

IEEE Standard for
Local and metropolitan area networks—

Part 21: Media Independent Handover Services

Amendment 1: Security Extensions to Media Independent Handover Services and Protocol

IEEE Computer Society

Sponsored by the
LAN/MAN Standards Committee

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

IEEE Std 802.21a™-2012
(Amendment to
IEEE Std 802.21™-2008)

3 May 2012

IEEE Std 802.21a™-2012
(Amendment to
IEEE Std 802.21™-2008)

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

Part 21: Media Independent Handover Services

Amendment 1: Security Extensions to Media Independent Handover Services and Protocol

Sponsor

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 29 March 2012

IEEE-SA Standards Board

Abstract: Extensions to IEEE Std 802.21-2008 are provided for security mechanisms to protect media independent handover services and mechanisms to use MIH to assist proactive authentication to reduce the latency due to media access authentication and key establishment with the target network.

Keywords: IEEE 802.21, IEEE 802.21a, proactive authentication, service access authentication, security protection

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

Copyright © 2012 by the Institute of Electrical and Electronics Engineers, Inc.
All rights reserved. Published 3 May 2012. 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 978-0-7381-7257-6 STD97232
Print: ISBN 978-0-7381-7363-4 STDPD97232

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.

Notice and Disclaimer of Liability Concerning the Use of IEEE Documents: IEEE Standards documents are developed within the IEEE Societies and the Standards Coordinating Committees of the IEEE Standards Association (IEEE-SA) Standards Board. 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 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.

Use of an IEEE Standard is wholly voluntary. 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 any IEEE Standard document.

IEEE does not warrant or represent the accuracy or content of the material contained in its standards, 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 in its standards 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 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 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.

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 the official position of IEEE or any of its committees and shall not be considered to be, nor 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 to ensure 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. Any person who would like to participate in evaluating comments or revisions to an IEEE standard is welcome to join the relevant IEEE working group at <http://standards.ieee.org/develop/wg/>.

Comments on standards should be submitted to the following address:

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

Photocopies: Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +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.

Notice to users

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

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 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. 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](http://standards.ieee.org) 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](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/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 <<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 for approval, the IEEE 802.21 Working Group had the following officers:

Subir Das, *Chair*
Juan Carlos Zuniga, *Vice-chair*
David Cypher, *Technical Editor*
H. Anthony Chan, *Secretary*

At the time this amendment was submitted to sponsor ballot, Security in Media Independent Handover task group had the following officers:

Yoshihiro Ohba, *Chair*
Lidong Chen, *Technical Editor*

When the IEEE 802.21 Working Group approved this amendment, the Working Group had the following membership:

Yoon Young An	Hongseok Jeon	Yoshihiro Ohba
Clint Chaplin	Lee Jin	Changmin Park
Lidong Chen	Farrokh Khatibi	Hyundo Park
H. Anthony Chan	Dapeng Liu	Charlie Perkins
Subir Das	Michael Lynch	Ajay Rajkumar
Antonio De la Oliva Delgado	Roger B. Marks	Karen Randall
Peretz Feder	Paul Nikolich	Stephen Shellhammer
Junghoon Jee	Christian Niephaus	Albert Vidal
		Juan Carlos Zuniga

Major contributions were recieved from the following individuals:

Fernando Bernal-Hidalgo
Ashutosh Dutta
Toshikazu Kodama
Rafael Marin-Lopez

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

George Babut	Shinkyo Kaku	Robert Robinson
Nancy Bravin	Stuart Kerry	Benjamin Rolfe
William Byrd	Farrokh Khatibi	Richard Roy
Radhakrishna Canchi	Brian Kiernan	Randall Safier
Anthony Chan	Yongbum Kim	Peter Saunderson
Clint Chaplin	Bruce Kraemer	Bartien Sayogo
Keith Chow	Joseph Kwak	John Short
Charles Cook	Paul Lambert	Gil Shultz
Subir Das	Jan-Ray Liao	Kapil Sood
Antonio De la Oliva Delgado	Greg Luri	Thomas Starai
Thomas Dineen	Michael Lynch	Rene Struik
Sourav Dutta	Elvis Maculuba	Walter Struppler
Richard Edgar	Wayne Manges	Jun Ichi Takada
Pieter-Paul Giesberts	Roger B. Marks	Steven Tilden
Reinhard Gloger	Gary Michel	Mark-Rene Uchida
Ron Greenthaler	Ronald Murias	Dmitri Varsanofiev
Randall Groves	Michael S. Newman	Prabodh Varshney
Michael Gundlach	Yoshihiro Ohba	John Vergis
David Hunter	Satoshi Oyama	Lei Wang
Ichirou Ida	Venkatesha Prasad	Stanley Wang
Noriyuki Ikeuchi	Karen Randall	Hung-Yu Wei
Atsushi Ito	Maximilian Riegel	Oren Yuen
Junghoon Jee		Juan Carlos Zuniga

