INTERNATIONAL STANDARD

ISO/ IEC/IEEE 8802-1X

Second edition
2021-12

Telecommunications and exchange between information technology systems — Requirements for local and metropolitan area networks —

Part 1X: Port-based network access control

Télécommunications et échange entre systèmes informatiques — Exigences pour les réseaux locaux et métropolitains —

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

Reference number
ISO/IEC/IEEE 8802-1X:2021(E)

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

Email: stds.ipr@ieee.org
Website: 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.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular, the different approval criteria needed for the different types of ISO/IEC documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives or www.iec.ch/members_experts/refdocs).

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.

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents) or the IEC list of patent declarations received (see patents.iec.ch).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation of the voluntary nature of standards, the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT), see www.iso.org/iso/foreword.html. In the IEC, see www.iec.ch/understanding-standards.

ISO/IEC/IEEE 8802-1X was prepared by the LAN/MAN of the IEEE Computer Society (as [IEEE Std 802.1X™-2020) and drafted in accordance with its editorial rules. It was adopted, under the "fast-track procedure" defined in the Partner Standards Development Organization cooperation agreement between ISO and IEEE, by Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 6, *Telecommunications and information exchange between systems*.

This second edition cancels and replaces the first edition (ISO/IEC/IEEE 8802-1X:2013), which has been technically revised. It also incorporates the Amendments ISO/IEC/IEEE 8802-1X:2013/Amd 1:2016 and ISO/IEC/IEEE 8802-1X:2013/Amd 2:2020.

A list of all parts in the ISO/IEC/IEEE 8802 series can be found on the ISO and IEC websites.

Any feedback or questions on this document should be directed to the user's national standards body. A complete listing of these bodies can be found at www.iso.org/members.html and www.iec.ch/national-committees.

IEEE Std 802.1X™-2020
(Revision of IEEE Std 802.1X™-2010
Incorporating IEEE Std 802.1Xbx™-2014
and IEEE Std 802.1Xck™-2018)

IEEE Standard for Local and Metropolitan Area Networks—

Port-Based Network Access Control

Developed by the

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

Approved 30 January 2020

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, EAP, EAPOL, IEEE 802.1X, key agreement, LANs, local area networks, MACsec, MACsec Key Agreeement, MAC security, MAC Service, MANs, metropolitan area networks, MKA, 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 978-1-5044-6440-6 STD24052
Print: ISBN 978-1-5044-6441-3 STDPD24052

Important Notices and Disclaimers Concerning IEEE Standards Documents

IEEE documents are made available for use subject to important notices and legal disclaimers. These notices and disclaimers, or a reference to this page, appear in all standards and may be found under the heading "Important Notices and Disclaimers Concerning IEEE Standards Documents." They can also be obtained on request from the IEEE or viewed at https://standards.ieee.org/ipr/disclaimers.html.

Notice and Disclaimer of Liability Concerning the Use of IEEE Standards Documents

IEEE Standards documents (standards, recommended practices, and guides), both full-use and trial-use, are developed within IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association ("IEEE SA") Standards Board. IEEE ("the Institute") develops its standards through a consensus development process, approved by the American National Standards Institute ("ANSI"), which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE Standards are documents developed through scientific, academic, and industry-based technical working groups. Volunteers in IEEE working groups are not necessarily members of the Institute and participate without compensation from IEEE. While IEEE administers the process and establishes rules to promote fairness in the consensus development process, 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.

IEEE Standards do not guarantee or ensure safety, security, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers and users of IEEE Standards documents are responsible for determining and complying with all appropriate safety, security, environmental, health, and interference protection practices and all applicable laws and regulations.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, and expressly disclaims all warranties (express, implied and statutory) not included in this or any other document relating to the standard, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; and quality, accuracy, effectiveness, currency, or completeness of material. In addition, IEEE disclaims any and all conditions relating to: results; and workmanlike effort. IEEE standards documents are supplied "AS IS" and "WITH ALL FAULTS."

