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

Part 1X:

Port-based network access control

**AMENDMENT 1: MAC security key
agreement protocol (MKA) extensions**

[ISO/IEC/IEEE 8802-1X:2013/Amd 1:2016](https://standards.iteh.ai/catalog/standards/sist/0a26d00d-56e9-4ddf-ab62-7b9da7cee70a/iso-iec-8802-1x-2013-amd-1-2016)

<https://standards.iteh.ai/catalog/standards/sist/0a26d00d-56e9-4ddf-ab62-7b9da7cee70a/iso-iec-8802-1x-2013-amd-1-2016>

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

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

*AMENDEMENT 1: Extensions du protocole d'accord de clés de
sécurité MAC*



PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat, the IEC Central Office and IEEE do not accept any liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies and IEEE members. In the unlikely event that a problem relating to it is found, please inform the ISO Central Secretariat or IEEE at the address given below.

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC/IEEE 8802-1X:2013/Amd 1:2016](https://standards.iteh.ai/catalog/standards/sist/0a26d00d-56e9-4ddf-ab62-7b9da7cee70a/iso-iec-ieee-8802-1x-2013-amd-1-2016)

<https://standards.iteh.ai/catalog/standards/sist/0a26d00d-56e9-4ddf-ab62-7b9da7cee70a/iso-iec-ieee-8802-1x-2013-amd-1-2016>



COPYRIGHT PROTECTED DOCUMENT

© IEEE 2014

All rights reserved. Unless otherwise specified, no part of this publication may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm, without permission in writing from ISO, IEC or IEEE at the respective address below.

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 Varembe
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.

Amendment 1 to ISO/IEC/IEEE 8802-1X:2013 was prepared by the LAN/MAN of the IEEE Computer Society (as IEEE 802.1Xbx-2014). 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.

iTeh STANDARD PREVIEW
(blank page)
(standards.iteh.ai)

ISO/IEC/IEEE 8802-1X:2013/Amd 1:2016
<https://standards.iteh.ai/catalog/standards/sist/0a26d00d-56e9-4ddf-ab62-7b9da7cee70a/iso-iec-ieee-8802-1x-2013-amd-1-2016>

IEEE Standard for
Local and metropolitan area networks—

Port-Based Network Access Control

Amendment 1: MAC Security Key Agreement
Protocol (MKA) Extensions

iTeh STANDARD PREVIEW
(standards.iteh.ai)

[ISO/IEC/IEEE 8802-1X:2013/Amd 1:2016](https://standards.iteh.ai/catalog/standards/sist/0a26d00d-56e9-4ddf-ab62-7b9da7cee70a/iso-iec-ieee-8802-1x-2013-amd-1-2016)

IEEE Computer Society

<https://standards.iteh.ai/catalog/standards/sist/0a26d00d-56e9-4ddf-ab62-7b9da7cee70a/iso-iec-ieee-8802-1x-2013-amd-1-2016>

Sponsored by the
LAN/MAN Standards Committee

iTeh STANDARD PREVIEW

(standards.iteh.ai)

ISO/IEC/IEEE 8802-1X:2013/Amd 1:2016

<https://standards.iteh.ai/catalog/standards/sist/0a26d00d-56e9-4ddf-ab62-7b9da7cee70a/iso-iec-ieee-8802-1x-2013-amd-1-2016>

IEEE Std 802.1Xbx™-2014

(Amendment to
IEEE Std 802.1X™-2010)

**IEEE Standard for
Local and metropolitan area networks—**

Port-Based Network Access Control

**Amendment 1: MAC Security Key Agreement
Protocol (MKA) Extensions**

iTeh STANDARD PREVIEW

Sponsor

(standards.iteh.ai)

LAN/MAN Standards Committee

of the

IEEE Computer Society

[ISO/IEC/IEEE 8802-1X:2013/Amd 1:2016](https://standards.iteh.ai/catalog/standards/sist/0a26d00d-56e9-4ddf-ab62-7b9da7cee70a/iso-iec-ieee-8802-1x-2013-amd-1-2016)

<https://standards.iteh.ai/catalog/standards/sist/0a26d00d-56e9-4ddf-ab62-7b9da7cee70a/iso-iec-ieee-8802-1x-2013-amd-1-2016>

Approved 10 December 2014

IEEE-SA Standards Board

Abstract: Media Access Control security (MACsec) Key Agreement protocol (MKA) data elements and procedures that provide additional security and manageability capabilities, including the ability to maintain secure communication while the operation of MKA is suspended, when used in conjunction with MACsec Cipher Suites that support Extended Packet Numbering are added in this amendment.