When the IEEE-SA Standards Board approved this standard on 29 March 2012, it had the following membership:

Richard H. Hulett, *Chair*
John Kulick, *Vice Chair*
Robert M. Grow, *Past Chair*
Judith Gorman, *Secretary*

Satish Aggarwal	Alexander Gelman	Oleg Logvinov
Masayuki Ariyoshi	Paul Houzé	Ted Olsen
Peter Balma	Jim Hughes	Gary Robinson
William Bartley	Young Kyun Kim	Jon Walter Rosdahl
Ted Burse	Joseph L. Koepfinger*	Mike Seavey
Clint Chaplin	David J. Law	Yatin Trivedi
Wael Diab	Thomas Lee	Phil Winston
Jean-Philippe Faure	Hung Ling	Yu Yuan

*Member Emeritus

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

Richard DeBlasio, DOE Representative
Michael Janezic, NIST Representative

Michelle Turner
IEEE Standards Senior Program Manager, Document Development

Lisa Perry
IEEE Standards Program Manager, Technical Program Development

Introduction

This introduction is not part of IEEE Std 802.21-2012, IEEE Standard for Local and metropolitan area networks—Part 21: Media Independent Handover Service—Amendment 1: Security Extensions to Media Independent Handover Services and Protocol.

This amendment specifies the extensions to IEEE Std 802.21-2008 for security mechanisms to protect media independent handover services and mechanisms to use Media Independent Handover (MIH) to assist proactive authentications to reduce the latency due to media access authentication and key establishment with the target network.

Contents

1.	Overview.....	2
1.3	General.....	2
2.	Normative references.....	2
3.	Definitions.....	3
4.	Abbreviations and acronyms.....	5
5.	General architecture.....	5
5.1	Introduction.....	5
5.1.9	Proactive authentication and key establishment.....	5
6.	MIH service.....	6
6.2	Service management.....	6
6.2.1	General.....	6
6.2.2	Service management primitives.....	6
6.5	Media independent event service.....	6
6.5.4	Information elements.....	6
7.	Service access point (SAP) and primitives.....	7
7.4	MIH_SAP primitives.....	7
7.4.1	MIH_Capability_Discover.....	7
7.4.1.1	MIH_Capability_Discover.request.....	7
7.4.1.1.2	Semantics of service primitives.....	7
7.4.1.2	MIH_Capability_Discover.indication.....	7
7.4.1.2.2	Semantics of service primitive.....	7
7.4.1.3	MIH_Capability_Discover.response.....	8
7.4.1.3.2	Semantics of service primitive.....	8
7.4.1.4	MIH_Capability_Discover.confirm.....	8
7.4.1.4.2	Semantics of service primitive.....	8
7.4.17	MIH_Net_HO_Candidate_Query.....	9
7.4.17.2	MIH_Net_HO_Candidate_Query.request.....	9
7.4.17.2.2	Semantics of service primitive.....	9
7.4.17.3	MIH_Net_HO_Candidate_Query.indication.....	9
7.4.17.3.2	Semantics of service primitive.....	9
7.4.17.4	MIH_Net_HO_Candidate_Query.response.....	10
7.4.17.4.1	Function.....	10
7.4.17.4.2	Semantics of service primitive.....	10
7.4.17.5	MIH_Net_HO_Candidate_Query.confirm.....	10
7.4.17.5.2	Semantics of service primitive.....	10
7.4.18	MIH_MN_HO_Candidate_Query.....	11
7.4.18.1	MIH_MN_HO_Candidate_Query.request.....	11
7.4.18.1.2	Semantics of service primitive.....	11
7.4.18.2	MIH_MN_HO_Candidate_Query.indication.....	11
7.4.18.2.2	Semantics of service primitive.....	11
7.4.18.3	MIH_MN_HO_Candidate_Query.response.....	12

