Central Secretariat, 1 rue de Varembe, Case Postale 56, CH-1211, Genève 20, Switzerland/Suisse. They are also available in the US from the IEEE Service Center.

⁷ISO/IEC publications are available from the ISO Central Secretariat.

ISO/IEC 10040 : 1992, Information technology—Open Systems Interconnection—Systems management overview.

ISO/IEC 10165-2 : 1992, Information technology—Open Systems Interconnection—Structure of management information—Management information—Part 2: Definition of management information.

1.4 Architecture

The relationship of the each of the security protocols to the Open Systems Interconnection (OSI) Basic Reference Model will be described in this subclause, which is under consideration.

2. Secure Data Exchange (SDE)

2.1 Overview

The SDE is an OSI Basic Reference Model (ISO 7498-1984) Layer 2 entity. This entity provides services that permit the secure exchange of data at Layer 2. As part of the Logical Link Control (LLC) sublayer, the SDE entity provides a connectionless service immediately above the Medium Access Control (MAC) sublayer in IEEE 802 LANs and MANs. It provides security across the MAC sublayer using cryptographic mechanisms and security services provided transparently at the boundary to the LLC entity. The relationship of the SDE entity to the IEEE 802 reference model is shown in figure 2-1.

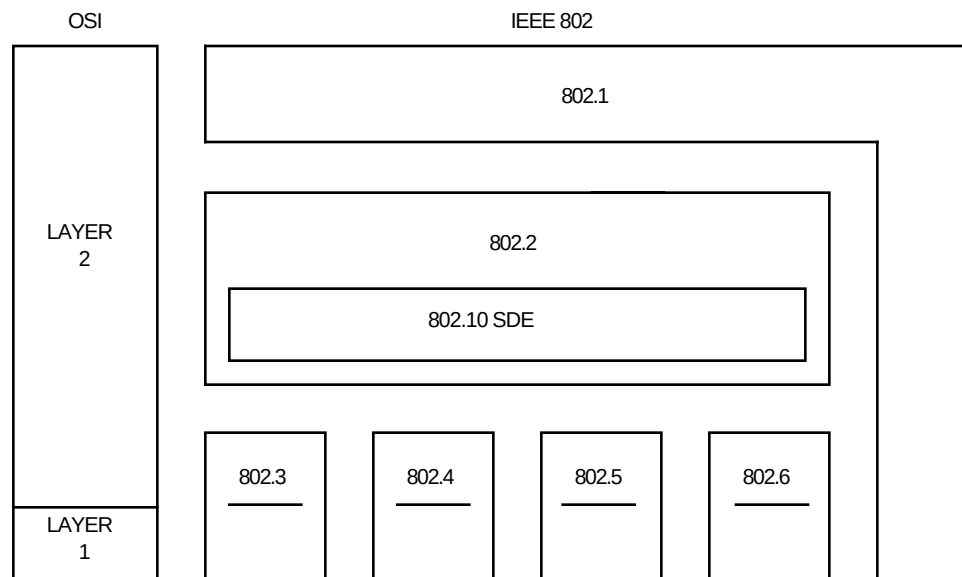


Figure 2-1—Relationship to IEEE 802 reference model

SDE is not applicable to MANs using IEEE 802.6 isochronous and connection-oriented protocols [IEEE Std 802.6-1990, IEEE Standards for Local and Metropolitan Area Networks: Distributed Queue Dual Bus (DQDB) Subnetwork of a Metropolitan Area Network (MAN) (ANSI)]. Nor is it applicable to integrated services using P802.9, Integrated Services (IS) Interface at the PHY Layers.

The SDE interface services specification to the MAC sublayer, to the boundary of the LLC entity, and to the SDE layer management functions is defined in this subclause. The security services provided and the threats these services protect against are described in 2.3. In 2.4, the service specifications are defined and the interface to the MAC sublayer and to the LLC entity boundary is described in detail.

The SDE entity provides security services and an interface at the boundary to the LLC entity. However, it does not specify any of the higher protocols that reside in the User Stack, including those of the LLC sublayer. The SDE interface is equivalent to the unprotected MAC interface and thus requires no change to the existing upper-layer protocols in the User Stack.⁸ SDE security services provided to a Key Management Stack or to a System Management Stack require the LLC protocol.

⁸ To use the management functionality of IEEE Std 802.1B-1992, IEEE Standards for Local and Metropolitan Area Networks: LAN/MAN Management, and ISO/IEC 9596, Common Management Information Protocol (CMIP), the SDE is modeled as part of LLC. If these management protocols are not used, it is possible to model SDE as a Data Link sublayer directly above the MAC sublayer.

