

IEEE Std 802.10-1998
(Revision of IEEE Std 802.10-1992,
incorporating IEEE Std 802.10b-1992,
802.10e-1993, 802.10f-1993,
802.10g-1995, and 802.10h-1997)

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

Sponsor

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

Approved 17 September 1998

IEEE SA-Standards Board

Abstract: IEEE 802.10 provides specifications for an interoperable data link layer security protocol and associated security services. The Secure Data Exchange (SDE) protocol is supported by an application layer Key Management Protocol (KMP) that establishes security associations for SDE and other security protocols. A security label option is specified that enables rule-based access control to be implemented using the SDE protocol. A method to allow interoperability with type-encoded Medium Access Control (MAC) clients is also provided, as well as a set of managed object classes to be used in the management of the SDE sublayer and its protocol exchanges.

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 © 1998 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 1998. Printed in the United States of America.

ISBN 0-7381-1419-7

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 IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) 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 societies and Standards Coordinating 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:

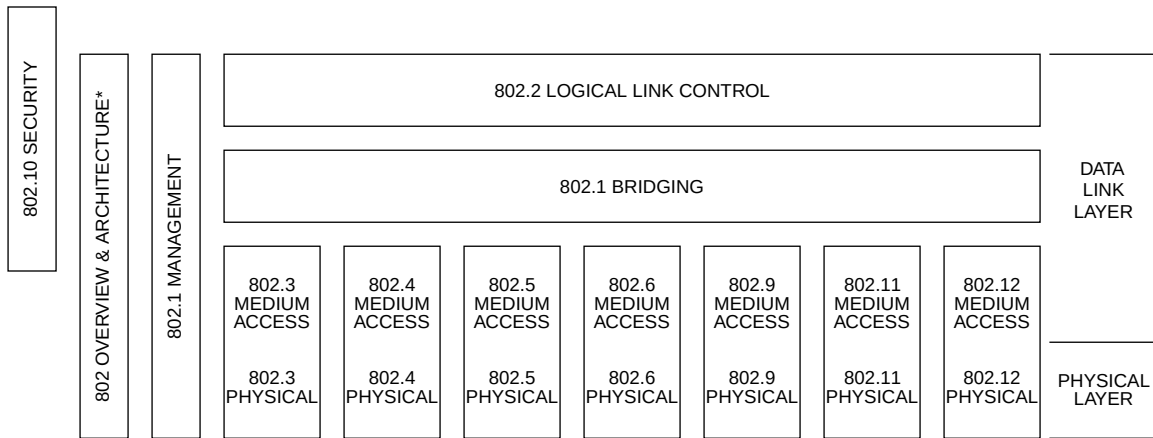
Secretary, IEEE-SA Standards Board
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
USA

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 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; (978) 750-8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Introduction to IEEE Std 802.10-1998

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.)



* Formerly IEEE Std 802.1A.

This family of standards deals with the Physical and Data Link layers as defined by the International Organization for Standardization (ISO) Open Systems Interconnection (OSI) Basic Reference Model (ISO/IEC 7498-1 : 1994). The access standards define seven 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 the technologies noted above are as follows:

- IEEE Std 802 *Overview and Architecture.* This standard provides an overview to the family of IEEE 802 Standards.
- ANSI/IEEE Std 802.1B and 802.1k [ISO/IEC 15802-2] *LAN/MAN Management.* Defines an OSI management-compatible architecture, and services and protocol elements for use in a LAN/MAN environment for performing remote management.
- ANSI/IEEE Std 802.1D [ISO/IEC 15802-3] *Media Access Control (MAC) Bridges.* Specifies an architecture and protocol for the interconnection of IEEE 802 LANs below the MAC service boundary.
- ANSI/IEEE Std 802.1E [ISO/IEC 15802-4] *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.
- ANSI/IEEE Std 802.1F *Common Definitions and Procedures for IEEE 802 Management Information*
- ANSI/IEEE Std 802.1G [ISO/IEC 15802-5] *Remote Media Access Control (MAC) Bridging.* Specifies extensions for the interconnection, using non-LAN communication technologies, of geographically separated IEEE 802 LANs below the level of the logical link control protocol.
- ANSI/IEEE Std 802.2 [ISO/IEC 8802-2] *Logical Link Control*
- ANSI/IEEE Std 802.3 [ISO/IEC 8802-3] *CSMA/CD Access Method and Physical Layer Specifications*
- ANSI/IEEE Std 802.4 [ISO/IEC 8802-4] *Token Passing Bus Access Method and Physical Layer Specifications*

- ANSI/IEEE Std 802.5 [ISO/IEC 8802-5] *Token Ring Access Method and Physical Layer Specifications*
- ANSI/IEEE Std 802.6 [ISO/IEC 8802-6] *Distributed Queue Dual Bus Access Method and Physical Layer Specifications*
- ANSI/IEEE Std 802.9 [ISO/IEC 8802-9] *Integrated Services (IS) LAN Interface at the Medium Access Control (MAC) and Physical (PHY) Layers*
- ANSI/IEEE Std 802.10 *Interoperable LAN/MAN Security*
- ANSI/IEEE Std 802.11 [ISO/IEC DIS 8802-11] *Wireless LAN Medium Access Control (MAC) and Physical Layer Specifications*
- ANSI/IEEE Std 802.12 [ISO/IEC 8802-12] *Demand Priority Access Method, Physical Layer and Repeater Specifications*

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

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

The following additional working group has authorized standards projects under development:

- 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.

IEEE Std 802.10-1998

The IEEE 802.10 Working Group was formed in May of 1988 to address the security LANs and MANs. It is sponsored by the IEEE LAN/MAN Standards Committee (LMSC). The working group currently has representation from vendors and users of security technology, and previously has also had representation from the government and general interest communities. The standard is an interoperability standard that is compatible with the existing IEEE 802 and OSI architectures.

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 the revision of standard was completed, the 802.10 LAN/MAN Security Working Group had the following membership:

Kenneth G. Alonge, *Chair and Technical Editor*
Joseph Maley, *Recording Secretary*

Russell Housley, *Vice Chair*
Richard McAllister, *Executive Secretary*

The following persons were on the balloting committee:

William B. Adams
Don Aelmore
Kenneth G. Alonge
Alan Arndt
Kit Athul
Thomas W. Bailey
Kathleen L. Briggs
Peter K. Campbell
James T. Carlo
David E. Carlson
Paul Chen
John Cronican
Robert S. Crowder
Philip H. Enslow
Changxin Fan
Mark R. M. Ferguson
Harvey A. Freeman
Gautam Garai
Patrick S. Gonia
Julio Gonzalez-Sanz

Russell D. Housley
Walter K. Hurwitz
Raj Jain
Gary C. Kessler
Stephen Barton Kruger
Kenneth C. Kung
Lanse M. Leach
Pil Joong Lee
Randolph S. Little
Joseph G. Maley
Peter Martini
Bennett Meyer
David S. Millman
Warren Monroe
John E. Montague
Shimon Muller
Paul Nikolich
Robert O'Hara
Donal O'Mahony
John M. Osepchuk
Roger Pandanda

Lucy W. Person
Ronald C. Petersen
Vikram Punj
Edouard Y. Rocher
James W. Romlein
Floyd E. Ross
Christoph Ruland
Norman Schneidewind
Donald A. Sheppard
Leo Sintonen
William R. Smith
Efsthios D. Sykas
Patricia Thaler
Geoffrey O. Thompson
Mark-Rene Uchida
John Viaplana
Elfed T. Weaver
Donald F. Weir
Qian-li Yang
Oren Yuen

When the IEEE-SA Standards Board approved this standard on 16 September 1998, it had the following membership:

Richard J. Holleman, *Chair*

Donald N. Heirman, *Vice Chair*

Judith Gorman, *Secretary*

Satish K. Aggarwal
Clyde R. Camp
James T. Carlo
Gary R. Engmann
Harold E. Epstein
Jay Forster*
Thomas F. Garrity
Ruben D. Garzon

James H. Gurney
Jim D. Isaak
Lowell G. Johnson
Robert Kennelly
E. G. "Al" Kiener
Joseph L. Koepfinger*
Stephen R. Lambert
Jim Logothetis
Donald C. Loughry

L. Bruce McClung
Louis-François Pau
Ronald C. Petersen
Gerald H. Peterson
John B. Posey
Gary S. Robinson
Hans E. Weinrich
Donald W. Zipse

