IEEE SA
STANDARDS ASSOCIATION

STANDARDS

**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

Amendment 1: Operations with Randomized and Changing MAC Addresses

IEEE Computer Society

Developed by the
LAN/ MAN Standards Committee

IEEE Std 802.11bh™-2024
(Amendment to IEEE Std 802.11-2024)

IEEE

IEEE Std 802.11bh™-2024
(Amendment to IEEE Std 802.11™-2024)

**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

Amendment 1: Operation with Randomized and Changing MAC Addresses

Developed by the

LAN/MAN Standards Committee
of the
IEEE Computer Society

Approved 26 September 2024

IEEE SA Standards Board

Abstract: This amendment specifies modifications to the IEEE Std 802.11 medium access control (MAC) sublayer mechanisms to preserve the existing services that might otherwise be restricted in environments where STAs in extended service set (ESS) use randomized or changing MAC addresses, without affecting the privacy of the users corresponding to the STAs. User privacy includes exposure of trackable information to third parties or exposure of an individual's presence of behavior.

This amendment introduces mechanisms to enable session continuity in the absence of unique MAC address-to-STA mapping. For STAs in an ESS that use randomized or changing MAC addresses, this amendment preserves the ability to provide customer support, conduct network diagnostics and troubleshooting, and detect device arrival in a trusted environment.

Keywords: IEEE 802.11™, 802.11bh™, Randomized and Changing MAC Address (RCM)

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

Print: ISBN 979-8-8557-2139-3 STDPD27888
PDF: ISBN 979-8-8557-2138-6 STD27888

Important Notices and Disclaimers Concerning IEEE Standards Documents

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

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

IEEE Standards documents are developed within IEEE Societies and subcommittees of IEEE Standards Association (IEEE SA) Board of Governors. IEEE develops its standards through an accredited consensus development process, which brings together volunteers representing varied viewpoints and interests to achieve the final product. IEEE standards are documents developed by volunteers with scientific, academic, and industry-based expertise in technical working groups. Volunteers are not necessarily members of IEEE or IEEE SA 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 makes no warranties or representations concerning its standards, and expressly disclaims all warranties, express or implied, concerning this standard, including but not limited to the warranties of merchantability, fitness for a particular purpose and non-infringement. IEEE Standards documents do not guarantee safety, security, health, or environmental protection, or guarantee against interference with or from other devices or networks. In addition, IEEE does not warrant or represent that the use of the material contained in its standards is free from patent infringement. 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 their 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: THE NEED TO PROCURE 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 balloting 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 is the approved IEEE standard.

Use by artificial intelligence systems

In no event shall material in any IEEE Standards documents be used for the purpose of creating, training, enhancing, developing, maintaining, or contributing to any artificial intelligence systems without the express, written consent of IEEE SA in advance. "Artificial intelligence" refers to any software, application, or other system that uses artificial intelligence, machine learning, or similar technologies, to analyze, train, process, or generate content. Requests for consent can be submitted using the Contact Us form.

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, 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 the presenter's views should be considered the personal views of that individual rather than the formal position of IEEE, IEEE SA, the Standards Committee, or the Working Group. Statements made by volunteers may not represent the formal position of their employer(s) or affiliation(s).

Comments on standards

Comments for revision of IEEE Standards documents are welcome from any interested party, regardless of membership affiliation with IEEE or IEEE SA. However, **IEEE does not provide interpretations, 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 subcommittees of the IEEE SA Board of Governors 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 evaluating comments or in revisions to an IEEE standard is welcome to join the relevant IEEE working group. You can indicate interest in a working group using the Interests tab in the Manage Profile & Interests area of the IEEE SA myProject system.[1] An IEEE Account is needed to access the application.

Comments on standards should be submitted using the Contact Us form.[2]

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 constitute compliance to any applicable regulatory requirements. Implementers of the standard are responsible for observing or referring to the applicable

[1] Available at: https://development.standards.ieee.org/myproject-web/public/view.html#landing.

[2] Available at: https://standards.ieee.org/content/ieee-standards/en/about/contact/index.html.

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.

Data privacy

Users of IEEE Standards documents should evaluate the standards for considerations of data privacy and data ownership in the context of assessing and using the standards in compliance with applicable laws and regulations.

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, neither IEEE nor its licensors waive any rights in copyright to the documents.

Photocopies

Subject to payment of the appropriate licensing fees, 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; https://www.copyright.com/. 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 10 years. When a document is more than 10 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 IEEE Xplore or contact IEEE.[3] For more information about the IEEE SA or IEEE's standards development process, visit the IEEE SA Website.