An SDE-specific Protocol Data Unit (SDE PDU) is introduced in 2.6. The SDE PDU has optional elements and fields to satisfy a broad range of potential security applications. A reserved Link Service Access Point (LSAP) in the clear header portion of the SDE PDU distinguishes the SDE PDU from LLC PDUs. In 2.5, the SDE PDU elements and element fields are defined and the transformation of an SDE SDU into an SDE PDU is described.

A security association is an important concept in this standard. A security association is a cooperative relationship between communicating entities, formed by sharing security management information. This shared information coordinates the transmission and reception processing of the SDE PDU. In practice, there are many defined security associations, but only one applies to the processing of a specific SDE PDU. A Security Association Identifier (SAID) associates a defined security association with a specific SDE PDU. In 2.6, the contents of the security management information are defined and the use of the SAID in finding the applicable security association is described.

The Layer 2 security services provided by the SDE rely on information from non-Layer 2 key management or system management entities. Management entities communicate the information to the SDE entity through a Security Management Information Base (SMIB). The implementation of the SMIB is a local issue; however, the standard specifies the structure of the information as defined in the Structure of Management Information (ISO/IEC 10165-2 : 1992). The SMIB, the security management architecture, and the procedures for processing the SDE PDU based upon the security management information contained in the SMIB are described in 2.6.

2.2 Definitions

For the purpose of this standard, the following definitions apply:

2.2.1 SDE Layer Manager (LM). The SDE portion of the Layer 2 Manager.

2.2.2 transparent. A protocol is said to be transparent if all of the following conditions are met:

- a) Previously existing protocol implementations are able to recover when receiving packets formed by this new protocol.
- b) The implementations of this protocol are able to process packets formed by previously existing protocols without problems.
- c) The protocol does not affect the operations of the (N+1) and (N-1)-layer implementations.

2.3 SDE security services

This subclause contains a description of the security services provided by, or supported by, the SDE entity, and the threats these security services protect against.

The security services are as follows:

- a) *Data confidentiality.* The SDE entity provides data confidentiality by enciphering the SDE SDU. The SDE entity provides for the use of multiple confidentiality algorithms and depends on an external key management service to establish a data enciphering key and data deciphering key and for choosing an appropriate cryptographic algorithm.
- b) *Connectionless integrity.* The SDE entity provides connectionless integrity by calculating an Integrity Check Value (ICV) and placing it in the ICV field of the SDE PDU. The SDE entity depends on an external key management service to establish an integrity algorithm and integrity key.
- c) *Data origin authentication.* Data origin authentication is achieved by the use of key management. It is supported by the SDE entity placing a Station ID in the Protected Header portion of the SDE

PDU. The inclusion of the Station ID also prevents undetected reflection of the SDE PDU. Data origin authentication can only be provided in conjunction with the integrity service.

- d) *Access control.* Access control is provided by key management or system management. The SDE entity's use of security associations supports management's access control decisions. The SDE entity cannot transmit or deliver a PDU unless a security association exists. It is management's responsibility to set up the security associations and the SDE's responsibility to enforce the access control policy. Access control is dependent on both integrity and authentication services. Access control can only be provided in conjunction with integrity and authentication.

The threats that these services protect against are as follows:

- Unauthorized disclosure
- Masquerading
- Unauthorized data modification
- Unauthorized resource use

The rationale for addressing these threats is contained in annex 2A. The dependencies among the security services are shown in table 2-1.

Table 2-1—Security service dependencies*

Service	Dependency
Confidentiality	No dependencies
Integrity	No dependencies
Authentication	Depends on integrity
Access control	Depends on authentication and integrity

*The SDE entity supports only Identity-Based Access Control as described in ISO 7498-2 : 1989.

It is not necessary for all stations in the LAN or MAN to employ the SDE protocol. It is possible for entities that do not employ the protocol to communicate with those that do employ the protocol.

The SDE protocol is required to be transparent to existing implementations. Transparency, in the context of this standard, consists of meeting the following requirements:

- a) Existing IEEE 802 entities shall be able to recover if they receive an SDE protected packet.
- b) SDE entities shall be able to accept non-SDE protected packets without impairment.
- c) The addition of security should not modify either the (N+1)-layer or (N-1)-layer implementations.

Note that the addition of the SDE protocol may cause certain network management values, such as the fragmentation size, to change, but can still be considered a transparent implementation.

2.4 SDE service specifications

The services provided by SDE are defined in this subclause. SDE is modeled as part of the LLC entity and relies on the services provided by the MAC sublayer. There are only two primitives that are used at the SDE boundary: UNITDATA.request and UNITDATA.indication. These primitives are described in detail in ISO/IEC 10039 : 1991.

In subsequent subclauses of this document, the primitives on the upper boundary of the SDE are prefixed with “SDE”, and the primitives on the lower boundary are prefixed with “MA” (see figure 2-2). The services provided at the upper SDE boundary include those provided by the MAC sublayer with the addition of those services provided transparently by the SDE.