*Member Emeritus

Kristin M. Dittmann
IEEE Standards Project Editor

Contents

1. Overview and model	1
1.1 Scope and purpose	1
1.2 References.....	1
1.3 Definitions and acronyms	3
1.4 Architecture	9
2. Secure Data Exchange (SDE)	9
2.1 Overview.....	9
2.2 Definitions	10
2.3 SDE security services	10
2.4 SDE service specifications	11
2.5 SDE PDU structure.....	13
2.6 SDE procedure.....	16
2.7 Minimum Essential Requirements (MERs).....	26
2.8 SDE sublayer management.....	27
3. Key Management	54
4. Bibliography	54
Annex 2A (informative) Service rationale	55
Annex 2B (informative) Example.....	65
Annex 2C (informative) Objectives of SDE	72
Annex 2D (informative) Rationale for placement.....	73
Annex 2E (normative) Fragmentation	77
Annex 2F (normative) ASN.1 encodings	82
Annex 2G (normative) Allocation of object identifier values.....	85
Annex 2H (informative) Recommended practice for SDE with IEEE 802.3 Type-encoded frames.....	91
Annex 2I (normative) Secure data exchange security label.....	94
Annex 2J (informative) Security label set registration service	102
Annex 2K (informative) Basic processing rules for security labels.....	103
Annex 2L (normative) Secure Data Exchange (SDE) Protocol Implementation Conformance Statement (PICS) proforma.....	106

IEEE Standards for Local and Metropolitan Area Networks:

Standard for Interoperable LAN/MAN Security (SILS)

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 in IEEE 802 LANs and MANs is described in Clause 3 (published separately as IEEE Std 802.10c-1998). 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 References

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

NOTE—Additional references are listed in 1.3 of IEEE Std 802.10c-1998.

ANSI X9.17-1985 (R1991), Financial Institution Key Management (Wholesale).¹

FIPS PUB 188: 1994, Standard Security Label for Information Transfer (SSL).²

IEEE Std 802-1990, IEEE Standards for Local Area Networks: Overview and Architecture.³

¹ANSI publications are available from the Sales Department, American National Standards Institute, 11 West 42nd Street, 13th Floor, New York, NY 10036, USA (<http://www.ansi.org/>).

²FIPS publications are available from the National Technical Information Service (NTIS), 5285 Port Royal Road, Springfield, VA 22161 USA, tel. (703) 605-6000.

³IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA (<http://standards.ieee.org/>).

IEEE Std 802.1F-1993 (Reaff 1998), IEEE Standards for Local and Metropolitan Area Networks: Common Definitions and Procedures for IEEE 802 Management Information.

Internet RFC 1457: 1993, R. Housley, Security Labeling Framework for the Internet.⁴

ISO/IEC 7498-1: 1994, Information technology—Open Systems Interconnection—Basic Reference Model—Part 1: The Basic Model.⁵

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

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

ISO/IEC 8802-2: 1998 [ANSI/IEEE Std 802.2, 1998 Edition], Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical link control.⁶

ISO/IEC 8824: 1990, Information technology—Open Systems Interconnection—Specification of Abstract Syntax Notation One (ASN.1) (Provisionally retained edition).

ISO/IEC 8825: 1990, Information technology—Open Systems Interconnection—Specification of basic encoding rules for Abstract Syntax Notation 1 (ASN.1) (Provisionally retained edition).

ISO/IEC 9595: 1991, Information technology—Open Systems Interconnection—Common management information service definition.

ISO/IEC 9596-1: 1991, Information technology—Open Systems Interconnection—Common management information protocol—Part 1: Specification.

ISO/IEC 9596-2: 1993, Information technology—Open Systems Interconnection—Common management information protocol—Part 2: Protocol Implementation Conformance Statement (PICS) proforma.

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

ISO/IEC 10164-1: 1993, Information technology—Open Systems Interconnection—Systems Management—Part 1: Object Management Function.

ISO/IEC 10165-1: 1993, Information technology—Open Systems Interconnection—Structure of management information—Part 1: Management Information Model.

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

ISO/IEC 10165-4: 1992, Information technology—Open Systems Interconnection—Structure of management information—Part 4: Guidelines for the definition of managed objects.

⁴Internet Requests for Comments (RFCs) are available from the DDN Network Information Center, SRI International, Menlo Park, CA 94025 USA. They are also available on the World Wide Web at the following URL: <http://www.internic.net/ds/rfc-index.html>.

⁵ISO and ISO/IEC publications are available from ISO, Case Postale 56, 1 rue de Varembe, CH-1211, Genève 20, Switzerland/Suisse (<http://www.iso.ch/>). 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.

ISO/IEC 10165-6: 1997, Information technology—Open Systems Interconnection—Structure of management information—Part 6: Requirements and guidelines for implementation conformance statement proforma associated with OSI management.

ISO/IEC 15802-1: 1995, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 1: Medium Access Control (MAC) service definition.

ISO/IEC 15802-2: 1995 [ANSI/IEEE Std 802.1B and IEEE Std 802.1k, 1995 Edition], Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Common specifications—Part 2: LAN/MAN management, service and protocol.

NISTIR 5308: 1993, N. Nazario, General Procedures for Registering Computer Security Objects.⁷

1.3 Definitions and acronyms

1.3.1 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.

1.3.1.1 access control: The prevention of unauthorized use of a resource, including the prevention of use of a resource in an unauthorized manner. (ISO/IEC 7498-2: 1989)⁸

1.3.1.2 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)

1.3.1.3 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.

1.3.1.4 bootstrap SAIDs: Four SAID values that 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 have a preestablished security association.

1.3.1.5 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.

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

1.3.1.7 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])⁹

1.3.1.8 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)

⁷This publication is available from the National Technical Information Service (NTIS), U. S. Dept. of Commerce, 5285 Port Royal Rd., Springfield, VA 22161 USA.

⁸Information on references can be found in 1.2.

⁹The numbers in brackets preceded by the letter B correspond to those of the bibliography in Clause 4.

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

1.3.1.10 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.

1.3.1.11 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.

1.3.1.12 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.

1.3.1.13 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.

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

1.3.1.15 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/IEC 7498-2: 1989)

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

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

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

1.3.1.19 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/IEC 7498-2: 1989)

1.3.1.20 decipherment: The reversal of a corresponding reversible encipherment. (ISO/IEC 7498-2: 1989)

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

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

1.3.1.23 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.

1.3.1.24 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: 1990)

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

1.3.1.26 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 checkvalue.

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

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

1.3.1.29 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.

1.3.1.30 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/IEC 7498-1: 1994)

1.3.1.31 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)

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

1.3.1.33 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)

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

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

1.3.1.36 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.

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

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

1.3.1.39 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/IEC 7498-1: 1994)

1.3.1.40 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/IEC 7498-2: 1989) *Note:* This is primarily intended for, although not limited to, connection-oriented service and may be either unilateral or mutual.

1.3.1.41 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 of which it is a member. 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.

1.3.1.42 policy: *See:* security policy.

1.3.1.43 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)

1.3.1.44 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 7498-1: 1994)

1.3.1.45 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.

1.3.1.46 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)

1.3.1.47 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.

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

1.3.1.49 secure data exchange (SDE) Layer Manager (LM): The SDE portion of the Layer 2 Manager.

1.3.1.50 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.

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

1.3.1.52 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.

1.3.1.53 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/IEC 7498-2: 1989)

1.3.1.54 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.

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

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

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

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

1.3.1.59 security threat: A potential violation of security. (ISO/IEC 7498-2: 1989)

1.3.1.60 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.

1.3.1.61 system 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/IEC 7498-1: 1994)

1.3.1.62 Tag Set Name: A numeric identifier associated with a set of security tags. (FIPS PUB 188: 1994)

1.3.1.63 threat: A potential violation of security. (ISO/IEC 7498-2: 1989)

1.3.1.64 transparent: The state of a protocol when 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.

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

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

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

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

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

1.3.2 Acronyms

This subclause contains acronyms that are applicable to the standard.

NOTE—Additional acronyms are listed in 1.2.1 of IEEE Std 802.10c-1998.

