INTERNATIONAL STANDARD

ISO/IEC/ IEEE 8802-1X

First edition
2013-12-01

Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks —

Part 1X: Port-based network access control

Technologies de l'information — Télécommunications et échange d'information entre systèmes — Réseaux locaux et métropolitains —

Partie 1X: Contrôle d'accès au réseau basé sur le port

Reference number
ISO/IEC/IEEE 8802-1X:2013(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56
CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

IEC Central Office
3, rue de Varembé
CH-1211 Geneva 20
Switzerland
E-mail inmail@iec.ch
Web www.iec.ch

Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York
NY 10016-5997, USA
E-mail stds.ipr@ieee.org
Web www.ieee.org

Published in Switzerland

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information contained in its standards.

The main task of ISO/IEC JTC 1 is to prepare International Standards. Draft International Standards adopted by the joint technical committee are circulated to national bodies for voting. Publication as an International Standard requires approval by at least 75 % of the national bodies casting a vote.

Attention is called to the possibility that implementation of this standard may require the 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. ISO/IEEE is not responsible for identifying essential patents or patent claims for which a license may be required, for conducting inquiries into the legal validity or scope of patents or patent claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance or a Patent Statement and Licensing Declaration Form, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from ISO or the IEEE Standards Association.

ISO/IEC/IEEE 8802-1X was prepared by the LAN/MAN Standards Committee of the IEEE Computer Society (as IEEE Std 802.1X-2010). It was adopted by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*, in parallel with its approval by the ISO/IEC national bodies, under the “fast-track procedure” defined in the Partner Standards Development Organization cooperation agreement between ISO and IEEE. IEEE is responsible for the maintenance of this document with participation and input from ISO/IEC national bodies.

ISO/IEC/IEEE 8802 consists of the following parts, under the general title *Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks*:

— *Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*

— *Part 1X: Port-based network access control*

— *Part 1AE: Media access control (MAC) security*

— *Part 15-4: Wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (WPANs)*

(Blank page)

IEEE Standard for

Local and metropolitan area networks—

Port-Based Network Access Control

802.1X™

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

IEEE
3 Park Avenue
New York, NY 10016-5997, USA

5 February 2010

IEEE Std 802.1X™-2010
(Revision of
IEEE Std 802.1X-2004)

(Blank page)

IEEE Std 802.1X™-2010
(Revision of
IEEE Std 802.1X-2004)

IEEE Standard for
Local and metropolitan area networks—

Port-Based Network Access Control

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 2 February 2010

IEEE-SA Standards Board

Abstract: Port-based network access control allows a network administrator to restrict the use of IEEE 802® LAN service access points (ports) to secure communication between authenticated and authorized devices. This standard specifies a common architecture, functional elements, and protocols that support mutual authentication between the clients of ports attached to the same LAN and that secure communication between the ports, including the media access method independent protocols that are used to discover and establish the security associations used by IEEE 802.1AE™ MAC Security.

Keywords: access control, authentication, authorization, controlled port, key agreement, LANs, local area networks, MAC security, MAC Service, MANs, metropolitan area networks, port-based network access control, secure association, security, service access point, uncontrolled port

The Institute of Electrical and Electronics Engineers, Inc.
3 Park Avenue, New York, NY 10016-5997, USA

PDF: ISBN 978-0-7381-6145-7 STD96008
Print: ISBN 978-0-7381-6146-4 STDPD96008

IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. The IEEE develops its standards through a consensus development process, approved by the American National Standards Institute, which brings together volunteers representing varied viewpoints and interests to achieve the final product. Volunteers are not necessarily members of the Institute and serve without compensation. While the IEEE administers the process and establishes rules to promote fairness in the consensus development process, the IEEE does not independently evaluate, test, or verify the accuracy of any of the information or the soundness of any judgments contained in its standards.

Use of an IEEE Standard is wholly voluntary. The IEEE disclaims liability for any personal injury, property or other damage, of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, or reliance upon this, or any other IEEE Standard document.