7.4.18.3.2	Semantics of service primitive	12
7.4.18.4	MIH_MN_HO_Candidate_Query.confirm	12
7.4.18.4.2	Semantics of service primitive	12
7.4.27	MIH_Push_Key	13
7.4.27.1	MIH_Push_key.request	13
7.4.27.1.1	Function	13
7.4.27.1.2	Semantics of service primitive	13
7.4.27.1.3	When generated	13
7.4.27.1.4	Effect on receipt	13
7.4.27.2	MIH_Push_key.indication	13
7.4.27.2.1	Function	13
7.4.27.2.2	Semantics of service primitive	14
7.4.27.2.3	When generated	14
7.4.27.2.4	Effect on receipt	14
7.4.27.3	MIH_Push_key.response	14
7.4.27.3.1	Function	14
7.4.27.3.2	Semantics of service primitive	14
7.4.27.3.3	When generated	15
7.4.27.3.4	Effect on receipt	15
7.4.27.4	MIH_Push_Key.confirm	15
7.4.27.4.1	Function	15
7.4.27.4.2	Semantics of service primitive	15
7.4.27.4.3	When generated	15
7.4.27.4.4	Effect on receipt	15
7.4.28	MIH_LL_Auth	15
7.4.28.1	MIH_LL_Auth.request	15
7.4.28.1.1	Function	15
7.4.28.1.2	Semantics of service primitive	16
7.4.28.1.3	When generated	16
7.4.28.1.4	Effect on receipt	16
7.4.28.2	MIH_LL_Auth.indication	16
7.4.28.2.1	Function	16
7.4.28.2.2	Semantics of service primitive	16
7.4.28.2.3	When generated	17
7.4.28.2.4	Effect on receipt	17
7.4.28.3	MIH_LL_Auth.response	17
7.4.28.3.1	Function	17
7.4.28.3.2	Semantics of service primitive	17
7.4.28.3.3	When generated	17
7.4.28.3.4	Effect on receipt	17
7.4.28.4	MIH_LL_Auth.confirm	17
7.4.28.4.1	Function	17
7.4.28.4.2	Semantics of service primitive	18
7.4.28.4.3	When generated	18
7.4.28.4.4	Effect on receipt	18
8.	Media independent handover protocol	19
8.4	MIH protocol frame format	19
8.4.1	General frame format	19
8.4.1a	Protected MIH protocol frame format	20
8.4.1a.1	MIH PDU protected by (D)TLS	20
8.4.1a.2	MIH PDU protected through EAP-generated MIH SA	21
8.4.1a.3	Protected MIH PDU upon transport address change	21

8.4.2	Fragmentation and reassembly	22
8.4.2.1	General	22
8.4.2.2	Fragmentation	23
8.4.2.3	Reassembly	23
8.6	MIH protocol messages	24
8.6.1	MIH messages for service management	24
8.6.1.1	MIH_Capability_Discover request	24
8.6.1.2	MIH_Capability_Discover response	24
8.6.1.11	MIH_Auth indication	25
8.6.1.12	MIH_Auth request	25
8.6.1.13	MIH_Auth response	26
8.6.1.14	MIH_Termination_Auth request	26
8.6.1.15	MIH_Termination_Auth response	27
8.6.1.16	MIH_Push_key request	27
8.6.1.17	MIH_Push_key response	27
8.6.1.18	MIH_LL_Auth request	27
8.6.1.19	MIH_LL_Auth response	28
8.6.3	MIH messages for command service	28
8.6.3.7	MIH_Net_HO_Candidate_Query request	28
8.6.3.8	MIH_Net_HO_Candidate_Query response	29
8.6.3.9	MIH_MN_HO_Candidate_Query request	29
8.6.3.10	MIH_MN_HO_Candidate_Query response	30
9.	MIH protocol protection	31
9.1	Protection established through MIH (D)TLS	31
9.2	Key establishment through an MIH service access authentication	31
9.2.1	MIH service access authentication	32
9.2.2	Key derivation and key hierarchy	38
9.2.3	EAP-generated MIH security association	40
9.2.4	Termination	41
9.3	MIH message protection mechanisms for EAP-generated SAs	41
9.3.1	MIH_Auth message protection	41
9.3.2	MIH PDU protection procedure	42
9.3.3	MIH PDU protection by AES-CCM	43
9.3.3.1	AES-CCM Parameters	44
9.3.3.2	Construct AES-CCM Nonce	44
9.3.3.3	Operational procedures in AES-CCM	44
9.3.3.3.1	Encapsulation	44
9.3.3.3.2	Decapsulation	45
9.3.3.4	Format of security TLV	45
9.3.4	MIH PDU protection by AES in CBC mode and HMAC-SHA1-96	46
9.3.4.1	Initialization vector for AES in CBC mode	46
9.3.4.2	Operational procedures in applying AES CBC and HMAC-SHA1-96	46
9.3.4.2.1	Encapsulation	46
9.3.4.2.2	Decapsulation	46
9.3.4.3	Format of security TLV	47
9.3.5	MIH PDU protection by HMAC-SHA1-96	47
9.3.5.1	MIC generation and verification	47
9.3.5.1.1	MIC generation	47
9.3.5.1.2	MIC verification	47
9.3.5.2	Format of security TLV	47
9.3.6	MIH PDU protection by AES-CMAC	48
9.3.6.1	MIC generation and verification	48