Errata

Errata, if any, for all IEEE standards can be accessed on the IEEE SA Website.[4] Search for standard number and year of approval to access the web page of the published standard. Errata links are located under the

[3] Available at: https://ieeexplore.ieee.org/browse/standards/collection/ieee.

[4] Available at: https://standards.ieee.org/standard/index.html.

Additional Resources Details section. Errata are also available in IEEE Xplore. Users are encouraged to periodically check for errata.

Patents

IEEE standards are developed in compliance with the IEEE SA Patent Policy.[5]

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 https://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.

IMPORTANT NOTICE

Technologies, application of technologies, and recommended procedures in various industries evolve over time. The IEEE standards development process allows participants to review developments in industries, technologies, and practices, and to determine what, if any, updates should be made to the IEEE standard. During this evolution, the technologies and recommendations in IEEE standards may be implemented in ways not foreseen during the standard's development. IEEE standards development activities consider research and information presented to the standards development group in developing any safety recommendations. Other information about safety practices, changes in technology or technology implementation, or impact by peripheral systems also may be pertinent to safety considerations during implementation of the standard. 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.

[5] Available at: https://standards.ieee.org/about/sasb/patcom/materials.html.

Participants

At the time this amendment was sent to the IEEE SA Standards Board for approval, the IEEE 802.11 Working Group (WG) had the following officers:

Robert Stacey, *Chair*
Jon Walter Rosdahl, *1st Vice Chair*
Stephen McCann, *2nd Vice Chair*
Volker Jungnickel, *Secretary*

The officers of the WG Task Group bh and the members of the WG ballot group for this amendment are as follows:

Mark Hamilton, *Chair*
Peter Yee, *Vice Chair*
Stephen Orr, *Vice Chair*
Jay Yang, *Secretary*
Carol Ansley, *Technical Editor*

Rana Abdelaal
Shaimaʼ AbidRabbu
Mohamed Abouelseoud
Osama S. Aboulmagd
Abdelrahman Abushattal
Tomoko Adachi
Olubukola Adakeja
Shubhodeep Adhikari
Peyush Agarwal
Sandeep Agrawal
Kosuke Aio
Abdel Karim Ajami
Dmitry Akhmetov
Srividhya Alagarsamy
Amer Al-Baidhani
Carlos Aldana
Sawaira Ali
Song-Haur An
Diego Arlandis
Antonio Arregui
Yusuke Asai
Alfred Asterjadhi
Kwok Shum Au
Oscar Au
Ziv Avital
Matthieu Avrillon
Geert Awater
Azizi Shahrnaz
Badenes Agustin
SunHee Baek
Eugene Baik
Gabor Bajko
Subharthi Banerjee
Dmitry Bankov
Priyanka Bansal
Zhanjing Bao
Stéphane Baron
David Barr
Anuj Batra
Tuncer Baykas
Chris Beg
Jianwei Bei
Yaron Ben Arie
Friedbert Berens
Christian Berger
Shirly Bethapudi
Nehru Bhandaru
Abhijit Bhattacharya
Tong Bian
Harry Bims
Lennert Bober
David Boldy
Veerendra Boodannavan
Daniel Borges
Albert Bredewoud
Frank Burkhardt
Seongho Byeon
Denis Bykov
Ugo Campiglio
Radhakrishna Canchi
Necati Canpolat
Bo Cao
Rui Cao
Laurent Cariou
William Carney
Dave Cavalcanti
Gurkan Cepni
Dongju Cha
Andy Chan
Chen-Yi Chang
Clint F. Chaplin
Abhishek Chaturvedi
Hui Che
Kirill Chemrov
Cheng Chen
Cheng-Ming Chen
Evelyn Chen
Shuqiao Chen
Xiaogang Chen
You-Wei Chen
George Cherian
Giovanni Chisci
Rojan Chitrakar
WenHsien Chiu
Baw Chng
Hangyu Cho
JinHo Choi
Jin Seek Choi
Jinsoo Choi
Seungho Choo
Tzu-Hsuan Chou
Liwen Chu
Jinyoung Chun
Bruce Chung
Chulho Chung
Dana Ciochina
John Coffey
Javier Contreras Albesa
Carlos Cordeiro
Diana Cortes
D.Nelson Costa
Yaoshen Cui
Claudio da Silva
Dibakar Das
Subir Das
Debashis Dash
Leonard Dauphinee
Mike Davis
Hendricus De Ruijter
Rolf J de Vegt
Antonio DeLaOlivaDelgado
Thomas Derham