The IEEE does not warrant or represent the accuracy or content of the material contained herein, and expressly disclaims any express or implied warranty, including any implied warranty of merchantability or fitness for a specific purpose, or that the use of the material contained herein is free from patent infringement. IEEE Standards documents are supplied **"AS IS."**

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, or every ten years for stabilization. When a document is more than five years old and has not been reaffirmed, or more than ten years old and has not been stabilized, 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.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon the advice of a competent professional in determining the exercise of reasonable care in any given circumstances.

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 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. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE.At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE. 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. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required.

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

Secretary, IEEE-SA Standards Board
445 Hoes Lane
Piscataway, NJ 08854
USA

Introduction

This introduction is not part of IEEE Std 802.1X-2010, IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control.

Port-based network access control allows a network administrator to restrict the use of IEEE 802 LAN service access points (ports) to secure communication between authenticated and authorized devices. IEEE Std 802.1X specifies an architecture, functional elements, and protocols that support mutual authentication between the clients of ports attached to the same LAN and secure communication between the ports.

The first edition of IEEE Std 802.1X was published in 2001. The second edition, IEEE Std 802.1X-2004, clarified areas related to mutual authentication and the interface between IEEE 802.1X specified state machine, and those specified by the Extensible Authentication Protocol (EAP), and by IEEE Std 802.11™ in support of IEEE Std 802.1X.

Work on this edition, IEEE Std 802.1X-2010, began as IEEE P802.1af™—an amendment to specify authenticated key agreement in support of IEEE 802.1AE MAC Security. Part of that work clarified and generalized the relationship between the common architecture specified for port-based network access control, and the functional elements and protocols that support that architecture as specified in IEEE Std 802.1X, other IEEE 802 Standards, and in IETF RFCs. The extent of the changes necessary to IEEE Std 802.1X-2004 made it appropriate to revise IEEE Std 802.1X as a whole. Further changes updated the standard to reflect best current practice, insisting, for example, upon mutual authentication methods and using such methods in examples. A greater emphasis is placed on the security of systems accessing the network, as well as upon the security of the network accessed, and some prior provisions, such as the ‘controlled directions’ parameters, have been removed and replaced with a more comprehensive treatment of segregating and limiting connectivity to unauthenticated systems.

Every effort has been made to maintain interoperability, without prior configuration, with implementations conforming to IEEE Std 802.1X-2004 and IEEE Std 802.1X-2001. However it is anticipated that claims of conformance in respect of some existing implementations will continue to refer to IEEE Std 802.1X-2004. Changes to the functionality provided by that prior edition and its documentation include those detailed in the following paragraph.

This edition, IEEE Std 802.1X-2010, describes applications of port-based network access that use IEEE 802.1AE MAC Security (MACsec) and/or MKA (MACsec Key Agreement protocol) as well as those previously supported. The specification of the use of EAP for authentication has been updated, enforcing a stricter separation between the port access control protocol (PACP), local to the Supplicant and Authenticator, and the EAP state machines proper. Details of particular EAP methods are no longer interpreted by the PACP machines. The existing EAPOL (EAP over LANs) PDU formats have not been modified, but additional EAPOL PDUs have been added to support MKA and the specification of EAPOL improved. The bibliography, previously Annex F, has been moved to Annex B. The discussions previously in Annex B and Annex C have been updated and integrated into the main body of the standard. The state machine diagram and language conventions, now used by a number of clauses in the standard, have been moved to a new Annex C.

Notice to users

Laws and regulations

Users of these documents should consult all applicable laws and regulations. Compliance with the provisions of this standard does not imply compliance to any applicable regulatory requirements.

Implementers of the standard are responsible for observing or referring to the applicable regulatory requirements. IEEE does not, by the publication of its standards, intend to urge action that is not in compliance with applicable laws, and these documents may not be construed as doing so.

Copyrights

This document is copyrighted by the IEEE. It is made available for a wide variety of both public and private uses. These include both use, by reference, in laws and regulations, and use in private self-regulation, standardization, and the promotion of engineering practices and methods. By making this document available for use and adoption by public authorities and private users, the IEEE does not waive any rights in copyright to this document.