ANSI	American National Standards Institute
ASN.1	Abstract Syntax Notation One
CMIP	Common Management Information Protocol
CMIS	Common Management Information Service
CSOR	Computer Security Objects Register
DA	Destination Address
DEA	Data Encryption Algorithm

DIS	Draft International Standard
DMI	Definition of Management Information
DSAP	Destination Service Access Point
GDMO	Guidelines for the Definition of Managed Objects
ICV	Integrity Check Value
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IV	Initialization Vector
LAN	Local Area Network
LLC	Logical Link Control
LM	Layer Manager
LME	Layer Management Entity
LMI	Layer Management Interface
LMMP	LAN/MAN Management Protocol
LMMPE	LAN/MAN Management Protocol Entity
LMMS	LAN/MAN Management Service
LMMU	LAN/MAN Management User
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
MIS-User	Management Information Services User
MO	Managed Object
MOCS	Management Object Conformance Statement
MSDU	MAC Service Data Unit
NM	Network Management
NMI	Network Management Interface
OID	Object Identifier
OSI	Open Systems Interconnection
OUI	Organizationally Unique Identifier
PDU	Protocol Data Unit
PE	Protocol Entity
PICS	Protocol Implementation Conformance Statement
RDN	Relative Distinguished Name
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
SMI	Structure of Management Information
SMIB	Security Management Information Base
SNAP	Subnetwork Service Access Point
SSAP	Source Service Access Point
SSL	Standard Security Label
TCB	Trusted Computing Base

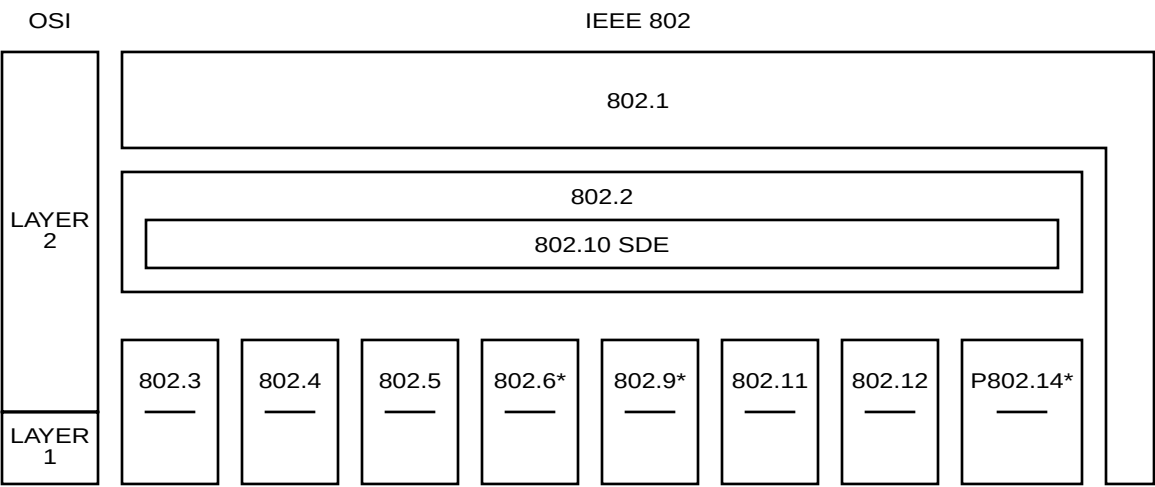
1.4 Architecture

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.¹⁰

2. Secure Data Exchange (SDE)

2.1 Overview

The SDE is an OSI Basic Reference Model (ISO/IEC 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.



*SDE is not applicable to MANs using isochronous and connection-oriented protocols.

Figure 2-1—Relationship to IEEE 802 reference model

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.¹¹ SDE security services provided to a Key Management Stack or to a System Management Stack require the LLC protocol.

¹⁰This subclause will be included in IEEE P802.10a, which at the time of this publication was not an approved IEEE standard, but is available as a draft. For information about obtaining draft standards, contact the IEEE.

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

See 1.3.1.

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 one or a combination of the following: key management, system management, and the labeling of SDE PDUs. 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

¹¹ To use the management functionality of ISO/IEC 15802-2, LAN/MAN management, service and protocol, 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.

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

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 15802-1: 1995.

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.

The primitives used across the SDE service interface are a subset of the MAC primitives defined in ISO/IEC 15802-1: 1995. Additional primitives specified by other MAC interfaces shall be passed unaltered through

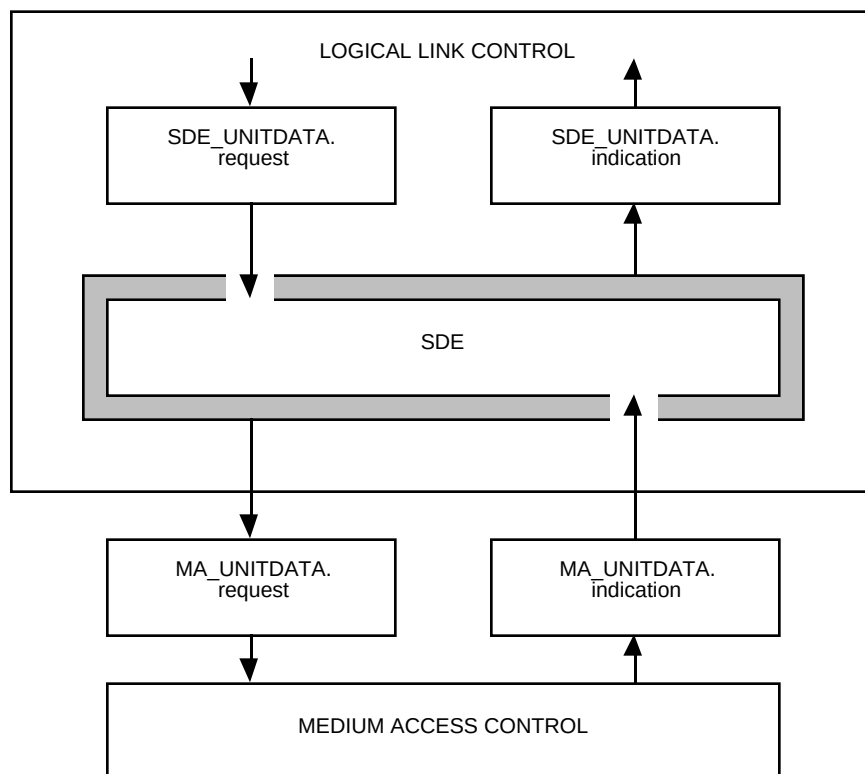


Figure 2-2—SDE primitives

SDE. Likewise, the minimum set of parameters of these primitives is specified. Other MAC interfaces, such as those in ISO/IEC 8802-5: 1998 [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 15802-1: 1995.

2.4.2 SDE_UNITDATA.indication parameters

The parameters associated with the SDE_UNITDATA.indication are defined in ISO/IEC 15802-1: 1995.

2.4.3 Services assumed

The service primitives assumed at the lower boundary of SDE are those defined in ISO/IEC 15802-1: 1995.

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.

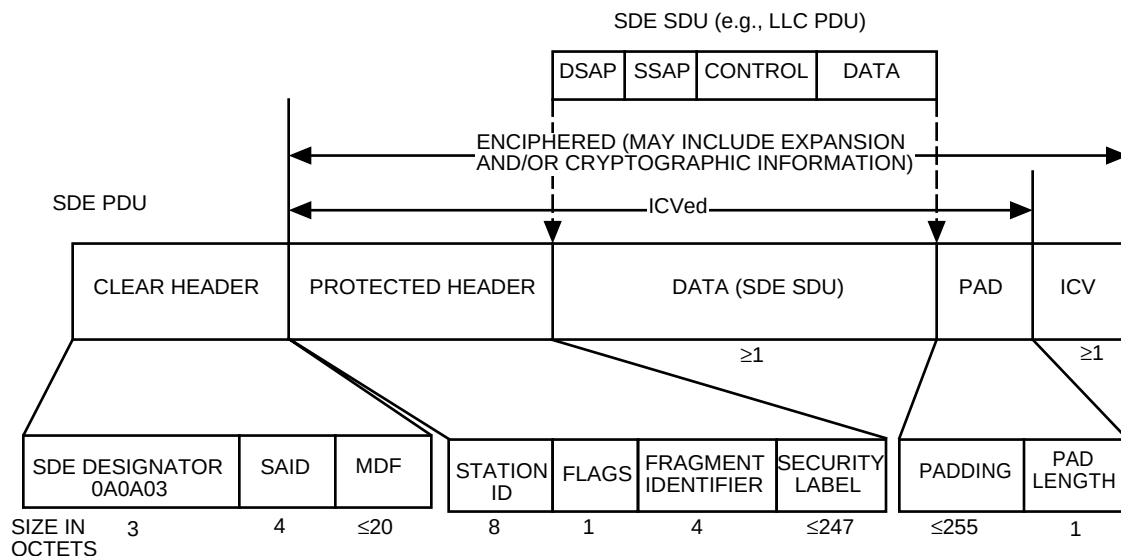


Figure 2-3—Structure of the SDE PDU

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.¹² When the Clear Header is present, its length will be from seven to 27 octets, inclusive.