Patrice Desmoulin
Rocco Di Taranto
Esmail Dinan
Xiandong Dong
Roya Doostnejad
Klaus Doppler
Rui Du
Zhenguo Du
Duan Ruchen
Richard Edgar
Martin Eiger
Alecsander Eitan
Manasi Ekkundi
Ahmed ElSherif
Marc Emmelmann
Vinko Erceg
Serhat Erkucuk
Shuang Fan
Juan Fang
Xuming Fang
Yonggang Fang
Shuling Feng
David Ferruz
Domenico Ficara
Matthew Fischer
Paul Fletcher
Yuki Fujimori
Ming Gan
Trivikram Gangur
Mehdi Ganji
Ning Gao
Lalit Garg
Thomas Gee
Alireza Ghaderipoor
Chittabrata Ghosh
Ravi Gidvani
James Gilb
Tim Godfrey
Bo Gong
Hemamali Gorthi
Fumihide Goto
Niranjan Grandhe
Michael Grigat
Jatin Grover
Jaheon Gu
Junrong Gu
Xiangxin Gu
Romain Guignard
Jing Guo
Yuchen Guo
Zheng Guo
Ziyang Guo
Binita Gupta
Luis Gutierrez
Taeyoung Ha
Muhammad Kumail Haider
David Halasz
Kenza Hamidouche
Jin-Kyu Han
Xiao Han
Thomas Handte
Zhao Hangbin
Christopher Hansen
Daniel Harkins
Edward Harrison
Brian Hart
Mahmoud Hasabelnaby
Victor Hayes
Rong He
Ziming He
Ahmadreza Hedayat
Ahmed Helmy
Sherief Helwa
Jerome Henry
Marco Hernandez
Lili Hervieu
Guido Hiertz
Ryuichi Hirata
Duncan Ho
Hamid Hosseinianfar
Ching-Wen Hsiao
Hung-Tao Hsieh
Chien-Fang Hsu
Ostrovsky Hsu
Yung Lin Hsu
Yungping Hsu
Chunyu Hu
Mengshi Hu
Xiaokun Hu
Chihan Huang
Gaoyong Huang
Guogang Huang
Lei Huang
Po-Kai Huang
Kaikai Huang
Sung Hyun Hwang
Hirohiko Inohiza
Insun Jang
Timothy Jeffries
Elliot Yu Chih Jen
Eunsung Jeon
Chenhe Ji
Feng Jiang
Jinjing Jiang
Wu Jiang
Zhiping Jiang
Hanjin Joh
Toby John
Vincent Knowles Jones IV
Insik Jung
Aniruddh Kabbinale
Ishaque Ashar Kadampot
Carl Kain
Naveen Kakani
Sanket Kalamkar
Manoj Kamath
Mahmoud Kamel
Sundeep Kancherla
Srinivas Kandala
HaoHua Kang
Kyu-Min Kang
Sugbong Kang
Teag Jin Kang
Anton Karamyshev
Shailender Karmuchi
G. Karthik
Sudhir Kasargod
Assaf Kasher
Oren Kedem
Connor Kennedy
Richard Kennedy
John Kenney
Stuart J. Kerry
Francis Keshmiri
Vytas Kezys
samir Khericha
Evgeny Khorov
Dongwan Kim
Geon Hwan Kim
Hyungjin Kim
Jeongki Kim
Myeong-Jin Kim
Sang Gook Kim
Sanghyun Kim
Yongho Kim
Youhan Kim
Akira Kishida
Shoichi Kitazawa
Arik Klein
Andrey Klimakov
Jarkko Kneckt
Jonghoe Koo
Michael Koundourakis
Bruce P. Kraemer
Alexander Krebs
Chung-Ta Ku
Manish Kumar
Ratnesh Kumbhkar
Chih-Chun Kuo
Aleksey Kureev
Kunal Lal
Massinissa Lalam
Zhou Lan
Leonardo Lanante
James Lansford
Hong Won Lee
Hyeong Ho Lee
Il-Gu Lee
Jack Lee
Joonsoo Lee
Mingyu Lee
Wookbong Lee
Xianfu Lei
Ilya Levitsky
Joseph Levy
Guoqing Li
Qinghua Li
Weiyi Li
Yanchun Li
Ryutaro Ohmoto
Hiraku Okada
Hassan Omar
Basak Ozbakiss
Pooria Pakrooh
Saju Palayur
Stephen Palm
Eunsung Park
Minyoung Park
Sungjin Park