Updating of IEEE documents

Users of IEEE standards should be aware that these documents may be superseded at any time by the issuance of new editions or may be amended from time to time through the issuance of amendments, corrigenda, or errata. An official IEEE document at any point in time consists of the current edition of the document together with any amendments, corrigenda, or errata then in effect. In order to determine whether a given document is the current edition and whether it has been amended through the issuance of amendments, corrigenda, or errata, visit the IEEE Standards Association website at http://ieeexplore.ieee.org/xpl/standards.jsp, or contact the IEEE at the address listed previously.

For more information about the IEEE Standards Association or the IEEE standards development process, visit the IEEE-SA website at http://standards.ieee.org.

Errata

Errata, if any, for this and all other standards can be accessed at the following URL: http://standards.ieee.org/reading/ieee/updates/errata/index.html. Users are encouraged to check this URL for errata periodically.

Interpretations

Current interpretations can be accessed at the following URL: http://standards.ieee.org/reading/ieee/interp/index.html.

Patents

Attention is called to the possibility that implementation of this amendment may require use of subject matter covered by patent rights. By publication of this amendment, no position is taken with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this amendment are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Contents

Figures

Tables

IEEE Standard for
Local and metropolitan area networks—

Port-Based Network Access Control

1. Overview

1.1 Scope

For the purpose of providing compatible authentication, authorization, and cryptographic key agreement mechanisms to support secure communication between devices connected by IEEE 802® Local Area Networks (LANs), this standard

a) Specifies a general method for provision of port-based network access control.

b) Specifies protocols that establish secure associations for IEEE Std 802.1AE™ MAC Security.

c) Facilitates the use of industry standard authentication and authorization protocols.

1.2 Purpose

IEEE 802 LANs are deployed in networks that convey or provide access to critical data, that support mission critical applications, or that charge for service. Protocols that configure, manage, and regulate access to these networks and network-based services and applications typically run over the networks themselves. Port-based network access control regulates access to the network, guarding against transmission and reception by unidentified or unauthorized parties, and consequent network disruption, theft of service, or data loss.

1.3 Introduction

The stations attached to an IEEE 802 LAN transmit and receive data frames using the service provided by the IEEE 802 LAN MAC at a service access point, often referred to as a port, within each end station or bridge. Port-based network access control specifies a common architecture comprising cooperative functional elements and protocols that

a) Use the service provided by the LAN MAC, at a common service access point, to support a Controlled Port that provides secure access-controlled communication and an Uncontrolled Port that supports protocols that initiate the secure communication or do not require protection.
b) Support mutual authentication between a Port Access Entity (PAE) associated with a Controlled Port, and a peer PAE associated with a peer port in a LAN attached station that desires to communicate through the Controlled Port.
c) Secure the communication between the Controlled Port and the authenticated peer port, excluding other devices attached to or eavesdropping on the LAN.
d) Provide the Controlled Port with attributes that specify access controls appropriate to the authorization accorded to the peer station or its user.

This standard specifies the use of EAP, the Extensible Authentication Protocol (IETF RFC 3748 [B14][1]), to support authentication using a centrally administered Authentication Server and defines EAP encapsulation over LANs (EAPOL, Clause 11) to convey the necessary exchanges between peer PAEs attached to a LAN.

Where communication over the LAN connecting a Controlled Port to its peer(s) is physically secure, no additional protocol is required to protect their communication. This mode of operation is supported by this standard. More commonly intrusion into the LAN communication is a principal security threat, and the result of mutual authentication is not simply Controlled Port authorization to transmit and receive data, but secure distribution of master keys and associated data to the communicating peers. Proof of possession of master keys subsequently serves as proof of mutual authentication in key agreement protocols. These protocols generate keys that are used to cryptographically protect data frames transmitted and received by the Controlled Port. IEEE Std 802.11™ Wireless LANs specifies protocols that associate wireless stations with access points and initiate mutual authentication using the procedures specified in this standard, the subsequent generation of keys to protect data transfer, and the cryptographic methods that protect data frames using those keys. IEEE Std 802.1AE MAC Security (MACsec) specifies cryptographic support of the Controlled Port for other media access methods. Authenticated key agreement for MAC Security, as specified in this standard, specifies the generation of the Secure Association Keys (SAKs) used by MACsec.