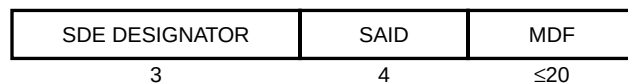


Figure 2-4—Clear Header

¹² Some bridges operate on data outside the MAC header. As a result, SDE frames that do not include the SDE Designator may not be processed correctly. Therefore, when bridges of this type are employed, the option for Clear Header should be selected.

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/IEC 8802-2: 1998 (P-bit equal to zero), in the third octet. 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.

The 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.

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).

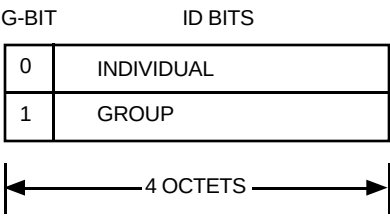


Figure 2-5—SAID format

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.

When the destination address is a group address, key management or system management will create group security associations by assigning a unique group SAID, distributing the keying material to the group members, and determining which services will be used for secure transmission of multicast data. To ensure that key management and system management can assign unique group SAIDs, the available numbers are divided as shown in Figure 2-6. Since some managers will be responsible for a large number of group security associations and other managers will be responsible for a few group security associations, three different group SAID classes are defined. The first class allows 1024 different managers, each responsible for 1 048 576 group security associations. A product vendor may obtain an identifier associated with this class

and assign a portion of the numbers to each instance of their product. The second class allows 131 072 different managers, each responsible for 4096 group security associations. The third class allows 2 097 152 different managers, each responsible for 256 group security associations.

One identifier from the third class of group SAIDs is reserved for testing and managers on isolated LANs. This reserved identifier is 800001 (hexadecimal). Therefore, group SAIDs between 80000100 and 800001FF (hexadecimal) are reserved for this purpose.

G-BIT	S1-BIT	S2-BIT	ID BITS	
0	INDIVIDUAL SAID			
1	1	10 BITS	20 BITS	
1	0	1	17 BITS	12 BITS
1	0	0	21 BITS	8 BITS

Figure 2-6—Group SAID Format

For the purpose of assigning group SAID identifiers, the Institute of Electrical and Electronics Engineers, Inc., USA, is the Registration Authority.¹³

2.5.2.1.3 Management-Defined field (MDF)

The MDF allows the transfer of information that may facilitate, but is not required for, the processing of the PDU. The MDF is variable in length and is an integral number of octets up to a maximum of 20. Its value is indicated by an entry in the SMIB. The MDF may contain any value and is *not* used to determine the appropriate security association. The MDF value is a unidirectional attribute of the security association and is constant for the duration of that security association. The MDF is optional.

An example of the application of the MDF is an SDE implementation that does not retain cryptographic state information. The transfer of cryptographic state information and keying information in the MDF could facilitate reception processing.

2.5.2.2 Protected Header

The Protected Header is in the portion of the SDE PDU to which the security services are applied. If present, the Protected Header contains up to four optional fields. The fields are Station ID, Flags, Fragment Identifier, and Security Label. These fields shall appear in the order listed if all options are selected. The Station ID uniquely identifies the originating station. It is eight octets and contains the canonical form of the MAC address as specified in IEEE Std 802-1990, Section 5.2. The first octet of the Station ID field shall contain the first octet of the MAC address; the contents of the field after the MAC address is undefined. Annex 2E covers the use of the Flags and Fragment Identifier fields to support fragmentation. Security labels are discussed in Annex 2I.

2.5.2.3 Data

The Data portion of the SDE PDU contains the SDE SDU, which is the MSDU parameter of the SDE service primitive.

¹³Communications regarding registration should be addressed to Registration Authority for IEEE Std 802.10, c/o Institute of Electrical and Electronics Engineers, 445 Hoes Lane, P.O. Box 1331, Piscataway, NJ 08855-1331, USA, tel. (732) 562-3813.

2.5.2.4 Pad

The Pad consists of the Padding and Pad Length fields. The Pad may be used to provide padding for confidentiality and integrity algorithms.¹⁴ Pad is selected on a per-security-association basis. If it is selected, each PDU processed under the association shall contain the Pad Length field.

2.5.2.4.1 Padding field

The Padding field is optional but may be required by the specific confidentiality or integrity algorithm selected. The maximum size of the Padding field is 255 octets. The content of the Padding field is a local matter.

The Padding field specifies an integral number of octets; therefore, the Padding field cannot be used to correct octet alignment problems caused by either the integrity or confidentiality algorithms.

2.5.2.4.2 Pad Length field

The value of the Pad Length field contains the number of octets in the Padding field. This value does not include the one octet required by the Pad Length field itself. If no integrity is requested, the Pad Length field is the last octet of the SDE PDU. If integrity is requested, the Pad Length field is the octet before the ICV.

2.5.2.5 ICV field

The ICV field is a security mechanism for detecting data modification. The ICV value, if present, is contained in the last field in the SDE PDU. The length of the ICV is an attribute of the security association. The ICV is calculated over the Protected Header, the Data field, and Pad. It is an optional field.

2.5.3 Building the SDE PDU

The means by which the information passed to the MAC is used to construct the SDE PDU is described in this subclause. (The MSDU is the SDE SDU.) All of the parameters of the service request except the MSDU are copied unaltered from the SDE_UNITDATA.request to the MA_UNITDATA.request. Likewise, on incoming processing, all parameters except the MSDU are copied unaltered from the MA_UNITDATA.indication to the SDE_UNITDATA.indication. The MSDU is used to generate the SDE PDU as shown in Figure 2-7. On reception, the process is reversed to reconstruct the MSDU. The encipherment algorithm may require the addition of fields specific to the algorithm. These fields will be added and removed as part of the encipherment or decipherment processing. They will be transmitted as part of the SDE PDU provided in the MSDU of the MAC service primitives. An example of this type of field is the Initialization Vector (IV) required by certain algorithms.

2.6 SDE procedure

All elements of the SDE procedures, including transmission and reception processing and all other elements that direct those procedures, are defined in this subclause. These other elements include management architecture, addressing, the SMIB, and the definitions of the managed objects.

The SDE management architecture is described in 2.6.1. The architectural description includes the following:

- a) The relationship between the management application entity and the SDE Layer Manager (LM);

¹⁴Many confidentiality algorithms take blocks (n bits) of cleartext and transform this cleartext to ciphertext as a unit. This block is known as a cryptographic block. The confidentiality algorithm may require that the input cleartext be a multiple of this block size. If the chosen confidentiality or integrity algorithm has this restriction, then the SDE protocol uses the Pad to make sure that the cleartext is a multiple of the block size. (The Pad follows the Data to allow stream processing for outgoing PDUs.)