Glenn Parsons
Emily Qi
Yinan Qi
Yue Qi
Bin Qian
Yurong Qian
Yingqiao Quan
Saira Rafique
Alireza Raissinia
Rakshith Rajashekar
Helene Ralle
Vishnu Ratnam
Oded Redlich
Josh Redmore
Dror Regev
Mor Reich
Meriam Rezk
Maximilian Riegel
Carlos Rios
Mark Rison
Joerg Robert
Craig Rodine
Stephen Rodriguez
Gil Rosenzweig Arbel
Sayak Roy
Kiseon Ryu
Bilal Sadiq
Sam Sambasivan
Stephan Sand
Amichai Sanderovich
Avik Santra
Naotaka Sato
Takuhiro Sato
Sigurd Schelstraete
Benedikt Schweizer
Jonathan Segev
Sangho Seo
Yongho Seok
Nikola Serafimovski
Kazunobu Serizawa
Ankit Sethi
Julien Sevin
Rubayet Shafin
Feng Shan
Vesh Raj Sharma Banjade
Amit Shaw
Stephen Shellhammer
Xiaoman Shen
Andy Shen
Ian Sherlock
Shuyu Si
Shimi Shilo
Atsushi Shirakawa
Ashish Shukla
Isabelle Siaud
Aditi Singh
Graham Smith
Luther Smith
Malcolm Smith
Youngwan So
Hao Song
Ayush Sood
Robert Sosack
Sudhir Srinivasa
Sundar Sriram
Dorothy Stanley
Adrian Stephens
Noel Stott
Rainer Strobel
Hang Su
Jung Hoon Suh
Bo Sun
Jiaqi Sun
Li-Hsiang Sun
Yanbin Sun
Yanjun Sun
Frank Suraci
Shuntaro Suzuki
Shivkumar Tadahal
Salvatore Talarico
Mohd. Talha
Yusuke Tanaka
Xiaohu Tang
Zhuqing Tang
Yatiraj Tantri Paniyoor
Rakesh Taori
Sidharth Thakur
Sri Ramya Thota
Bin Tian
Hiromichi Tomeba
Alejandro Torrijo
Kazuyuki Tota
Solomon Trainin
Anton Tretiakov
Tsung-Han Tsai
Genadiy Tsodik
Yuki Tsujimaru
Kiran Uln
Yoshio Urabe
Maulik Vaidya
Inaki Val
Richard Van Nee
Allert Van Zelst
Prabodh Varshney
Daniel Verenzuela
Sindhu Verma
Sameer Vermani
Pascal Viger
Bo Wang
Chao Chun Wang
Hao Wang
Huizhao Wang
Lei Wang
Pu Wang
Stephen Qi Wang
Qi Wang
Ying Wang
Zisheng Wang
Roy Want
Lisa Ward
Dong Wei
Hung-Yu Wei
Matthias Wendt
Menzo Wentink
Gregory White
Leif Wilhelmsson
Chao-Yi Wu
Guangsheng Wu
Kanke Wu
Ming Wu
Tianyu Wu
Wayne Wu
Xuming Wu
John Wullert
Qing Xia
Huangfu Xiang
Bo Xiao
Liangxiao Xin
Yan Xin
Fangxin Xu
Yanchao Xu
Yue Xu
Hassan Yaghoobi
Ryota Yamada
Aiguo Yan
Min Yan
Zhongjiang Yan
Subrahmanyam Yanamandra
Hui Yang
Lin Yang
Mao Yang
Ning Yang
Rui Yang
Steve TS Yang
Xun Yang
Yang Yang
Kazuto Yano
James Yee
Yongjiang Yi
Su Khiong Yong
Yelin Yoon
Christopher Young
Heejung Yu
Jian Yu
Fangchao Yuan
Ruochen Zeng
Yan Zeng
Hongyuan Zhang
Jiayin Zhang
Yan Zhang