Keywords: authorized port, confidentiality, data origin authenticity, IEEE 802.1X™, IEEE 802.1Xbx™, integrity, LANs, local area networks, MAC Bridges, MAC security, MAC Service, MANs, metropolitan area networks, port based network access control, secure association, security, transparent bridging

iTeh STANDARD PREVIEW (standards.iteh.ai)

[ISO/IEC/IEEE 8802-1X:2013/Amd 1:2016](https://standards.iteh.ai/catalog/standards/sist/0a26d00d-56e9-4ddf-ab62-7b9da7cee70a/iso-iec-ieee-8802-1x-2013-amd-1-2016)

<https://standards.iteh.ai/catalog/standards/sist/0a26d00d-56e9-4ddf-ab62-7b9da7cee70a/iso-iec-ieee-8802-1x-2013-amd-1-2016>

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

Copyright © 2014 by The Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 22 December 2014. Printed in the United States of America.

IEEE and 802 are registered trademarks in the U.S. Patent & Trademark Office, owned by The Institute of Electrical and Electronics Engineers, Incorporated.

PDF: ISBN 978-0-7381-9435-6 STD20045
Print: ISBN 978-0-7381-9436-3 STDPD20045

IEEE prohibits discrimination, harassment and bullying. For more information, visit <http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html>.
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.

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 Notice” or “Important Notices and Disclaimers Concerning IEEE Standards Documents.”

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. Volunteers 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 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

IEEE draft and approved standards are copyrighted by IEEE under U.S. and international copyright laws. They are made available by IEEE and are adopted 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 these documents available for use and adoption by public authorities and private users, IEEE does not waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate fee, IEEE will grant users a limited, non-exclusive license to photocopy portions of any individual standard for company or organizational internal use or individual, non-commercial use only. To arrange for payment of licensing fees, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

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/xpl/standards.jsp> 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>.

ISO/IEC/IEEE 8802-1X:2013/Amd 1:2016

Errata

<https://standards.ieht.ai/catalog/standards/sist/0a26d00d-56e9-4ddf-ab62-7b9da7cee70a/iso-iec-ieee-8802-1x-2013-amd-1-2016>

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 amendment 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*

Ting Ao	Hitoshi Hayakawa	Karen Randall
Christian Boiger	Jeremy Hitt	Maximilian Riegel
Paul Bottorff	Rahil Hussain	Dan Romascanu
David Chen	Tony Jeffree	Jessy V. Rouyer
Feng Chen	Michael Johas Teener	Panagiotis Saltsidis
Weiyang Cheng	Peter Jones	Behcet Sarikaya
Diego Crupnicoff	Hal Keen	Daniel Sexton
Rodney Cummings	Marcel Kiessling	Johannes Specht
Patrick Diamond	Yongbum Kim	Kevin B. Stanton
Aboubacar Kader Diarra	Philippe Klein	Wilfried Steiner
Janos Farkas	Jouni Korhonen	Vahid Tabatabaee
Norman Finn	Jeff Lynch	Patricia Thaler
Geoffrey Garner	Ben Mack-Crane	Jeremy Touve
Anoop Ghanwani	Christophe Mangin	Karl Weber
Mark Gravel	James McIntosh	Yuehua Wei
Eric W. Gray	Eric Multanen	Brian Weis
Craig Gunther	Donald Pannell	Jordon Woods
Stephen Haddock		Juan-Carlos Zuniga

iTeh STANDARD PREVIEW
 (standards.iteh.ai)

ISO/IEC/IEEE 8802-1X:2013/Amd 1:2016

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

Thomas Alexander	Tony Jeffree	Satoshi Obara
Butch Anton	Peter Jones	Satoshi Oyama
Olugbenga Ayinde	Shinkyō Kaku	Karen Randall
William Byrd	Piotr Karocki	Maximilian Riegel
Juan Carreon	Stuart Kerry	Jessy V. Rouyer
Keith Chow	Max Kicherer	Mick Seaman
Charles Cook	Jeff Koftinoff	Kapil Sood
Grazia Delia	Bruce Kraemer	Thomas Starai
Sourav Dutta	Yasushi Kudoh	Rene Struik
Richard Edgar	Thomas Kurihara	Walter Struppler
Yukihiro Fujimoto	Paul Lambert	Joseph Tardo
Devon Gayle	Hyeong Ho Lee	William Taylor
Gregory Gillooly	Shen Loh	Patricia Thaler
Randall Groves	Elvis Maculuba	Dmitri Varsanofiev
Michael Gundlach	Jouni Malinen	Hung-Yu Wei
Werner Hoelzl	Michael Newman	Brian Weis
Atsushi Ito	Nick S.A. Nikjoo	Oren Yuen
		Daidi Zhong