9.3.6.1.1	MIC generation	48
9.3.6.1.2	MIC verification	48
9.3.6.2	Format of security TLV	48
9.4	Common procedures	49
9.4.1	Sending	49
9.4.2	Receiving	49
10.	Proactive authentication.....	50
10.1	Media specific proactive authentication	50
10.1.1	Procedures in a media specific proactive authentication	51
10.1.1.1	PoS and candidate media specific authenticator discovery	51
10.1.1.2	Proactive authentication through EAP or ERP	51
10.1.1.3	Media specific association handshake	51
10.1.2	Proactive authentication message format	51
10.2	Bundling media access authentication with MIH service access authentication	51
10.2.1	Media specific key derivation.....	51
10.2.1.1	Derivation of media specific root key (MSRK).....	51
10.2.1.2	Derivation of media specific pairwise master keys (MSPMKs).....	52
10.2.2	Media specific key distribution.....	53
10.2.2.1	Push key distribution	53
10.2.2.2	Reactive pull key distribution	53
10.2.2.3	Optimized proactive pull key distribution	53
Annex A (informative)	Bibliography	55
Annex D (normative)	Mapping MIH messages to reference points	56
Annex F (normative)	Data type definition	57
Annex G (normative)	Information element identifiers	60
Annex H (normative)	MIIS basic schema	61
Annex J (informative)	IEEE 802.21 MIB.....	63
Annex K (informative)	Example MIH message fragmentation.....	65
Annex L (normative)	MIH protocol message code assignment	68
Annex M (normative)	Protocol implementation conformance statement (PICS) proforma.....	69
Annex N (informative)	Authentication and key distribution procedures	71
Annex O (informative)	Protection through transport protocols.....	77

IEEE Standard for
Local and metropolitan area networks—

Part 21: Media Independent Handover Services

Amendment 1: Security Extensions to Media Independent Handover Services and Protocol

IMPORTANT NOTICE: IEEE Standards documents are not intended to ensure safety, health, or environmental protection, or ensure against interference with or from other devices or networks. Implementers 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.

This IEEE document is made available for use subject to important notices and legal disclaimers. These notices and disclaimers appear in all publications containing this document and may be found under the heading "Important Notice" or "Important Notices and Disclaimers Concerning IEEE Documents." They can also be obtained on request from IEEE or viewed at <http://standards.ieee.org/TPR/disclaimers.html>.

(This amendment specifies enhancements to IEEE Std 802.21™.)

NOTE—The editing instructions are shown in **bold italic**. Four editing instructions are used: change, delete, insert, and replace. **Change** is used to make corrections in existing text or tables. The editing instruction specifies the location of the change and describes what is being changed by using ~~strike through~~ (to remove old material) and underline (to add new material). **Delete** removes existing material. **Insert** adds new material without disturbing the existing material. Insertions may require renumbering. If so, renumbering instructions are given in the editing instruction. **Replace** is used to make changes in figures or equations by removing the existing figure or equation and replacing it with a new one. Editing instructions, change markings, and this NOTE will not be carried over into future editions because the changes will be incorporated into the base standard.¹

¹Notes in text, tables, and figures are given for information only and do not contain requirements needed to implement the standard.

1. Overview

1.3 General

Change the list in 1.3 as follows:

The following items are not within the scope of this standard:

- Intra-technology handover [except for handovers across extended service sets (ESSs) in case of IEEE 802.11]
- Handover policy
- ~~Security mechanisms~~ Media specific protection mechanisms
- Enhancements specific to particular link-layer technologies that are required to support this standard (they will be carried out by those link-layer technology standards)
- Higher layer (layer 3 and above) enhancements that are required to support this standard

2. Normative references

Insert the following normative references into Clause 2 in alphabetical order:

FIPS 198, The Keyed-Hash Message Authentication Code (HMAC).²

IETF RFC 2409 (1998) The Internet Key Exchange (IKE).³

IETF RFC 3748 (2004) Extensible Authentication Protocol (EAP).

IETF RFC 4302 (2005), IP Authentication Header.

IETF RFC 4303 (2005), IP Encapsulating Security Payload.

IETF RFC 4306 (2005), The Internet Key Exchange (IKEv2) Protocol.

IETF RFC 4347 (2006), Datagram Transport Layer Protocol.

IETF RFC 5246 (2008), The Transport Layer Security (TLS) Protocol Version 1.2.

IETF RFC 5296 (2008), EAP Extensions for EAP Re-authentication Protocol (ERP).

NIST SP 800-38A, Recommendation for Block Cipher Modes of Operation.⁴

NIST SP 800-38B, Recommendation for Block Cipher Modes of Operation—The CMAC Mode for Authentication.