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

Tomoko Adachi
Kosuke Aio
Abdel Karim Ajami
Thomas Alexander
Boon Chong Ang
Butch Anton
Alfred Asterjadhi
Philippe Astier
Kwok Shum Au
Harry Bims
Vern Brethour
William Byrd
Radhakrishna Canchi
Paul Cardinal
Pin Chang
Hui Che
Cheng Chen
Paul Chiuchiolo
Baw Chng
Subir Das
Mike Davis
Hendricus De Ruijter
Antonio DeLaOlivaDelgado
Xiandong Dong
Alecsander Eitan
Marc Emmelmann
Joseph Epstein
Michael Fischer
P. Flynn
Avraham Freedman
Ming Gan
David Goodall
Binita Gupta
Gloria Gwynne
David Halasz
Mark Hamilton
Daniel Harkins
Brian Hart
Jerome Henry
Marco Hernandez
Lili Hervieu
Werner Hoelzl
Po-Kai Huang
David Hunter
Raj Jain
SangKwon Jeong
Pranav Jha
Joe Natharoj Juisai
Lokesh Kabra
Srinivas Kandala
Ruslan Karmanov
Piotr Karocki
Stuart Kerry
Yongbum Kim
Youhan Kim
Shoichi Kitazawa
Jarkko Kneckt
Alexander Krebs
Takashi Kuramochi
Massinissa Lalam
Hyeong Ho Lee
Richard Lee
James Lepp
Joseph Levy
Guoqing Li
Jialing Li
Qinghua Li
Weiyi Li
Yong Liu
Federico Lovison
Yongsen Ma
Jouni Malinen
William Rogelio Marchand Nino
Ignacio Marin Garcia
Edward Mccall
Stephen McCann
Jonathon Mclendon
Richard Mellitz
Nedime Pelin Mohamed Hassan Salem
Michael Montemurro
Rick Murphy
Okan Mutgan
Gaurang Naik
Stephen Orr
Satoshi Oyama
Bansi Patel
Abhishek Patil
Gaurav Patwardhan
Arumugam Paventhan
Clinton Powell
R. K. Rannow
Maximilian Riegel
Mark Rison
Stephen Rodriguez
Benjamin Rolfe
Jon Rosdahl
Naotaka Sato
Jhony Sembiring
Yongho Seok
Nikola Serafimovski
Rubayet Shafin
Ian Sherlock
Di Dieter Smely
Graham Smith
Luther Smith
Robert Stacey
Dorothy Stanley
Noel Stott
Walter Struppler
Gerald Stueve
Mark Sturza
Bo Sun
Li-Hsiang Sun
Allert Van Zelst
Dmitri Varsanofiev
Prabodh Varshney
John Vergis
Hejun Wang
Lei Wang
Yi-Hsiu Wang
Lisa Ward
Stephen Webb
Dong Wei
Matthias Wendt
Menzo Wentink
Scott Willy
Andreas Wolf
John Wullert
Fangxin Xu
Peng Yan
Jay Yang
Yu Yuan
Sven Zeisberg
Jiayi Zhang
Lihua Zhu
Juan Carlos Zuniga

When the IEEE SA Standards Board approved this recommended practice on 26 September 2024, it had the following membership:

David J. Law, *Chair*
Jon Walter Rosdahl, *Vice Chair*
Gary Hoffman, *Past Chair*
Alpesh Shah, *Secretary*

Sara R. Biyabani
Ted Burse
Stephen Dukes
Doug Edwards
J. Travis Griffith
Guido R. Hiertz
Ronald W. Hotchkiss
Hao Hu
Yousef Kimiagar
Joseph L. Koepfinger*
Howard Li
Xiaohui Liu
John Haiying Lu
Kevin W. Lu
Hiroshi Mano
Paul Nikolich
Robby Robson
Lei Wang
F. Keith Waters
Sha Wei
Philip B. Winston
Don Wright

*Member Emeritus

Introduction

This introduction is not part of IEEE Std 802.11bh-2024, 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—Amendment 1: Operation with Randomized and Changing MAC Addresses.

This amendment specifies modifications to the IEEE Std 802.11 medium access control (MAC) sublayer mechanisms to preserve the existing services that might otherwise be restricted in environments where STAs in an extended service set (ESS) use randomized or changing MAC addresses, without affecting the privacy of the users corresponding to the STAs. User privacy includes exposure of trackable information to third parties or exposure of an individual's presence of behavior.

This amendment introduces mechanisms to enable session continuity in the absence of unique MAC address-to-STA mapping. For STAs in an ESS that use randomized or changing MAC addresses, this amendment preserves the ability to provide customer support, conduct network diagnostics and troubleshooting, and detect device arrival in a trusted environment.

Contents

1 . Overview 18

1.3 Supplementary information on purpose 18

3. Definitions, acronyms, and abbreviations 18

3.2 Definitions specific to IEEE Std 802.11 18
3.4 Abbreviations and acronyms 18

4. General description 18

4.5 Overview of the services 18
4.5.4 Access control and data confidentiality services 18
4.5.4.10 MAC privacy enhancements 18

6. Layer management 19

6.4 Table of MLME SAP interfaces 19
6.5 MLME SAP primitives 19
6.5.7 Associate 19
6.5.7.2 MLME-ASSOCIATE.request 19
6.5.7.3 MLME-ASSOCIATE.confirm 20
6.5.7.4 MLME-ASSOCIATE.indication 21
6.5.7.5 MLME-ASSOCIATE.response 21