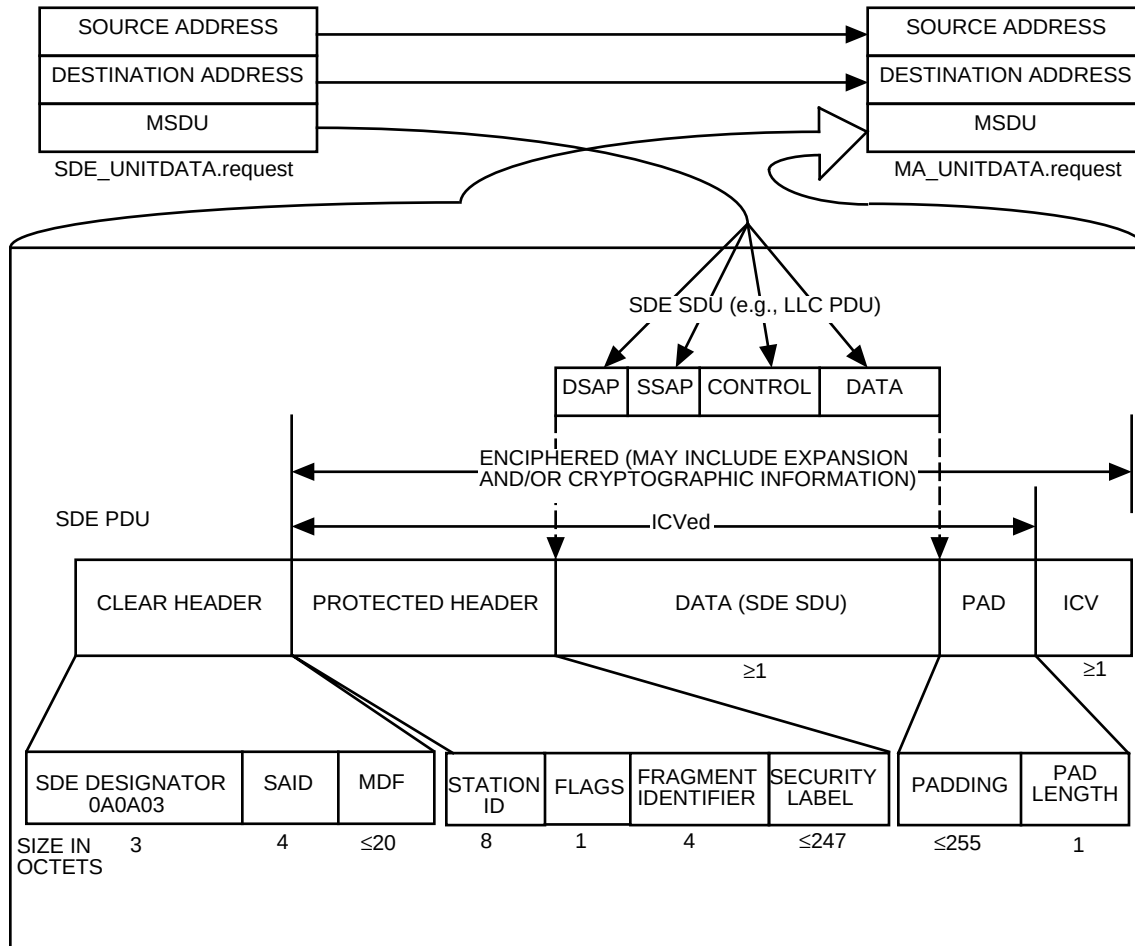


Figure 2-7—Construction of the SDE PDU

- b) The role of the SMIB in their relationship;
- c) How security associations are coordinated through the use and the exchange of SAIDs; and
- d) The structure of the SDE managed objects.

The type of addressing used by the SDE entity is described in 2.6.2. The details of the SDE objects that are attributes of SDE managed objects are described in 2.6.3. Finally, the transmission and reception procedures are described in 2.6.4 and 2.6.5, respectively.

2.6.1 SDE management architecture

Each station that employs the SDE protocol has access to an SMIB. The SMIB contains a list of the current security associations. Key management and security management or both are responsible for maintaining this information base.

The SMIB provides the interface between the local System Management Application Entity (SMAE) and the LM of the protocol stack. This is illustrated in Figure 2-8.

There are three types of SDE managed objects: station, Service Access Point (SAP), and security association. Station objects, which set certain parameters for the SDE entity, apply to all processing by the SDE entity. The SAP objects apply to a specific SAP. The security association objects apply only to a specific instance of PDU transmission, reception, or both.

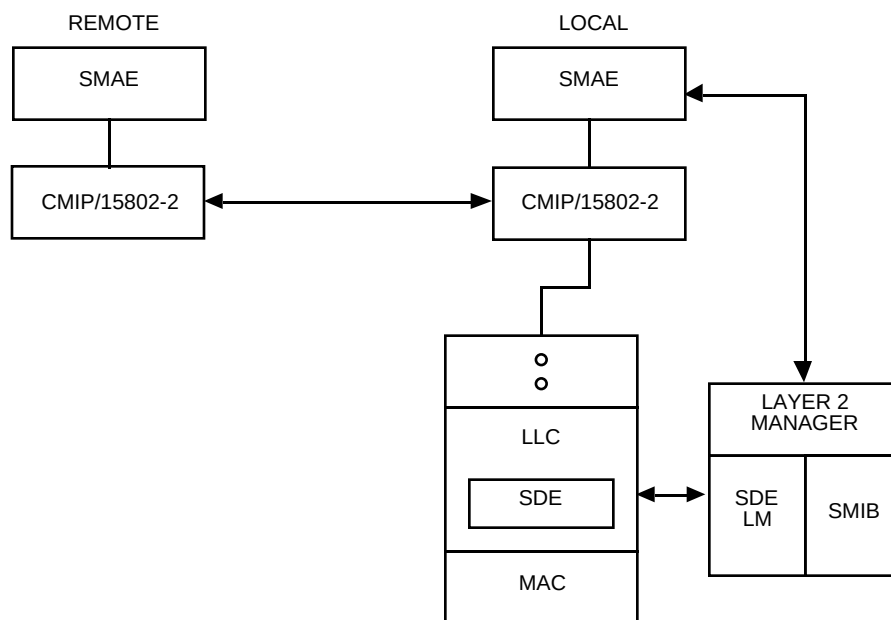


Figure 2-8—SDE management architecture

Since multiple security associations can exist at any time, the SDE entity shall identify which security association applies to that SDE PDU. For example, this identification may be passed via the optional SAID.

How the value of the SAID is coordinated between SDE entities is independent of the SDE protocol; however, it is useful to examine how a pairwise SAID could be established. During either a key or system management exchange, parties A and B exchange the values of the attributes of the security association managed object. These values specify the security parameters (e.g., the security services employed, keys, etc.) that will be needed for the security association. In this example, the SAID identifies this security association. This process is illustrated in Figure 2-9.

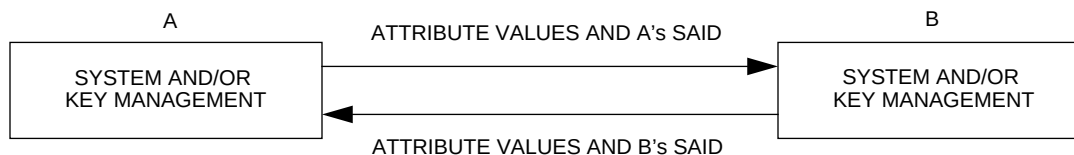


Figure 2-9—Initial exchange

System and/or key management enters the value for the security association object into the SMIB. An example of an SMIB that contains a table of security associations and the values of the associated attributes is illustrated in Figure 2-10.

The security association shall be selected for each PDU transferred through the SDE entity. Outgoing PDUs are PDUs that originate at one of the SDE stacks (i.e., System Management Stack, Key Management Stack, or one of the User Stacks) and are to be delivered to the MAC sublayer. Incoming PDUs are PDUs that arrive from the MAC sublayer and are to be delivered to one of these stacks. Incoming PDUs may contain the SDE Clear Header, which can be used to select the security association; whereas the Clear Header may be created for outgoing PDUs after the security association has been found. For this reason, the mechanism for select-

ATTRIBUTES								
SECURITY ASSOCIATION #1	SECURITY ASSOCIATION #1 ATTRIBUTE VALUES							
○ ○ ○								
SECURITY ASSOCIATION #n	SECURITY ASSOCIATION #n ATTRIBUTE VALUES							

Figure 2-10—Example SMIB containing security associations

ing the security associations can be different. The different parameters and/or PDU fields that can be used for selecting the appropriate security association from the SMIB are shown in Figure 2-11.

Outgoing
— SDE SAP and/or outgoing MAC SA/DA pair
Incoming
— SAID and/or incoming MAC SA/DA pair

Figure 2-11—Parameters used for selecting security association

2.6.2 Addressing

All addresses referred to in this protocol are either LSAP addresses or MAC addresses. The LSAP address syntax and semantics are defined in ISO/IEC 8802-2: 1998, while the specifics of the MAC addresses are defined in IEEE Std 802-1990.

The Station ID contains the MAC address corresponding to the individual address of the station that originated the outgoing PDU. In group transmissions with a shared secret key, the Station ID prevents parties external to the multicast group from tricking the receiving party into believing that the PDU came from a party other than its originator. It does *not* prevent members within the same group from changing PDUs so that they appear to have originated from another valid member of the same group. The inclusion of a Station ID also provides protection against reflection where that protection is not provided implicitly by the SDE confidentiality or integrity algorithms or from the services of the key management protocols.

2.6.3 SDE objects

Security managed objects as outlined in 2.6.1 are described in this subclause. Security objects that apply to the entire SDE are described in 2.6.3.1; security objects that apply to transmission to and from an SDE SAP are described in 2.6.3.2; security objects that are specific to the security associations are described in 2.6.3.3; and SAIDs are described in 2.6.3.4.

2.6.3.1 Station objects

The station objects apply to the entire SDE regardless of security association. The formal definition of each of the objects in the SDE clause will be defined in 2.8, SDE sublayer management. The objects described in this and the following two subclauses are abstractions provided for the purpose of describing the protocol

processing. Some implementations may choose only manual management of these objects; in which case, the representation becomes a purely local matter. In this and the following two subclauses, the object names will be in boldface type.