NIST SP 800-38C, Recommendation for Block Cipher Modes of Operation—The CCM Mode for Confidentiality and Authentication.

NIST SP 800-108, Recommendation for Key Derivation Using Pseudorandom Functions.

²FIPS publications are made available at: <http://csrc.nist.gov/publications/PubsFIPS.html>.

³IETF RFCs are available from the Internet Engineering Task Force website at <http://www.ietf.org/rfc.html>.

⁴NIST publications are available from the National Institute of Standards and Technology (<http://www.nist.gov/>).

3. Definitions

Insert the following definitions in alphabetically order:

authenticated encryption: An algorithm to convert plaintext data to ciphertext and generate a message authentication code with a cryptographic key as a parameter to provide confidentiality, integrity, and authenticity of the data. *See also:* **encryption**; **MIC algorithm**.

authentication process: A process to assure that the claimed identity belongs to the entity. It is also called entity authentication. In this standard, an access authentication is an entity authentication with the identity used to access a specific network or a media independent handover (MIH) service.

authentication server: A server used for authentication purposes. When EAP is used as an authentication protocol, the authentication server is an EAP server.

authenticator: A network entity to execute EAP with a mobile node called a peer. An authenticator can use a backend server to conduct EAP execution. *Syn:* **EAP authenticator**.

candidate authenticator: An authenticator that is associated with a candidate PoA.

candidate network: A network that is a potential target to the MN's movement

candidate PoS: A potential PoS that can serve the MNs after movement.

decryption: An algorithm to convert ciphertext of data to plaintext with a cryptographic key as a parameter. It is an inverse operation of encryption.

EAP authenticator: *See:* **authenticator**.

EAP peer: The entity that responds to the EAP authenticator.

EAP Re-authentication: An authentication protocol using a key established in a previous EAP execution as defined in IETF RFC 5296.⁵

EAP Server: The entity that terminates the EAP execution with the EAP peer. In the case where no back-end authentication server is used, the EAP server is a part of the EAP authenticator. In the case where a backend authentication server is used, the EAP server is located on the backend authentication server.

encryption: An algorithm to convert plaintext data to ciphertext to provide confidentiality with a cryptographic key as a parameter.

extensible authentication protocol (EAP): An access authentication framework specified in IETF RFC 3748. It can support different authentication methods, called EAP methods.

media specific authentication server: An authentication server used for media specific access authentication.

media specific authenticator: An authenticator used for a media specific network access authentication.

⁵Information on normative references can be found in Clause 2.

media specific network access authentication: An authentication protocol for media access purpose specified for a specific media access. It may establish keys to be used in media specific protection mechanisms.

media specific protection mechanism: A mechanism that is applied to media specific layers to protect the data traffic using an encryption algorithm, an integrity protection algorithm, an authenticated encryption algorithm, or a combination of an encryption algorithm and an integrity protection algorithm.

message authentication code (a.k.a. message integrity code): A data string generated over a message with a symmetric key by an algorithm, called message authentication code algorithm. It is used to verify the integrity of the message and to authenticate the origin of the message.

message authentication code algorithm: An algorithm to generate a message authentication code on a data message with a symmetric key to provide integrity protection and message origination authentication. *See:* **message authentication code.**

message integrity code (MIC): *See:* **message authentication code.**

MIH security association (SA): An MIH security association is a set of cryptographic attributes established between the peer MIH entities for protecting MIH messages at the MIH protocol layer. An MIH SA is established via TLS handshake or EAP execution, where both the TLS handshake and EAP execution take place over the MIH protocol. When an MIH SA is established via TLS handshake, the TLS master key and its child keys, TLS random values and the TLS cipher suite negotiated in the TLS handshake are a part of the MIH SA. When an MIH SA is established via EAP execution, an MSK or rMSK and its child keys, MIH random values and the MIH cipher suite negotiated between the peer MIH entities are associated with the MIH SA.

MIH service access authentication: An authentication process that authorizes the access to media independent services.

MIH service access authentication server: An authentication server used to execute the MIH service access authentication. *See:* **authentication server.**

proactive authentication: A media specific authentication with the candidate network(s) executed prior to a handover to one of the candidate networks.

protection mechanisms for MIH messages: A protection mechanism that is applied to MIH PDU using an encryption algorithm, an integrity protection algorithm, an authenticated encryption algorithm, or a combination of an encryption algorithm and an integrity protection algorithm.

serving authenticator: The authenticator which is associated with the serving PoA.

serving PoS: An MIH PoS that is currently providing the MIH services to the mobile node.

Security association identifier (SAID): An identifier of an MIH security association. When an SA is established through TLS, it is the TLS session ID. When an SA is generated through an EAP execution, it is assigned by the authenticator and the ID value is an octet string unique for a pair of MIH functions.