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.

In publishing and making its standards available, IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity nor is IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing any IEEE Standards document, should rely upon his or her own independent judgment in the exercise of reasonable care in any given circumstances or, as appropriate, seek the advice of a competent professional in determining the appropriateness of a given IEEE standard.

IN NO EVENT SHALL IEEE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE PUBLICATION, USE OF, OR RELIANCE UPON ANY STANDARD, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Translations

The IEEE consensus development process involves the review of documents in English only. In the event that an IEEE standard is translated, only the English version published by IEEE should be considered the approved IEEE standard.

Official statements

A statement, written or oral, that is not processed in accordance with the IEEE SA Standards Board Operations Manual shall not be considered or inferred to be the official position of IEEE or any of its committees and shall not be considered to be, or be relied upon as, a formal position of 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 of IEEE.

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE. However, IEEE does not provide consulting information or advice pertaining to IEEE Standards documents. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Since IEEE standards represent a consensus of concerned interests, it is important that any responses to comments and questions also receive 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 comments or questions except in those cases where the matter has previously been addressed. For the same reason, IEEE does not respond to interpretation requests. Any person who would like to participate in revisions to an IEEE standard is welcome to join the relevant IEEE working group.

Comments on standards should be submitted to the following address:

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

Laws and regulations

Users of IEEE Standards documents should consult all applicable laws and regulations. Compliance with the provisions of any IEEE Standards document 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

Photocopies

Updating of IEEE Standards documents

Users of IEEE Standards documents 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.

Every IEEE standard is subjected to review at least every ten years. When a document is more than ten years old and has not undergone a revision process, 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 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 SA Website at http://ieeexplore.ieee.org/browse/standards/collection/ieee or contact IEEE at the address listed previously. For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website at http://standards.ieee.org.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website at the following URL: http://standards.ieee.org/findstds/errata/index.html. Users are encouraged to check this URL for errata periodically.

Patents

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 by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE SA Website at http://standards.ieee.org/about/sasb/patcom/patents.html. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. 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 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 the IEEE Standards Association.

Participants

At the time this standard was submitted to the IEEE SA Standards Board for approval, the IEEE 802.1 working group had the following membership:

Glenn Parsons, *Chair*
John Messenger, *Vice Chair*
Mick Seaman, *Security Task Group Chair, Editor*

Astrit Ademaj
Ralf Assmann
Jens Bierschenk
Christian Boiger
Paul Bottorff
Radhakrishna Canchi
Feng Chen
Weiying Cheng
Paul Congdon
Rodney Cummings
Josef Dorr
Hesham Elbakoury
Thomas Enzinger
János Farkas
Donald Fedyk
Norman Finn
Geoffrey Garner
Craig Gunther
Marina Gutierrez
Stephen Haddock
Mark Hantel
Marc Holness
Satoko Itaya
Yoshihiro Ito
Michael Karl
Stephan Kehrer
Randy Kelsey
Hajime Koto
James Lawlis
Christophe Mangin
Scott Mansfield
Kenichi Maruhashi
David McCall
Larry McMillan
Tero Mustala
Roy Myers
Hiroki Nakano
Bob Noseworthy
Tomoki Ohsawa
Hiroshi Ohue
Donald R. Pannell
Michael Potts
Dieter Proell
Wei Qiu
Karen Randall
Maximilian Riegel
Jessy V. Rouyer
Atsushi Sato
Frank Schewe
Maik Seewald
Johannes Specht
Marius Stanica
Guenter Steindl
Karim Traore
Hao Wang
Xinyuan Wang
Tongtong Wang
Ludwig Winkel
Karl Weber
Brian Weis
Jordon Woods
Nader Zein
Takahiro Yamaura
Helge Zinner
William Zhao
Harald Zweck

The following members of the individual balloting committee voted on this standard. Balloters may have voted for approval, disapproval, or abstention.