Use of the Controlled Port can be restricted by access controls bound to the results of authentication and distributed via AAA protocols such as Diameter (IETF RFC 3588 [B13]) or RADIUS (IETF RFC 2865 [B8]). Attributes supporting certain port-based network access control scenarios are described in IETF RFC 3580, IETF RFC 4675, and IETF RFC 4849.

Clause 7 illustrates use of the above components and protocols in typical network access control scenarios.

1.4 Provisions of this standard

The scope (1.1) of this standard is addressed by detailed specification of the following:

a) The principles of port-based network access control operation, identifying the protocol components that compose a port-based network access control implementation (Clause 6).

[1]The numbers in brackets correspond to those of the bibliography in Annex B.

b) A PAE component, that supports authentication, authorization, and the key agreement functionality required by IEEE Std 802.1AE to allow a MAC Security Entity (SecY) to protect communication through a port (6.3, Clause 12).

c) A Port Access Controller (PAC) component, that controls communication where the attached LAN is deemed to be physically secure and provides point-to-point connectivity (6.4).

d) The key hierarchy used by the PAE and SecY (6.2).

e) The use of EAP by PAEs to support authentication and authorization using a centrally administered Authentication or AAA Server (Clause 8).

f) An encapsulation format, EAPOL, that allows EAP Messages and other protocol exchanges to support authentication and key agreement to be carried directly by a LAN MAC service (Clause 11).

g) A MAC Security Key Agreement protocol (MKA) that the PAE uses to discover associations and agree the keys used by a SecY (Clause 9).

h) An EAPOL Announcement protocol that allows a PAE to indicate the availability of network services, helping other PAEs to choose appropriate credentials and parameters for authentication and network access (Clause 10).

i) Requirements for management of port-based access control, identifying the managed objects and defining the management operations for PAEs (12.9).

j) SMIv2 MIB objects that can be used with SNMPv3 to manage PAEs (Clause 13).

The use of port-based network access control in a number of applications is described (Clause 7) to illustrate the use of these components and the requirements taken into account in their specification. To facilitate migration to this standard, Annex G (informative) uses the same concepts to describe the architectural modeling of unsecured multi-access LANs, a widely deployed form of authenticated port-based network access control that does not meet the security requirements of this standard. Administrative connectivity to unauthenticated devices, as required for use of industry standard ‘Wake-on-LAN’ (WoL) protocols, is described for the scenarios of Clause 7; Annex F (informative) provides background information on WoL.

This standard defines conformance requirements (Clause 5) for the implementation of the following:

k) Port Access Entities (PAEs)

l) Port Access Controllers (PACs)

Annex A provides PICS (Protocol Implementation Conformance Statement) Proformas for completion by suppliers of implementations that are claimed to conform to this standard.

The basic architectural concepts, such as ‘port’, that this standard relies on are reviewed in Annex D.

This standard uses and selects options provided by EAP and AAA protocol specifications, but does not modify those specifications (see Clause 2 for references). Annex E (informative) provides EAP and RADIUS usage guidelines.

The specification and conformance requirements for association discovery and key agreement for IEEE 802.11 Wireless LANs are outside the scope of this standard (see IEEE Std 802.11). That standard makes use of the PAE specified by this standard.

2. Normative references

The following referenced documents are indispensable for the application of this document (i.e., they must be understood and used, so each referenced document is cited in text and its relationship to this document is explained). For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments or corrigenda) applies.

IEEE Std 802.1D™, IEEE Standard for Local and Metropolitan Area Networks: Media access control (MAC) Bridges.[2, 3]

IEEE Std 802.1Q™, IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks.

IEEE Std 802.1AB™, IEEE Standard for Local and Metropolitan Area Networks: Station and Media Access Control Connectivity and Discovery.

IEEE Std 802.1ad™-2005, IEEE Standard for Local and Metropolitan Area Networks: Virtual Bridged Local Area Networks—Amendment 4: Provider Bridges.

IEEE Std 802.1AE™-2006, IEEE Standard for Local and Metropolitan Area Networks: Media Access Control (MAC) Security.

IEEE Std 802.1AX™, IEEE Standard for Local and Metropolitan Area Networks: Link Aggregation.