Change definition 3.17 media independent handover point of service (MIH PoS) as follows:

3.17 media independent handover point of service (MIH PoS): Network-side MIHF instance that exchanges MIH messages with an MN-based MIHF. The same MIH Network Entity includes an MIH PoS for each MIH-enabled mobile node with which it exchanges MIH messages. A single MIH PoS can host more than one MIH service. The same MIH Network Entity can include multiple MIH Points of Service that

can provide different combinations of MIH services to the respective mobile nodes based on subscription or roaming conditions. Note that for a network entity comprising multiple interfaces, the notion of MIH PoS is associated with the network entity itself and not with just one of its interfaces. For MIH service access authentication, a PoS serves as an authenticator. Moreover, when a service access authentication establishes keys for proactive authentication, a PoS provides key distribution service for media specific authenticators.

4. Abbreviations and acronyms

Insert the following abbreviations and acronyms in alphabetical order:

AES	advanced encryption standard
AS	authentication server
CBC	cipher block chaining
CCM	counter with CBC message authentication code
DTLS	datagram transport layer security
EAP	extensible authentication protocol
ERP	EAP Re-authentication Protocol
HMAC	keyed-hash message authentication code
IV	Initialization vector
MIAK	media independent authentication key
MIC	message integrity code
MIEK	media independent encryption key
MIIK	media independent integrity key
MISK	media independent session key
MSA	media specific authenticator
MSK	master session key
MSPMK	media specific pairwise master key
MSRK	media specific root key
PRF	pseudorandom function
rMSK	re-authentication master session key
SA	security association
SAID	security association identifier
SHA	secure hash algorithm
TLS	transport layer security
TLV	Type Length Value (a form of encoding, or an item encoded using that encoding)

5. General architecture

5.1 Introduction

Insert new 5.1.9 after 5.1.8 as follows:

5.1.9 Proactive authentication and key establishment

This standard provides mechanisms for a mobile node to conduct a proactive authentication and key establishment with the candidate authenticator(s) and PoA(s). The proactive authentication is conducted through media specific network access authentication where authentication messages are exchanged between authentication end-points via a PoS. The MIH protocol is used for encapsulating the authentication messages between the MN and the PoS. A successful proactive authentication and key establishment allow a PoA in the target network to obtain a key(s) to protect the communication link between the mobile node and the PoA after the handover.

6. MIH service

6.2 Service management

6.2.1 General

Change list after first paragraph as follows:

Prior to providing the MIH services from one MIHF to another, the MIH entities need to be configured properly. This is done through the following service management functions:

- MIH capability discovery
- MIH registration
- MIH service access authentication
- MIH event subscription

6.2.2 Service management primitives

Insert new rows after last row in Table 3 as follows:

Table 3—Service management primitives

Service management parameters	(L)ocal (R)emote	Defined in	Comments
MIH_Push_Key	L, R	7.4.27	Install a key in a remote PoA
MIH_LL_Auth	L, R	7.4.28	Carry out a proactive authentication over MIH between the MN and the PoS using link layer frames.

6.5 Media independent event service

6.5.4 Information elements

Insert information elements in Table 10 as follows:

Table 10—Information elements

Name of information elements	Description	Data type
PoA-specific information elements		
IE_AUTHENTICATOR_LINK_ADDR	An L2 address of the authenticator, which serves the PoA	LINK_ADDR
PoA-specific higher layer service information elements		
IE_AUTHENTICATOR_IP_ADDR	The IP address of the authenticator, which serves the PoA.	IP_ADDR
IE_PoS_IP_ADDR	PoS's IP address.	IP_ADDR

7. Service access point (SAP) and primitives

7.4 MIH_SAP primitives

7.4.1 MIH_Capability_Discover

7.4.1.1 MIH_Capability_Discover.request

7.4.1.1.2 Semantics of service primitives

Change text as follows:

```
MIH_Capability_Discover.request (
    DestinationIdentifier,
    LinkAddressList,
    SupportedMihEventList,
    SupportedMihCommandList,
    SupportedIsQueryTypeList,
    SupportedTransportList,
    MBBHandoverSupport,
    SupportedSecurityCapList
)
```

Insert the following parameters:

Parameters:

Name	Data type	Description
SupportedSecurityCapList	MIH_SEC_CAP	(Optional) List of supported MIH security capabilities on the local MIHF.