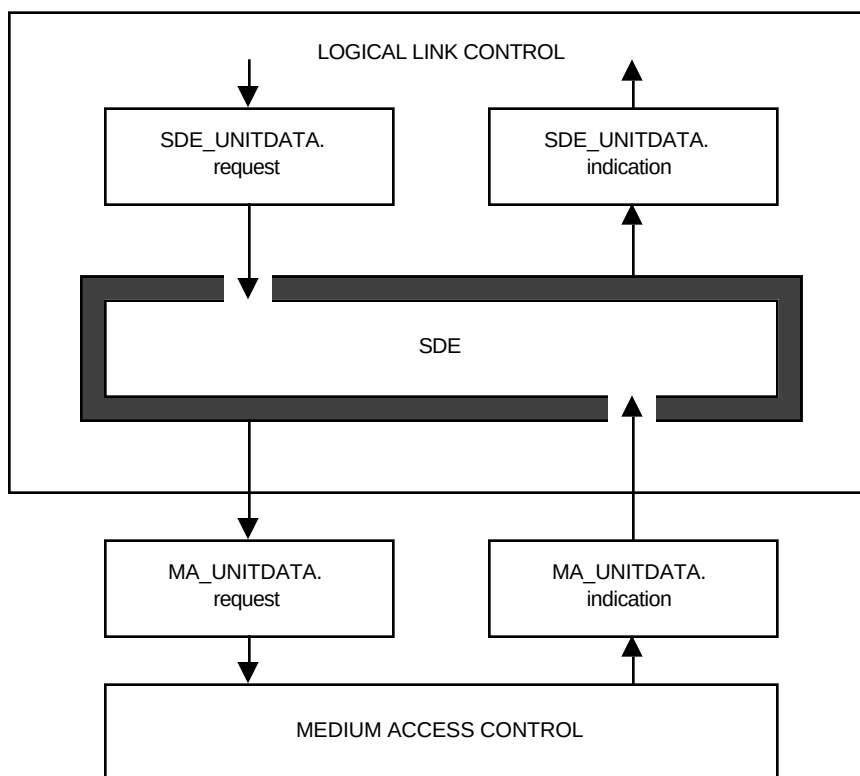


Figure 2-2—SDE primitives

The primitives used across the SDE service interface are a subset of the MAC primitives defined in ISO/IEC 10039 : 1991. Additional primitives specified by other MAC interfaces shall be passed unaltered through SDE. Likewise, the minimum set of parameters of these primitives is specified. Other MAC interfaces, such as those in ISO/IEC 8802-5 : 1992 [B2] are also allowed, and shall be passed through without modification. The MAC primitives that make up the SDE subset are as follows:

UNITDATA.request	Source Address (SA) Destination Address (DA) MAC Service Data Unit (MSDU)
UNITDATA.indication	SA DA MSDU

2.4.1 SDE_UNITDATA.request parameters

The parameters associated with the SDE_UNITDATA.request are defined in ISO/IEC 10039 : 1991.

2.4.2 SDE_UNITDATA.indication parameters

The parameters associated with the SDE_UNITDATA.indication are defined in ISO/IEC 10039 : 1991.

2.4.3 Services assumed

The service primitives assumed at the lower boundary of SDE are those defined in ISO/IEC 10039 : 1991.

The SDE entity assumes the existence of an SMIB that is accurately maintained by a method outside the scope of the SDE entity.

2.5 SDE PDU structure

The structure of the SDE PDU is described in this subclause. The SDE PDU format is described in 2.5.1. In 2.5.2, the relative positions of the various elements of the SDE PDU are defined. This subclause includes descriptions of the fields in terms of size and content. These fields are also defined as either optional or mandatory. The transformation of an SDE SDU to an SDE PDU is described in 2.5.3.

2.5.1 SDE PDU format

SDE uses a single PDU type. The PDU contains an integral number of octets. The PDU format, which may contain up to five elements, is shown in figure 2-3. These elements include the Clear Header, Protected Header, Data (SDE SDU), Pad, and the ICV. All of these elements are optional except Data. The contents of the Protected Header, Data, and Pad may be transformed prior to transmission by the integrity algorithm. The contents of the Protected Header, Data, Pad, and ICV shall always be transformed when the confidentiality algorithm is applied.