IEEE Std 802.2™, 1998 Edition [ISO/IEC 8802-2: 1998], Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 2: Logical link control.[4]

IEEE Std 802.3™, IEEE Standard for Information technology—Local and metropolitan area networks—Part 3: Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

IEEE Std 802.11™, IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.

IEEE Std 802.17™-2004 IEEE Standard for Information Technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 17: Resilient packet ring (RPR) access method and physical layer specifications.

IEEE Std 802.1AR™, IEEE Standard for Local and Metropolitan Area Networks: Secure Device Identifier.

IETF RFC 2578, STD 58, Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2), McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., Waldbusser, S., April 1999.[5]

---

[2]IEEE publications are available from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA. IEEE publications can be ordered on-line from the IEEE Standards Website: http://www.standards.ieee.org.

[3]The IEEE standards or products referred to in this clause are trademarks of the Institute of Electrical and Electronics Engineers, Inc.

[4]ISO [IEEE] and ISO/IEC [IEEE] documents are available from ISO Central Secretariat, 1 rue de Varembé, Case Postale 56, CH-1211, Genève 20, Switzerland/Suisse; and from the Institute of Electrical and Electronics Engineers, 445 Hoes Lane, Piscataway, NJ 08854, USA. ISO [IEEE] and ISO/IEC [IEEE] documents can be ordered on-line from the IEEE Standards Website: http://www.standards.ieee.org.

[5]IETF RFCs are available from the Internet Engineering Task Force website at http://www.ietf.org/rfc.html.

IETF RFC 2579, STD 58, Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2), McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., Waldbusser, S., April 1999.

IETF RFC 2580, STD 58, Conformance Statements for SMIv2, McCloghrie, K., Perkins, D., Schoenwaelder, J., Case, J., Rose, M., Waldbusser, S., April 1999.

IETF RFC 2863, The Interfaces Group MIB using SMIv2, McCloghrie, K. and Kastenholz, F., June 2000.

IETF RFC 2869, RADIUS Extensions, Rigney, C., Willats, W., and Calhoun, P., June 2000.

IETF RFC 3394, Advanced Encryption Standard (AES) Key Wrap Algorithm, J. Schaad, R. Housley, September 2002.

IETF RFC 3410, Introduction and Applicability Statements for Internet Standard Management Framework, J. Case, R. Mundy, D. Partain, B. Stewart, December 2002.

IETF RFC 3579, RADIUS (Remote Authentication Dial In User Service) Support For Extensible Authentication Protocol (EAP), Aboba, B., Calhoun, P., September 2003.

IETF RFC 3580, IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Guidelines, Congdon, P., Aboba, B., Smith, A., Zorn, G., Roese, J., September 2003.

IETF RFC 3629, STD 63, UTF-8, a transformation format of ISO 10646, Yergeau, F., November 2003.

IETF RFC 4017, Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs, Stanley, D., Walker, J., Aboba, B., March 2005.

IETF RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.1, Diercks, T., Rescorla, E., April 2006.

IETF RFC 4675, RADIUS Attributes for Virtual LAN and Priority Support, Congdon, P., Sanchez, M., Aboba, B., September 2006.

IETF RFC 5216, The EAP-TLS Authentication Protocol, Simon, D., Aboba, B., Hurst, R., March 2008.

IETF RFC 5247, Extensible Authentication Protocol (EAP) Key Management Framework, Aboba, B., Simon, D., Eronen, P., October 2007.

FIPS Publication 197, The Advanced Encryption Standard (AES), U.S. DoC/NIST, November 26, 2001.

NIST Federal Information Processing Standard 140-2, Security Requirements for Cryptographic Modules[6], 3 December 2002.NIST Special Publication 800-38B, Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Morris Dworkin, May 2005.[7]

NIST Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, E. Barker, J. Kelsey, revised March 2007.

NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions, Lily Chen, November 2008.

[6]National Institute of Standards and Technology, FIPS 140-2 is available at http://www.nist.gov/cmvp.

[7]NIST Special Publications (800 Series) are available at http://csrc.nist.gov/publications/PubsSPs.html.