7.4.1.2 MIH_Capability_Discover.indication

7.4.1.2.2 Semantics of service primitive

Change text as follows:

```
MIH_Capability_Discover.indication (
    SourceIdentifier,
    LinkAddressList,
    SupportedMihEventList,
    SupportedMihCommandList,
    SupportedIsQueryTypeList,
    SupportedTransportList,
    MBBHandoverSupport,
    SupportedSecurityCapList
)
```

Insert the following parameters:

Parameters:

Name	Data type	Description
SupportedSecurityCapList	MIH_SEC_CAP	(Optional) List of supported MIH security capabilities on the remote MIHF.

7.4.1.3 MIH_Capability_Discover.response

7.4.1.3.2 Semantics of service primitive

Change text as follows:

```
MIH_Capability_Discover.response(
    DestinationIdentifier,
    Status,
    LinkAddressList,
    SupportedMihEventList,
    SupportedMihCommandList,
    SupportedIsQueryTypeList,
    SupportedTransportList,
    MBBHandoverSupport,
    SupportedSecurityCapList
)
```

Insert the following parameters:

Parameters:

Name	Data type	Description
SupportedSecurityCapList	MIH_SEC_CAP	(Optional) List of supported MIH security capabilities on the local MIHF.

7.4.1.4 MIH_Capability_Discover.confirm

7.4.1.4.2 Semantics of service primitive

Change text as follows:

```
MIH_Capability_Discover.confirm(
    SourceIdentifier,
    Status,
    LinkAddressList,
    SupportedMihEventList,
    SupportedMihCommandList,
    SupportedIsQueryTypeList,
    SupportedTransportList,
    MBBHandoverSupport,
    SupportedSecurityCapList
)
```

Insert the following parameters:

Parameters:

Name	Data type	Description
SupportedSecurityCapList	MIH_SEC_CAP	(Optional) List of supported MIH security capabilities on the remote MIHF.

7.4.17 MIH_Net_HO_Candidate_Query

7.4.17.2 MIH_Net_HO_Candidate_Query.request

7.4.17.2.2 Semantics of service primitive

Change the following text as follows:

```
MIH_Net_HO_Candidate.Query.request (
    DestinationIdentifier,
    SuggestedNewLinkList,
    SuggestedCandidateAuthenticatorList,
    QueryResourceReportFlag
)
```

Insert the following parameters:

Parameters

Name	Data type	Description
SuggestedCandidateAuthenticator-List	LIST(LINK_AUTHENTICATOR_LIST)	List of media specific authenticator's addresses for the suggested candidate PoAs.

7.4.17.3 MIH_Net_HO_Candidate_Query.indication

7.4.17.3.2 Semantics of service primitive

Change text as follows:

```
MIH_Net_HO_Candidate.Query.indication (
    SourceIdentifier,
    SuggestedNewLinkList,
    SuggestedCandidateAuthenticatorList,
    QueryResourceReportFlag
)
```

Insert the following parameter:

Parameters

Name	Data type	Description
SuggestedCandidateAuthenticator-List	LIST(LINK_AUTHENTICATOR_LIST)	List of media specific authenticator's addresses for the suggested candidate PoAs.

7.4.17.4 MIH_Net_HO_Candidate_Query.response

7.4.17.4.1 Function

7.4.17.4.2 Semantics of service primitive

Change text as follows:

```
MIH_Net_HO_Candidate_Query.response(
    DestinationIdentifier,
    Status,
    SourceLinkIdentifier,
    HandoverStatus,
    PreferredLinkList,
    PreferredCandidateAuthenticatorList
)
```

Insert the following parameter:

Parameter

Name	Data type	Description
PreferredCandidateAuthenticator-List	LIST(LINK_AUTHENTICATOR_LIST)	List of the corresponding media specific authenticator's addresses for the preferred candidate PoAs.

7.4.17.5 MIH_Net_HO_Candidate_Query.confirm

7.4.17.5.2 Semantics of service primitive

Change text as follows:

```
MIH_Net_HO_Candidate_Query.confirm(
    SourceIdentifier,
    Status,
    SourceLinkIdentifier,
    HandoverStatus,
    PreferredLinkList,
    PreferredCandidateAuthenticatorList
)
```

Insert the following parameter:

Parameter

Name	Data type	Description
PreferredCandidateAuthenticator-List	LIST(LINK_AUTHENTICATOR_LIST)	List of the corresponding media specific authenticator's addresses for the preferred candidate PoAs.

7.4.18 MIH_MN_HO_Candidate_Query

7.4.18.1 MIH_MN_HO_Candidate_Query.request

7.4.18.1.2 Semantics of service primitive

Change the following text as indicated as follows:

```
MIH_MN_HO_Candidate.Query.request(
    DestinationIdentifier,
    SourceLinkIdentifier,
    CandidateLinkList,
    QoSResourceRequirements,
    IPConfigurationMethods,
    DHCPServerAddress,
    FAAddress
    AccessRouteAddress,
    CandidateAuthenticatorList
)
```

Insert the following parameter as follows:

Parameter

Name	Data type	Description
CandidateAuthenticatorList	LIST(LINK_AUTHENTICATOR_LIST)	List of the corresponding media specific authenticator's addresses for the candidate PoAs.