- a) **Station_Clear_Hdr:** Boolean. Station_Clear_Hdr=TRUE indicates that the Clear Header is always used when communicating with other SDE entities.
Station_Clear_Hdr=FALSE indicates that there is no Clear Header expected on any incoming PDUs, and there is none placed on outgoing PDUs.
For communication using this mode of the protocol, both stations shall agree to have Station_Clear_Hdr=FALSE. Delivery of SDE PDUs with no clear header (Station_Clear_Hdr=False) will have unpredictable results if the receiving entity is one of the following:

Its Layer 2 entity does not employ SDE.

Its station object Station_Clear_Hdr=TRUE.

- b) **Station_MDF:** Boolean. Station_MDF shall be set to TRUE if the station sends or desires to receive the MDF in the Clear Header. The actual inclusion or exclusion of the MDF is determined by the value of the Assoc_MDF attribute.

2.6.3.2 SDE SAP objects

These objects may be defined by 2.8, SDE sublayer management, and in Annex 2E.

2.6.3.3 Security association objects

The SDE entity uses security associations available to it via the SMIB to provide the necessary services required for the secure transmission of data. The following are security objects that are attributes of a security association managed object:

- a) **Local_SAID:** Octetstring. This contains the value of the SAID expected in incoming PDUs if Station_Clear_Hdr=TRUE.
- b) **Remote_SAID:** Octetstring. This contains the value placed in the SAID field of outgoing PDUs if Station_Clear_Hdr=TRUE.
- c) **Assoc_MDF:** Boolean. This indicates whether or not the MDF is used for the security association. If Station_MDF=FALSE, then this Boolean is always FALSE. The length and value of the MDF field in the PDU are unidirectional characteristics of the security association. Key management and/or system management can force this Boolean to FALSE. If the Boolean is TRUE, the value of the following attribute is placed in the MDF of outgoing PDUs:
 - 1) **Remote_MDF:** Octetstring. This attribute contains the value that will be placed in the MDF field in the Clear Header if the Assoc_MDF=TRUE.
- d) **Protection set:** These attributes indicate the security services to be provided by SDE.
 - 1) **Confid:** Boolean. If TRUE, it indicates that data confidentiality is to be provided for the security association.
 - 2) **Integ:** Boolean. If TRUE, it indicates that connectionless integrity is to be provided for the security association.
- e) **Security fields present:** Booleans indicate the presence (TRUE) or absence (FALSE) of security fields. These values shall remain constant over the life of the security association.
 - 1) **Padding_pres:** Boolean. Flag for the Pad Length field.
 - 2) **ID_pres:** Boolean. Flag for the Station ID.
- f) **Confid_Alg_ID:** Octetstring. This is a label that specifies a complex object corresponding to a confidentiality algorithm if Confid=TRUE. The definition of the algorithm shall include everything that is necessary for the encipherment or decipherment to occur. This includes, but is not limited to, the length and placement of IVs, block size, and mode of operation.

- g) **Integ_Alg_ID:** Octetstring. This is a label that specifies a complex object corresponding to an integrity algorithm if Integ=TRUE. The definition of the algorithm shall include everything that is necessary for the ICV to be calculated and verified upon receipt. This includes, but is not limited to, the length and placement of IVs, block size, and mode of operation.
- h) **SDE_SAP:** Octetstring. This indicates the SDE SAP for the security association. This is used as part of the index into the SMIB for outgoing PDUs. On incoming PDUs, it indicates which protocol stack should receive the PDU.
- i) **Remote_SDE:** Boolean. This boolean is TRUE if the remote entity implements SDE protocol and is FALSE otherwise.
- j) **Outgoing_Source_MAC_Address:** Octetstring. This corresponds to the individual address of the station that originated the outgoing PDU. It is the value included in the Station ID field of the Protected Header.
- k) **Outgoing_Destination_MAC_Address:** Octetstring. This address may be an individual or group address associated with the remote station(s).
- l) **Incoming_Destination_MAC_Address:** Octetstring. This may be an individual or group address associated with the local station.
- m) **Incoming_Source_MAC_Address:** Octetstring. If the Incoming_Destination_MAC_Address is an individual address, this object contains a single individual address. If the Incoming_Destination_MAC_Address is a group address, this object contains a list of individual addresses.

Within the SDE entity, the security association is represented by the security association object. Generic entries corresponding to multiple MAC addresses may be allowed in the SMIB depending on local policy. Changing the values of any of the security association attributes (or attributes of the complex objects labeled by the Confid_Alg_ID and the Integ_Alg_ID attributes) causes a new security association to be formed and the prior security association to be invalidated. The SAID is a convenient tag for the identification of these objects.

2.6.3.4 SAIDs

The SAID is primarily used to identify the security association, although it can be used for other purposes. In security associations between two entities, each entity chooses its own SAID and communicates it to the remote entity during a system and/or key management exchange. In security associations for multicast or broadcast groups, it is the responsibility of system management and/or key management to assign and coordinate the SAID used for that multicast or broadcast group address. Half of the possible values of the SAIDs are reserved as group SAIDs (see Figure 2-5).

There are bootstrap values (see 2.5.2.1.2) for the SAID that are sometimes used for communications with the System Management and/or Key Management Stacks. The communications under these bootstrap SAIDs have no security protection (confidentiality, integrity) and do not have a Station ID. In addition, no padding can be applied.

2.6.4 Transmission procedures

The transmission procedures are those involved in processing an SDE_UNITDATA.request. The functions are represented as a flow chart shown in Figure 2-12. (Object values are contained in the SMIB.) Also, Annex 2B contains an example of the transmission and reception procedures using specific algorithms.

In response to an SDE_UNITDATA.request from the LLC sublayer, the supplied address parameters or the SDE SAP or both are used to search for a security association in the SMIB.

- a) If the search is successful, a security header comprised of a Clear Header and a Protected Header may be created and prepended to the Data field that contains the MSDU of the request. The options of integrity and/or confidentiality may be provided. A Pad may be created and an ICV may be com-

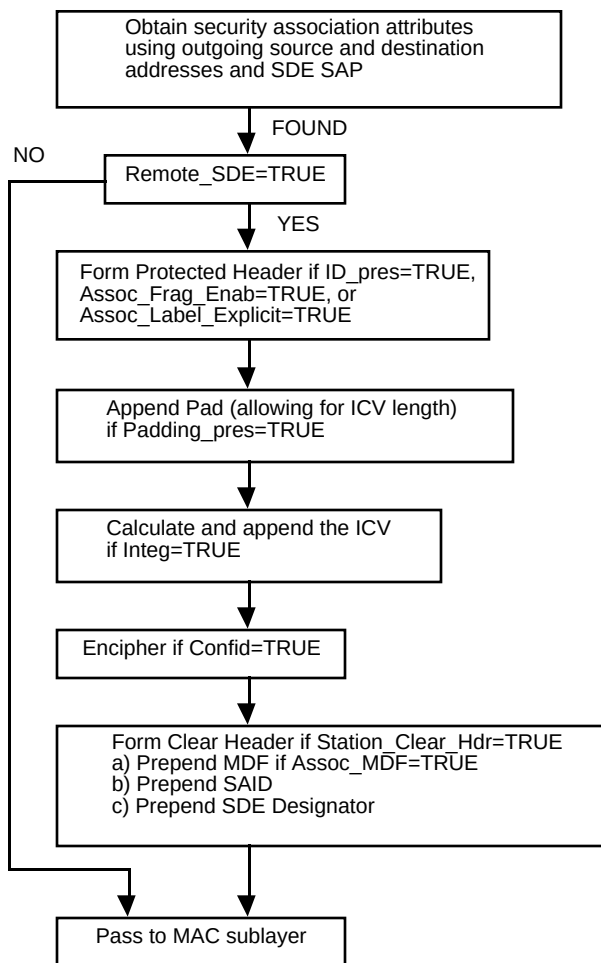


Figure 2-12—Transmission of an MA_UNITDATA.request

- puted; both are appended to the Data field. The Protected Header, Data, Pad, and the ICV may be enciphered. Finally, an MA_UNITDATA.request is constructed and passed on to the MAC sublayer.
- b) If no security association is found, the SDE LM is notified.

If the expansion causes the PDU to exceed the maximum size the MAC will accept, fragmentation may be required. Fragmentation is not part of this standard; however, if it is implemented, the method of fragmentation specified in Annex 2E is the recommended approach.

2.6.4.1 Obtaining the security association

The security association shall be retrieved from the SMIB if a security association exists. The outgoing MAC addresses and the SDE SAP are used to search for the security association in the SMIB. If a security association is found, the values for each object of the security association are returned. If the request is originated by system management and/or key management, the SMIB may contain a bootstrap SAID security association that will allow communication. If no security association is found corresponding to the SDE SAP and addresses specified in the SDE_UNITDATA.request, the SDE entity indicates the error to the SDE LM and discards the PDU.