Thomas Alexander
Johann Amsenga
Butch Anton
Harry Bims
Kenneth Bow
Rich Boyer
Nancy Bravin
Vern Brethour
Matthew Brown
Demetrio Bucaneg, Jr.
William Byrd
Radhakrishna Canchi
Paul Cardinal
Juan Carreon
Janos Farkas
Avraham Freedman
Devon Gayle
Tim Godfrey
Zhigang Gong
Randall Groves
Marek Hajduczenia
Marco Hernandez
Werner Hoelzl
Yasuhiro Hyakutake
Raj Jain
SangKwon Jeong
Pranav Jha
Lokesh Kabra
Srinivas Kandala
Piotr Karocki
Stuart Kerry
Evgeny Khorov
Yongbum Kim
Hyeong Ho Lee
Suzanne Leicht
James Lepp
Michael Lynch
John Mackay
Jouni Malinen
Roger Marks
Arthur Marris
Stephen McCann
Brett Mcclellan
Richard Mellitz
Michael Montemurro
Nick S.A. Nikjoo
Satoshi Obara
Robert O'Hara
Carlos Pardo
Bansi Patel
Arumugam Paventhan
David Piehler
Walter Pienciak
Clinton Powell
Karen Randall
R. K. Rannow
Maximilian Riegel
Robert Robinson
Jessy Rouyer
John Sargent
Frank Schewe
Michael Seaman
Thomas Starai
Walter Struppler
Michael Thompson
Mark-Rene Uchida
Alexander Umnov
Dmitri Varsanofiev
George Vlantis
Lisa Ward
Stephen Webb
Brian Weis
Scott Willy
Chun Yu Charles Wong
Oren Yuen

When the IEEE SA Standards Board approved this standard on 30 January 2020, it had the following membership:

Gary Hoffman, *Chair*
Vacant, *Vice-Chair*
Jean-Philippe Faure, *Past Chair*
Konstantinos Karachalios, *Secretary*

Ted Burse
Doug Edwards
Travis Griffith
Grace Gu
Guido Hiertz
John Kulick
David J. Law
Joseph L.Koepfinger*
Howard Li
Dong Liu
Kevin Lu
Paul Nikolich
Damir Novosel
Jon Rosdahl
Dorothy Stanley
Mehmet Ulema
Lei Wang
Sha Wei
Philip Winston
Daidi Zhong

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 802.1X™-2020, IEEE Standard for Local and Metropolitan Area Networks—Port-Based Network Access Control.

This edition of IEEE Std 802.1X™ incorporates IEEE Std 802.1X-2010 and its amendments, IEEE Std 802.1Xbx-2014 and IEEE Std 802.1Xck-2018.

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

The third edition, IEEE Std 802.1X-2010, added authenticated key agreement in support of IEEE Std 802.1AE™ MAC Security (MACsec) and 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 IETF RFCs. Further changes updated the standard to reflect best current practice, insisting, for example, on mutual authentication methods and using such methods in examples. A greater emphasis was placed on the security of systems accessing the network, as well as on the security of the network accessed, with a more comprehensive treatment of segregating and limiting connectivity to unauthenticated systems. Applications of port-based network access that use MACsec and/or MACsec Key Agreement protocol (MKA) were described.

IEEE Std 802.1X-2010 included a number of improvements to the specification of the port access control protocol (PACP) state machines and their relationship to EAP methods and state machines. Systems conformant to IEEE Std 802.1X-2020 or IEEE Std 802.1X-2010 should interoperate, 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 with respect to some existing implementations, not needing to support IEEE Std 802.1AE and already conforming to best current practice as of 2010, will continue to refer to IEEE Std 802.1X-2004.

The first amendment to IEEE Std 802.1X-2010, IEEE Std 802.1Xbx-2014, extended MKA to further support and use the extended packet numbering Cipher Suites specified by the IEEE Std 802.1AEbw™-2013. Secure connectivity association (CA) members can temporarily suspend MKA operation without causing protocol timeouts that would disrupt secure data transfer, thus allowing in-service control plane software upgrades.