9. Frame formats 23

9.3 Format of individual frame types 23
9.3.3 (PV0) Management frames 23
9.3.3.5 Association Request frame format 23
9.3.3.6 Association Response frame format 23
9.3.3.9 Probe Request frame format 23
9.3.3.11 Authentication frame format 24
9.4 Management and Extension frame body components 25
9.4.1.11 Action field 25
9.4.2 Elements 25
9.4.2.1 General 25
9.4.2.240 RSNXE 27
9.4.2.316 Device ID element 27
9.4.2.317 IRM element 28
9.4.2.318 Measurement ID element 28
9.4.2.319 PASN Encrypted Data element 29
9.4.2.320 PASN ID element 30
9.6.36 IRM Action frame details 31
9.6.36.1 General 31
9.6.36.2 Duplicate IRM 31
9.6.36.3 New IRM 32

11. MLME 33

11.3.3 Frame filtering based on STA state 33

11.10 Radio measurement procedures 33

12. Security 34

12.2.13 Identifying a non-AP STA with changing MAC address 34
12.2.13.1 Device ID 34
12.2.13.2 Identifiable random MAC address (IRM) 37
12.7.2 EAPOL-Key frames 39
12.7.3 EAPOL-Key PDU construction and processing 40
12.7.4 EAPOL-Key PDU notation 41
12.7.6 4-way handshake 41
12.7.6.1 General 41
12.7.6.3 4-way handshake message 2 41
12.7.6.4 4-way handshake message 3 42
12.7.6.5 4-way handshake message 4 42
12.13.2 Discovery of a PASN capable AP 42
12.13.3 Key establishment with PASN authentication 42
12.13.3.2 PASN frame construction and processing 42
12.13.8 PTKSA derivation with PASN authentication 44
12.13.11 Encrypting the Encrypted Data field for PASN 45

13. Fast BSS Transition 46

13.4.2 FT initial mobility domain association in an RSN 46

Annex B (normative) Protocol Implementation Conformance Statements (PICS) proforma 47

B.2 Abbreviations and special symbols 47
B.2.2 General abbreviations for Item and Support columns 47
B.4 PICS proforma—IEEE Std 802.11-2020 47
B.4.3 IUT Configuration 47

Annex C (normative) ASN.1 encoding of the MAC and PHY MIB 49

C.3 MIB detail 49

Annex AF (informative) Example of an opaque identifier scheme 50

AF.1 General 50
AF.2 Generation of opaque identifiers 50
AF.3 Processing of opaque identifiers 51
AF.4 Using opaque identifiers 51
AF.5 Security of scheme 51

Annex AG (informative) Examples of device ID and IRM usage 52

AG.1 Examples of device ID usage 52
AG.2 Examples of IRM Usage 57
AG.3 Example of device ID and IRM usage 61

List of Tables

Table 6-1—MLME SA interface 19

Table 9-64—Association Request frame body 23

Table 9-65—Association Response frame body 23

Table 9-71—Presence of fields and elements in Authentication frames 24

Table 9-68—Probe Request frame body 24

Table 9-81—Category values 25

Table 9-130—Element IDs 25

Table 9-190—AKM suite selectors 26

Table 9-142—Optional subelement IDs for Beacon request 26

Table 9-373—Extended RSN Capabilities field 27

Table 9-417a—Device ID Status field values 27

Table 9-417b—IRM Status field values 28

Table 9-417c—Element IDs for Encrypted Data field of the PASN Encrypted Data element 29

Table 9-658a—IRM Action field 31

Table 9-417d—PASN ID Status field values 31

Table 12-10—KDE selectors 39

Table 12-11—Integrity and key wrap algorithms 40

List of Figures

Figure 9-1074a—Device ID element format 27

Figure 9-1074b—IRM element format 28

Figure 9-1074c—Measurement ID element format 28

Figure 9-1074d—PASN Encrypted Data element format 29

Figure 9-1074e—Robust Device ID element format 29

Figure 9-1074g—Robust PASN ID element format 30

Figure 9-1074h—PASN ID element format 30

Figure 9-1074f—Robust IRM element format 30

Figure 9-1322a—Duplicate IRM frame Action field format 31

Figure 9-1322b—New IRM frame Action field format 32

Figure 12-50a—Device ID KDE format 39

Figure 12-50c—PASN ID KDE format 40

Figure 12-50b—IRM KDE format 40

Figure AG-1—Example of device ID exhanges in PASN 53

Figure AG-2—Example of device ID exchange in FILS 54

Figure AG-3—Example of device ID and PASN ID exchange in PASN 56

Figure AG-4—Example of IRM exchange in 4-way handshake 58

Figure AG-5—Example of IRM exchange in FILS 59

Figure AG-6—Example of IRM exchange in PASN 61

Figure AG-7—Example of device ID exchange and IRM exchange in 4-way handshake 63

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

Amendment 1: Operation with Randomized and Changing MAC Addresses

NOTE—The editing instructions contained in this amendment define how to merge the material contained therein into the existing base standard and its amendments to form the comprehensive standard.