From this step in the process until the end of transmission processing, it will be assumed that an appropriate security association is already established.

2.6.4.2 Transmission to non-SDE entities

If Remote_SDE = FALSE, bypass further SDE processing and pass the SDE_UNITDATA.request to the MAC sublayer.

2.6.4.3 Forming the Protected SDE Header

After the security association is retrieved from the SMIB, a Protected Header is formed and prepended to the Data field in the SDE_UNITDATA.request, if either one or a combination of the following are TRUE: ID_pres, Assoc_Frag_Enab, and Assoc_Label_Explicit.

If ID_pres=TRUE, the Outgoing_Source_MAC_Address is placed in the Station_ID field. The Station_ID is an optional field. Refer to Annex 2E for the appropriate processing if Assoc_Frag_Enab=TRUE. Refer to Annex 2I for the appropriate processing if Assoc_Label_Explicit=TRUE.

2.6.4.4 Pad

If padding is required by the security association (Padding_pres=TRUE), the maximum size of Pad is 256 octets (255 Padding octets plus a one octet Pad Length field). Pad may be used to expand the size of the outgoing PDU for the integrity algorithm, for the confidentiality algorithm, or in a local manner.

2.6.4.5 Calculation of the ICV

If integrity should be applied (Integ=TRUE), the ICV is computed over the Protected Header, Data, and Pad using the algorithm specified in the SMIB. The ICV is appended to the Data field.

2.6.4.6 Encipherment of the PDU

If confidentiality is an attribute of the security association (Confid=TRUE), then the Protected Header, Data, Pad, and ICV will be enciphered using the algorithm specified in the SMIB.

2.6.4.7 Clear Header

The Clear Header is used both to signal the remote SDE entity that the PDU had been processed by the local SDE entity and to supply the necessary information to determine the appropriate security association. If Station_Clear_Hdr=TRUE, the Clear Header is placed in the outgoing PDU.

MDF: If Assoc_MDF=TRUE, then the Remote_MDF is placed in the outgoing PDU. It is an optional field.

SAID: The Remote_SAID shall be placed in the SAID field of the PDU. It is a mandatory field when the Clear Header is present.

SDE Designator: The SDE Designator is placed as the first three octets in the outgoing PDU. It is a mandatory field when the Clear Header is present.

2.6.4.8 MAC request

The SDE PDU is passed to the MAC sublayer as the MSDU parameter in the MA_UNITDATA.request. All other parameters are passed through, unaltered, by the SDE entity.

2.6.5 Reception procedures

When an MA_UNITDATA.indication is received from the MAC sublayer, processing can vary, depending on the local management functions. The security association shall be identified, and the appropriate security

mechanisms are applied to the PDU. If appropriate, the PDU is deciphered and the ICV is checked. Finally, the SDE_UNITDATA.indication is forwarded to the designated stack.

If any security-relevant exceptions are encountered during processing by the SDE entity, the PDU in question is discarded and the SDE LM is notified.

The reception functions are those involved in processing an MA_UNITDATA.indication (see Figure 2-13).

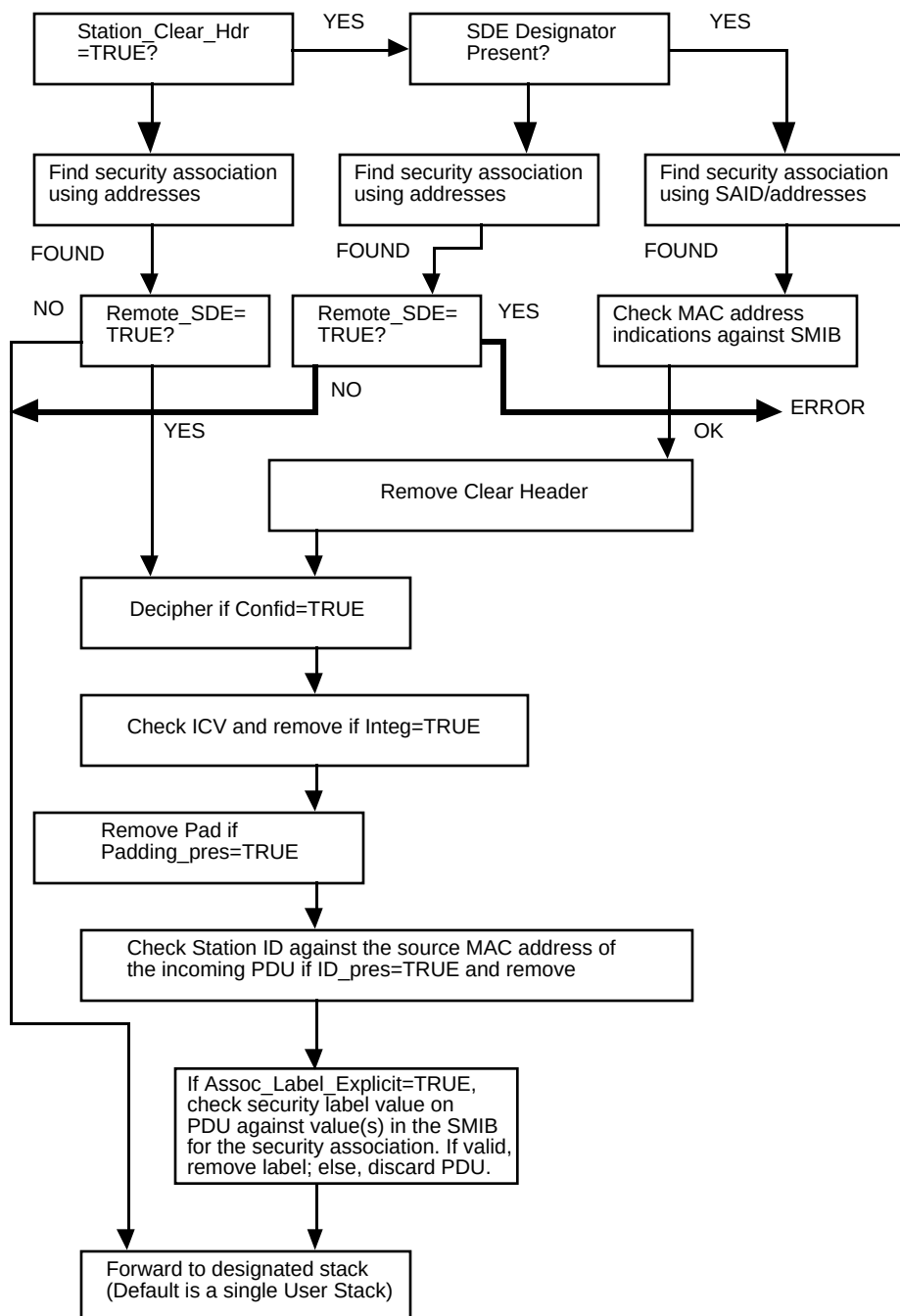


Figure 2-13—Reception of an MA_UNITDATA.indication

2.6.5.1 Requirements for reception

Before a station can process an incoming SDE PDU, a security association shall exist for communication to be allowed. Note that it is possible to configure the SMIB such that loss of information in the SMIB (e.g., power failure) could prevent automated recovery.

The bootstrap values of the SAID shall have a security association in the SMIB. There are four bootstrap values: Individual Key Management, Group Key Management, Individual System Management, and Group System Management.

2.6.5.1.1 Station configured for Clear Header

If Station_Clear_Hdr = TRUE, then the presence of an SDE Designator indicates that an SAID may be used for finding the security association. A security association shall exist for all communications, even with non-SDE entities. An association for communication with a non-SDE entity is found by searching the SMIB using the source and destination addresses. If the security association has Remote_SDE = FALSE, the PDU will bypass the rest of the security processing and be forwarded to the stack designated by the SDE SAP.

The SDE entity checks the source and destination address parameters in the MA_UNITDATA.indication against those denoted by the security association (Incoming_Source_MAC_Address and Incoming_Destination_MAC_Address). The security association in the SMIB may indicate the presence of an MDF. The MDF is used in a locally determined manner. The Clear Header is removed before the PDU is deciphered.

2.6.5.1.2 Station configured with no Clear Header

If Station_Clear_Hdr=FALSE, then the security association and the correct protocol stack shall be determined based on source and destination addresses in the MA_UNITDATA.indication. If Remote_SDE = FALSE for the security association, the PDU will bypass the rest of the security processing and be forwarded to the stack designated by the SDE SAP.

2.6.5.1.3 Decipherment of the PDU

If Confid=TRUE, the confidentiality algorithm is selected from the SMIB, and the PDU is deciphered.