The second amendment to IEEE Std 802.1X-2010, IEEE Std 802.1Xck-2018, specified a YANG data model for configuration and status reporting, using the information model previously specified in this standard.

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 6733 [B25]) or RADIUS (IETF RFC 2865 [B6]). Attributes supporting certain port-based network access control scenarios are described in IETF RFC 3580 [B13], IETF RFC 4675 [B17], IETF RFC 4849 [B18], IETF RFC 7268 [B28], and IETF RFC 8044 [B29].

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).

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).

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

j) SMIv2 MIB objects that can be used with SNMPv3 to manage PAEs (Clause 13).
k) YANG configuration and operational state models for PAE and PAE System components (Clause 14).

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 F (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 E (informative) provides background information on WoL.

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

l) Port Access Entities (PAEs)
m) 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', on which this standard relies are reviewed in IEEE Std 802.1AC.

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 D (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.

DMTF, Alert Standard Format (ASF) Specification, Version 2.0, 23 April 2003.[2]

iana-if-type YANG Module, Internet Assigned Numbers Authority.[3]

IEEE Std 802®, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture.[4, 5]

IEEE Std 802d™, IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture Amendment 1: Allocation of Uniform Resource Name (URN) Values in IEEE 802 Standards.

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

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

IEEE Std 802.1AC™, IEEE Standard for Local and metropolitan area networks—Media Access Control (MAC) Service Definition.

IEEE Std 802.1AE™, 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.[6]

IEEE Std 802.3™, IEEE Standard for Ethernet.

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 802.1AR™, 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., and Waldbusser, S., April 1999.[7]

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., and Waldbusser, S., April 1999.

[2]DMTF publications are available from the DMTF at https://www.dmtf.org.

[3] Available at https://www.iana.org/assignments/iana-if-type/iana-if-type.xhtml.

[4] IEEE publications are available from The Institute of Electrical and Electronics Engineers https://standards.ieee.org.

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

[6] ISO and ISO/IEC documents are available from the International Organization of Standardization (http://www.iso.org) and from the International Electrotechnical Commission (http://www.iec.ch). These documents are also available from the American National Standards Institute (http://ansi.org).

[7]IETF RFCs are available from the Internet Engineering Task Force website at https://www.ietf.org.

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

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

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

IETF RFC 3418, STD 62, Management Information Base (MIB) for the Simple Network Management Protocol (SNMP), Preshun, R., Case, J., McCloghrie, K., Rose, M., Waldbusser, S., December 2002.

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

IETF RFC 4346, The Transport Layer Security (TLS) Protocol Version 1.3, Diercks, T., Rescorla, E., April 2006.

IETF RFC 4493, The AES-CMAC Algorithm, Song, J.H., Lee, J., and Iwata, T., June 2006.

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

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

IETF RFC 7170, Tunnel Extensible Authentication Protocol (TEAP) Version 1, Zhou, H., Cam-Winget, N., Salowey, J., and Hanna, S., May 2014.

IETF RFC 7317, A YANG Data Model for System Management, Bierman A., and Bjorklund M., August 2014.

IETF RFC 7950, The YANG 1.1 Data Modeling Language, Bjorklund, M., editor., August 2016.

IETF RFC 8343, A YANG Data Model for Interface Management, Bjorklund, M., March 2018.

IETF RFC 8446, The Transport Layer Security (TLS) Protocol Version 1.3, Rescorla, E., August 2018.

ISO/IEC 18033-3: 2010, Information technology—Security techniques—Encryption algorithms—Part 3:Block ciphers.

NIST Special Publication 800-108, Recommendation for Key Derivation Using Pseudorandom Functions, Lily Chen, October 2009.[8]

[8] NIST Special Publication FIPS 800-108 is available at https://csrc.nist.gov/publications/detail/sp/800-108/final.