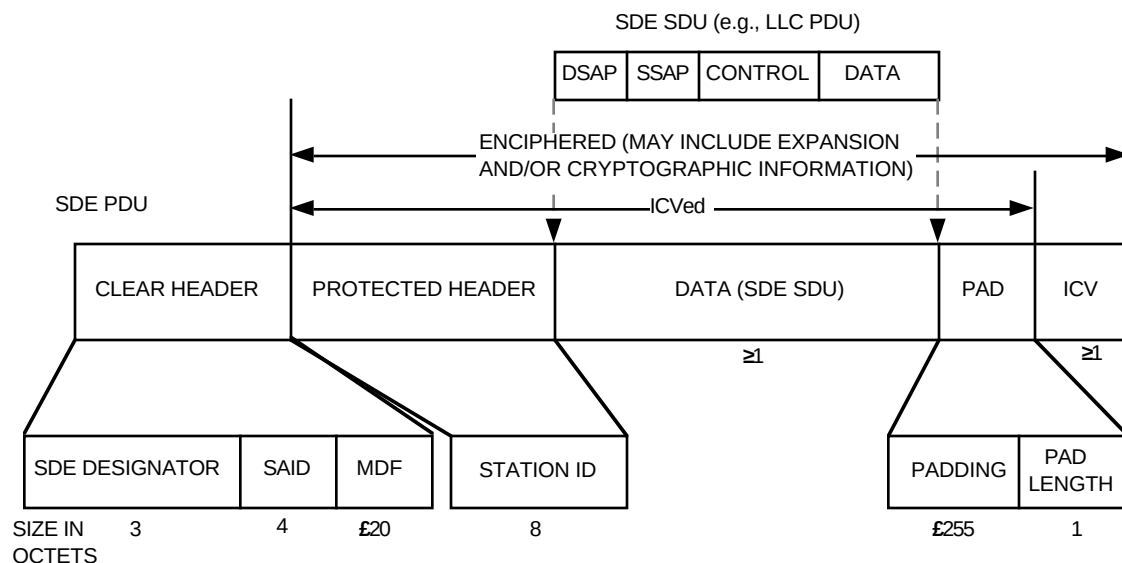


Figure 2-3—Structure of the SDE PDU

2.5.2 Elements of the SDE PDU

2.5.2.1 Clear Header

The Clear Header (see figure 2-4) identifies the SDE PDUs and aids in the processing of information contained in these PDUs. The content of the Clear Header is determined during security association setup and is constant for the life of that security association. The use of the Clear Header is optional. When the Clear Header is present, its length will be from seven to 27 octets, inclusive.

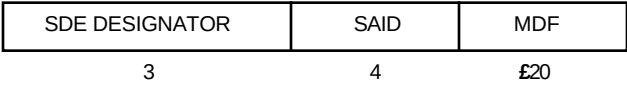


Figure 2-4—Clear Header

2.5.2.1.1 SDE Designator

The first three octets of the Clear Header constitute the SDE Designator, which ensures that a non-SDE entity that contains an LLC-entity will not process the SDE PDU. The SDE Designator contains the value of a reserved LSAP in each of the first two octets and the Unnumbered Information control field, as defined in ISO 8802-2 : 1989 (P-bit equal to zero), in the third octet.⁹ In this and subsequent subclauses, the octets in each field shown are ordered left to right and the leftmost bit is the first bit received from, or sent to, the MAC sublayer. The SDE Designator is mandatory when the Clear Header is present.

2.5.2.1.2 SAID

The SAID field identifies the security association. It contains the SAID associated with the destination SDE entity. If the destination is a group address, the SAID value is common for all the stations in the group and is negotiated by key management or system management. The SAID field is four octets in length and is mandatory when the Clear Header is present.

The format of the SAID is shown in figure 2-5. The leftmost bit of the SAID is called the G-bit. This is the first bit received from the MAC sublayer. It is used to indicate whether the security association identified by the SAID is common to a group of SDE entities (value set to 1) or an individual SDE entity (value set to 0).

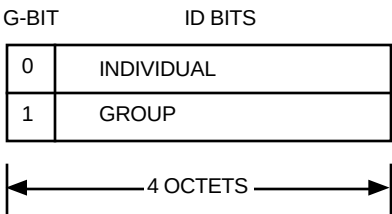


Figure 2-5—SAID format

Four SAID values are reserved for the purpose of establishing initial communication with key management or system management when an SAID has not already been negotiated. These SAID values are called “bootstrap” SAIDs, and identify preestablished security associations. If the bootstrap SAID is used for key management, the ID bits contain all zeroes. If the bootstrap SAID is used for system management, the ID bits contain all ones. The use of the bootstrap SAID mechanism is optional. Communication to the System Management and Key Management Stacks may be accomplished via the use of any security association whose SDE_SAP object indicates the appropriate stack. Also note that the function of key management or system management can reside on a User Stack; however, the bootstrap SAIDs cannot be used to support those implementations.

⁹The reserved LSAP contains the binary value 0101 0000, where the leftmost digit is the least significant. This value has been assigned by ISO and IEC to ensure unique identification of SDE PDUs. The value of the Unnumbered Information Control field is 1100 0000, where the first “1” is the least significant bit. In hexadecimal, the SDE Designator is represented as a sequence of three octets with values 0A 0A 03, ordered left to right.