2.6.5.2 ICV checking

If Integ=TRUE, the PDU is assumed to have an ICV that shall be checked using the chosen algorithm retrieved from the SMIB and subsequently removed from the PDU. If the ICV fails, the PDU is discarded and the SDE LM is notified.

2.6.5.3 Pad

The SDE entity strips any Pad that may be present in the PDU.

2.6.5.4 Station ID

If ID_pres=TRUE, the SDE entity checks that the contents of the Station ID field are the same as the source address in the MA_UNITDATA.indication. The Station ID field is removed.

2.6.5.5 Security label

If Assoc_Label_Explicit=TRUE, the SDE entity checks the security label value to ensure that it is within the set of allowed values for the association in the SMIB. If valid, the security label is removed. If not valid, discard the PDU and notify local management.

Refer to Annex 2I for detailed security label processing.

2.6.5.6 SDE_UNITDATA.indication

The parameters received in the MA_UNITDATA.indication are passed up to the appropriate protocol stack in the SDE_UNITDATA.indication with the SDE SDU (e.g., the LLC PDU) replacing the received MSDU.

2.7 Minimum Essential Requirements (MERs)

The MERs are stated in terms of the values of certain management objects in 2.7.1 and 2.7.2. Additional MERs are contained in 2.7.3 and 2.7.4. These objects are abstractions used to represent the options for the SDE entity. These MERs do not mean that the objects shall be managed remotely. The effect of setting the object to a particular value shall affect the protocol state as described previously in Clause 2. When constrained to the values specified in the following two subclauses and combined with transmission and reception processing, these objects delineate the minimally compliant protocol state machine.

2.7.1 Station objects

- a) Station_Clear_Hdr: Boolean
SDE entities shall allow the Station_Clear_Hdr to be TRUE. Entities with Station_Clear_Hdr set to TRUE are not interoperable with stations that have Station_Clear_Hdr set to FALSE.
- b) Station_MDF: Boolean
All entities shall allow the Station_MDF to be FALSE. Entities may support TRUE, but then values for each individual security association are determined by system and/or key management. If Station_Clear_Hdr is set to FALSE, then Station_MDF shall also be set to FALSE.

2.7.2 Security association objects

- a) Assoc_MDF: Boolean
This attribute is TRUE if the MDF will be used on the security association. Any party in the negotiation can force the MDF not to be used. The protocol processing shall not depend on the presence of the MDF in any implementation. Each entity shall have the capability of communicating with this attribute set to FALSE. If TRUE is supported, the entity shall have the capability of supporting an integral length (in octets) from zero to 20.
- b) Protection Set: Includes Confid and Integ Booleans
An entity shall be capable of operating with at least one security association having a TRUE value in at least one of these two Booleans. Entities implementing only Integrity, or only Confidentiality, shall be considered conformant.
- c) Padding_pres: Boolean
The Pad field is mandatory only if either the integrity or confidentiality algorithm requires padding. Thus, some entities may support this object only being TRUE, and others may support it only set to FALSE. Still others may support both. If the TRUE value is supported, the entity shall be able to accept a maximum length of Pad (256 including Pad Length field).¹⁵ Negotiation of the

¹⁵The maximum Pad length must be specified due to its effect on stream processing and buffer sizes. It cannot be restricted to the block-size of the Integrity or Confidentiality algorithm since this would defeat the objective of algorithm independence and require conformance testing to be tied to a particular cryptographic algorithm.

Padding_pres by key management and/or system management may allow the value to be set to FALSE where neither cryptographic algorithm requires padding.

d) ID_pres: Boolean

A device shall be capable of supporting ID_pres=FALSE.

2.7.3 SAID requirements

All entities shall support the reception of bootstrap, group, and individual SAIDs. In systems with key management appearing on the User Stack, the SDE entity associates the bootstrap SAID with the appropriate stack identified by the SDE SAP in the SMIB. If no security association is found for the SAID, the PDU is discarded and the SDE LM is notified.

2.7.4 Security services

Compliant entities shall support at least the Data Confidentiality Service or the Connectionless Integrity Service.

- a) To claim that the entity provides the service of Data Confidentiality, the entity shall allow Confid to be TRUE. The strength of this service is dependent upon the confidentiality algorithm used.
- b) To claim that the entity provides the service of Connectionless Integrity, the entity shall allow Integ to be TRUE. The strength of this service is dependent upon the integrity algorithm used. The entity shall be able to send and receive PDUs with ICVs.

2.8 SDE sublayer management

2.8.1 Overview

This clause specifies the managed objects that permit the operation of the SDE to be remotely operated, managed, and maintained. Both fully specified managed objects and partially specified managed objects together with their contained management information are documented.

2.8.2 Scope

This standard provides specifications for ISO/IEC 10165-style managed object classes that represent SDE sublayer resources that are subject to management. These specifications define managed object classes, attribute types, specific attributes, actions, and notification types in accordance with ISO/IEC 10165-4: 1992 (GDMO) and the generic definitions contained in ISO/IEC 10165-2: 1992 (DMI). This standard also follows the procedures and uses the managed objects defined in IEEE Std 802.1F-1993.

This standard provides the following two types of management information to the developers of SDE sublayer management services:

- a) Definition of the managed object classes required for management of the SDE protocol; including their relationships with other managed objects within the Data Link layer and the bindings that are required in the naming of an instantiation of the management service, and;
- b) Definition of common management information such as ATTRIBUTES, PACKAGES, BEHAVIOURS, NOTIFICATIONS, and encodings of information that are used in managing the exchange of data in accordance with SDE specifications.

These managed object classes allow a manager (or management application processes) to monitor and control resources, represented as managed objects, through local agents in other (managed) systems. Event reports (notifications) may be returned from resources in other systems through their local agents to a designated manager or managers.

2.8.3 Definitions

2.8.3.1 LAN/MAN Management definitions

The SDE sublayer management subclause makes use of the following terms defined in ISO/IEC 15802-2: 1995 and ISO/IEC 7498-1: 1994:

- a) LAN/MAN Management

2.8.3.2 Common Definitions and Procedures for IEEE 802 Management Information definitions

The SDE sublayer management subclause makes use of the following terms defined in the text of IEEE Std 802.1F-1993:

- a) MACAddress
- b) ResourceTypeID

2.8.3.3 Management Framework definitions

The SDE sublayer management subclause makes use of the following terms defined in ISO/IEC 7498-4: 1989:

- a) managed object
- b) management information base
- c) systems management

2.8.3.4 Abstract Syntax Notation One (ASN.1) definitions

The SDE sublayer management subclause makes use of the following terms defined in ISO/IEC 8824: 1990:

- a) object identifier
- b) type

2.8.3.5 Common Management Information Service (CMIS) definitions

The SDE sublayer management subclause makes use of the following terms defined in ISO/IEC 9595: 1991:

- a) attribute (of managed object)
- b) Common Management Information Services

2.8.3.6 Guidelines for the Definition of Managed Objects (GDMO) definitions

The SDE sublayer management subclause makes use of the following terms defined in ISO/IEC 10165-4: 1992:

- a) managed object class definition
- b) template

2.8.3.7 Systems Management Overview definitions

The SDE sublayer management subclause makes use of the following terms defined in ISO/IEC 10040: 1992:

- a) agent
- b) agent role
- c) generic definitions
- d) layer management protocol
- e) managed object class
- f) managed (open) system
- g) management information
- h) manager
- i) manager role
- j) notification
- k) notification type
- l) (systems management) operation
- m) systems management application protocol

2.8.3.8 Structure of Management Information (SMI) Information Model definitions

The SDE sublayer management subclause makes use of the following terms defined in ISO/IEC 10165-1: 1993:

- a) abstract datatype
- b) attribute type
- c) attribute value assertion
- d) behaviour
- e) containment
- f) containment hierarchy
- g) distinguished name
- h) inheritance
- i) inheritance hierarchy
- j) name binding
- k) naming tree
- l) mandatory package
- m) (conditional) package
- n) relative distinguished name
- o) subclass
- p) subordinate object
- q) superclass
- r) superior object
- s) unrestricted abstract datatype

2.8.4 Management model

This standard describes the management of the SDE sublayer in terms of a general model of resource management within an open systems environment. Two major components of this management model are a *managing system* and a *managed system*.

Within the managing system (manager role), management processes invoke management operations that are translated into management messages, which are sent to the managed system. A managed system (agent role) provides an interface to those internal resources that are to be managed and processes the applicable management (operations) messages.

The internal resources of the managed system are represented at the interface by abstractions known as *managed objects*. Each managed object responds to a defined set of management operations with internal actions and notifications that the managed system translates into messages. These messages are sent to the manage-