7.4.18.2 MIH_MN_HO_Candidate_Query.indication

7.4.18.2.2 Semantics of service primitive

Change the following text as follows:

```
MIH_MN_HO_Candidate.Query.indication(
    DestinationIdentifier,
    SourceLinkIdentifier,
    CandidateLinkList,
    QoSResourceRequirements,
    IPConfigurationMethods,
    DHCPServerAddress,
```

FAAddress
 AccessRouteAddress,
CandidateAuthenticatorList
)

Insert the following parameter as follows:

Parameter

Name	Data type	Description
CandidateAuthenticatorList	LIST(LINK_AUTHENTICATOR_LIST)	List of the corresponding media specific authenticator's addresses for the candidate PoAs.

7.4.18.3 MIH_MN_HO_Candidate_Query.response

7.4.18.3.2 Semantics of service primitive

Change the following text as follows:

MIH_MN_HO_Candidate_Query.response(
 DestinationIdentifier,
 Status,
 SourceLinkIdentifier,
 HandoverStatus,
 PreferredCandidateLinkList,
 PreferredCandidateAuthenticatorList
)

Insert the following parameter:

Parameter

Name	Data type	Description
PreferredCandidateAuthenticator-List	LIST(LINK_AUTHENTICATOR_LIST)	List of the corresponding media specific authenticator's addresses for the preferred candidate PoAs.

7.4.18.4 MIH_MN_HO_Candidate_Query.confirm

7.4.18.4.2 Semantics of service primitive

Change the following text as follows:

MIH_MN_HO_Candidate_Query.confirm(
 DestinationIdentifier,
 Status,
 SourceLinkIdentifier,
 HandoverStatus,
 PreferredCandidateLinkList,
 PreferredCandidateAuthenticatorList
)

Insert the following parameter:

Parameter

Name	Data type	Description
PreferredCandidateAuthenticator-List	LIST(LINK_AUTHENTICATOR_LIST)	List of the corresponding media specific authenticator's address for the preferred candidate PoAs.

Insert new subclauses (7.4.27 and 7.4.28) as follows:

7.4.27 MIH_Push_Key

7.4.27.1 MIH_Push_key.request

7.4.27.1.1 Function

This primitive is used to request a remote MIHF (PoS) to install a key(s) in a target PoA(s).

7.4.27.1.2 Semantics of service primitive

```
MIH_Push_key.request (
    DestinationIdentifier,
    LinkTupleIdentifierList
)
```

Parameters:

Name	Data type	Description
DestinationIdentifier	MIHF_ID	This identifies a remote MIHF that will be the destination of this request.
LinkTupleIdentifierList	LIST(LINK_TUPLE_ID)	This identifies a list of links of target PoAs for which keys are pushed.

7.4.27.1.3 When generated

This primitive is generated by an MIH user in the MN to request a remote MIHF in the serving PoS to install a key in a target PoA.

7.4.27.1.4 Effect on receipt

The local MIHF shall generate an MIH_Push_Key request message to the remote MIHF.

7.4.27.2 MIH_Push_key.indication

7.4.27.2.1 Function

This primitive is used to pass a key to the corresponding MIH user on the serving PoS.

7.4.27.2.2 Semantics of service primitive

```
MIH_Push_key.indication (
    SourceIdentifier,
    KeyMapping
)
```

Parameters:

Name	Data type	Description
SourceIdentifier	MIHF_ID	This identifies the invoker, which is a remote MIHF.
KeyMapping	KEY_MAPPING	This specifies a mapping of a link identifier for which the key is pushed and a lifetime.

7.4.27.2.3 When generated

This primitive is generated by the local MIHF after receiving an MIH_Push_Key request message from the remote MIHF.

7.4.27.2.4 Effect on receipt

A media specific key is delivered to the corresponding MIH user.

7.4.27.3 MIH_Push_key.response

7.4.27.3.1 Function

This primitive is used to indicate that the key installation request has been received and MIH user has executed it.

7.4.27.3.2 Semantics of service primitive

```
MIH_Push_key.response (
    DestinationIdentifier,
    LinkTupleIdentifierList,
    Status
)
```

Parameters:

Name	Data type	Description
DestinationIdentifier	MIHF_ID	This identifies a remote MIHF that will be the destination of this response.
LinkTupleIdentifierList	LIST(LINK_TUPLE_ID)	This identifies a list of links for which keys are pushed.
Status	STATUS	This represents the operation result.