When the IEEE-SA Standards Board approved this amendment on 10 December 2014, it had the following membership:

John Kulick, *Chair*
Jon Walter Rosdahl, *Vice Chair*
Richard H. Hulett, *Past Chair*
Konstantinos Karachalios, *Secretary*

Peter Balma
 Farooq Bari
 Ted Burse
 Clint Chaplain
 Stephen Dukes
 Jean-Phillippe Faure
 Gary Hoffman

Michael Janezic
 Jeffrey Katz
 Joseph L. Koepfinger*
 David J. Law
 Hung Ling
 Oleg Logvinov
 Ted Olsen
 Glenn Parsons

Ron Peterson
 Adrian Stephens
 Peter Sutherland
 Yatin Trivedi
 Phil Winston
 Don Wright
 Yu Yuan

*Member Emeritus

Also included are the following nonvoting IEEE-SA Standards Board liaisons:

Richard DeBlasio, *DOE Representative*
 Michael Janezic, *NIST Representative*

iTeh STANDARD PREVIEW
 (standards.iteh.ai)

Catherine Berger
IEEE-SA Content Production and Management
 Kathryn Bennett
Program Manager, IEEE-SA Technical Program Operations

<https://standards.iteh.ai/catalog/standards/sist/0a26d00d-56e9-4ddf-ab62-7b9da7cee70a/iso-iec-ieee-8802-1x-2013-amd-1-2016>

Introduction

This introduction is not part of IEEE Std 802.1XTM-2014, IEEE Standard for Local and metropolitan area networks—Port-Based Network Access Control—Amendment 1: MAC Security Key Agreement Protocol (MKA) Extensions.

This first amendment to IEEE Std 802.1X-2010, extends MKA to realize additional security and manageability capabilities made possible by the IEEE Std 802.1AETM amendment that added extended packet numbering Cipher Suites to IEEE Std 802.1AETM-2006. Secure connectivity association (CA) members can now temporarily suspend MKA operation without causing protocol timeouts that would disrupt secure data transfer, thus allowing in-service control plane software upgrades.

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 802.11TM in support of IEEE Std 802.1X.

The third edition, IEEE Std 802.1X-2010, added authenticated key agreement in support of IEEE Std 802.1AETM MAC Security, clarifying and generalizing 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. 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 was placed on the security of systems accessing the network, as well as upon the security of the network accessed, and some prior provisions, with a more comprehensive treatment of segregating and limiting connectivity to unauthenticated systems. Applications of port-based network access that use IEEE Std 802.1AE MAC Security (MACsec) and/or MKA (MACsec Key Agreement protocol) are described.

Every effort was made to ensure that systems conformant to IEEE Std 802.1X-2010 will 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 in respect of 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. IEEE Std 802.1X-2010 includes 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.

Contents

2. Normative references	2
3. Definitions	5
4. Abbreviations and acronyms	6
5. Conformance	7
5.11 MKA options	7
6. Principles of port-based network access control operation	8
6.2 Key hierarchy	8
7. Port-based network access control applications	9
9. MACsec Key Agreement protocol (MKA)	10
9.1 Protocol design requirements	10
9.5 Key server election	14
9.8 SAK generation, distribution, and selection	16
9.15 MKA participant timer values	17
9.16 MKA management	17
9.18 In-service upgrades	18
9.19 In-service upgrade examples	22
11. EAPOL PDUs	26
11.5 EAPOL protocol version handling	26
11.11 EAPOL-MKA	26
12. PAE operation	32
12.1 Model of operation	32
12.2 KaY interfaces	32
12.5 Logon Process	33
12.9 PAE management	34
13. PAE MIB	36
13.4 Security considerations	36
13.5 Definitions for PAE MIB	36
Annex A (normative) PICS Proforma	85
A.9 MKA requirements and options	85
Annex B (informative) Bibliography	86
Annex H (informative) Test vectors	88
H.1 KDF	88
H.2 CAK Key Derivation	89
H.3 CKN Derivation	89
H.4 KEK Derivation	90