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 ~~strikethrough~~ (to remove old material) and underscore (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. Overview

1.3 Supplementary information on purpose

Insert the following at the end of the list:

— Defines a mechanism to enable private (from third parties) device identification of IEEE 802.11 STAs that use randomized or changing MAC addresses.

3. Definitions, acronyms, and abbreviations

3.2 Definitions specific to IEEE Std 802.11

Insert the following definitions maintaining alphabetical order:

device identifier (ID): [device ID] An ID provided by an access point (AP) in an extended service set (ESS) to a non-access point (non-AP) station (STA) to allow the non-AP STA to identify itself to that same ESS during association at a future time.

identifiable random medium access control (MAC) address: [IRM] A random local MAC address provided by a non-access point (non-AP) station (STA) to identify itself to an extended service set (ESS).

measurement identifier (ID): [measurement ID] A transient device ID that an extended service set (ESS) can provide to a non-access point (non-AP) station (STA) to allow the non-AP STA to identify itself to another access point (AP) in the same ESS during a beacon report measurement procedure.

preassociation security negotiation identifier (ID): [PASN ID] A device ID that an extended service set (ESS) can provide to a non-access point (non-AP) station (STA) to allow the non-AP STA to identify itself to a known ESS during PASN authentication at a future time.

3.4 Abbreviations and acronyms

Insert the following acronym definition maintaining alphabetical order:

IRM identifiable random MAC address

4. General description

4.5 Overview of the services

4.5.4 Access control and data confidentiality services

4.5.4.10 MAC privacy enhancements

Change the last paragraph as follows.

To mitigate ~~this sort of~~ traffic analysis and tracking, a non-AP STA can support the ability to periodically and randomly change its MAC addresses and reset counters and seeds prior to association. Such a non-AP STA using the device ID mechanism, upon reconnecting to a network, can provide either a device ID or a

PASN ID previously provided by the network. Such a non-AP STA using the identifiable random MAC address (IRM) mechanism, upon reconnecting to the network can provide the IRM the STA previously provided to the network. Such a non-AP STA can use both device ID and IRM mechanisms concurrently. Such a STA can also use a measurement ID, previously provided by the network, to assist while performing beacon report measurement procedures. These mechanisms allow the network to recognize the STA while providing protection against third party tracking or traffic analysis. When the network can recognize the STA, it can map an already established shared identity state (see 12.2.12) to this STA, which can allow the network to provide network acquisition steering and selection, or allow the network to connect transactional information obtained preassociation or in a prior association to the device that is associating. While discovering networks, a non-AP STA can refrain from gratuitously transmitting Probe Request frames containing SSIDs of favored BSS networks.

6. Layer management

6.4 Table of MLME SAP interfaces

Insert the following row in Table 6-1 (header row shown for convenience).

Table 6-1—MLME SA interface

Service Name	MLME-XXX	Type	References	Comments
IRM Duplicate	IRMDUPLICATE	1	9.6.36 (IRM Action frame details)	See 12.2.13.2 (Identifiable random MAC address (IRM))

6.5 MLME SAP primitives

6.5.7 Associate

6.5.7.2 MLME-ASSOCIATE.request

6.5.7.2.2 Semantics of the service primitive

Change the primitive parameters list as follows (not all parameters are shown):

The primitive parameters are as follows:

MLME-ASSOCIATE.request(
...
Device ID,
IRM,
VendorSpecificInfo
)

Insert the following rows to the parameter description table before the VendorSpecificInfo row (header row shown for convenience):

Name	Type	Valid Range	Description
Device ID	Device ID element	As defined in 9.4.2.316	Specifies the device ID for the requesting STA. Optionally present if dot11FILSActivated is true and dot11DeviceIDActivated is true, otherwise not present.
IRM	IRM element	As defined in 9.4.2.317	Specifies the IRM for the requesting STA. Optionally present if dot11FILSActivated is true and dot11IRMActivated is true, otherwise not present.

6.5.7.3 MLME-ASSOCIATE.confirm

6.5.7.3.2 Semantics of the service primitive

Change the primitive parameters list as follows (not all parameters are shown):

The primitive parameters are as follows:

MLME-ASSOCIATE.confirm(
...
Device ID,
IRM,
PASN ID,
VendorSpecificInfo
)

Insert the following rows to the parameter description table before the VendorSpecificInfo row (header row shown for convenience):

Name	Type	Valid Range	Description
Device ID	Device ID element	As defined in 9.4.2.316	Specifies the device ID for the requesting STA. Optionally present if dot11FILSActivated is true and dot11DeviceIDActivated is true, otherwise not present.
IRM	IRM element	As defined in 9.4.2.317	Specifies the IRM for the requesting STA. Optionally present if dot11FILSActivated is true and dot11IRMActivated is true, otherwise not present.
PASN ID	PASN ID element	As defined in 9.4.2.320	Specifies the PASN ID for the requesting STA. PASN ID is present if Device ID is present; otherwise not present.

6.5.7.4 MLME-ASSOCIATE.indication

6.5.7.4.2 Semantics of the service primitive

Change the primitive parameters list as follows (not all parameters are shown):

The primitive parameters are as follows:

MLME-ASSOCIATE.indication(
...
Device ID,
IRM,
VendorSpecificInfo
)

Insert the following rows to the parameter description table before the VendorSpecificInfo row (header row shown for convenience):

Name	Type	Valid Range	Description
Device ID	Device ID element	As defined in 9.4.2.316 (Device ID element)	Specifies the device ID for the requesting STA. Optionally present if dot11FILSActivated is true and dot11DeviceIDActivated is true, otherwise not present.
IRM	IRM element	As defined in 9.4.2.317 (IRM element)	Specifies the IRM for the requesting STA. Optionally present if dot11FILSActivated is true and dot11IRMActivated is true, otherwise not present.

6.5.7.5 MLME-ASSOCIATE.response

6.5.7.5.2 Semantics of the service primitive

Change the primitive parameters list as follows (not all parameters are shown):

The primitive parameters are as follows:

MLME-ASSOCIATE.response(
...
Device ID,
IRM,
PASN ID,
VendorSpecificInfo
)

Insert the following rows to the parameter description table before the VendorSpecificInfo row (header row shown for convenience):

Name	Type	Valid Range	Description
Device ID	Device ID element	As defined in 9.4.2.316	Specifies the device ID for the requesting STA. Optionally present if dot11FILSActivated is true and dot11DeviceIDActivated is true, otherwise not present.
IRM	IRM element	As defined in 9.4.2.317	Specifies the IRM for the requesting STA. Optionally present if dot11FILSActivated is true and dot11IRMActivated is true, otherwise not present.
PASN ID	PASN ID element	As defined in 9.4.2.320	Specifies the PASN ID for the requesting STA. PASN ID is present if Device ID is present; otherwise not present.

9. Frame formats

9.3 Format of individual frame types

9.3.3 (PV0) Management frames

9.3.3.5 Association Request frame format

Insert the following new rows before the Vendor Specific field of Table 9-64 (header row shown for convenience.)

Table 9-64—Association Request frame body

Order	Information	Notes
61	Device ID	If dot11DeviceIDActivated is true and dot11FILSActivated is true, the Device ID element is optionally present when using FILS authentication; otherwise, it is not present.
62	IRM	If dot11IRMActivated is true and dot11FILSActivated is true, the IRM element is optionally present when using FILS authentication; otherwise, it is not present.

9.3.3.6 Association Response frame format

Insert the following new rows before the Vendor Specific field of Table 9-65 (header row shown for convenience.)

Table 9-65—Association Response frame body

Order	Information	Notes
78	Device ID	If dot11DeviceIDActivated is true and dot11FILSActivated is true, the Device ID element is optionally present when using FILS authentication; otherwise, it is not present.
79	IRM	If dot11IRMActivated is true and dot11FILSActivated is true, the IRM element is optionally present when using FILS authentication; otherwise, it is not present.
80	PASN ID	The PASN ID element is present if the Device ID element is present and dot11PASNActivated is true; otherwise, it is not present.

9.3.3.9 Probe Request frame format

Insert the following item into the appropriate place in Table 9-68 (header row shown for convenience.)

Table 9-68—Probe Request frame body

Order	Information	Notes
43	Measurement ID	The Measurement ID element is optionally present if dot11DeviceIDActivated is true

9.3.3.11 Authentication frame format

Change the following rows in Table 9-71 as shown (header row shown for convenience)

Table 9-71—Presence of fields and elements in Authentication frames

Authentication algorithm	Authentication transaction sequence number	Status Code	Presence of fields and elements from order 4 onward
PASN Authentication	1	Reserved	RSNE is present. RSNXE is present if any subfield of the Extended RSN Capabilities field in this element, except the Field Length subfield, is nonzero. PASN Parameters element is present. Timeout Interval element is optionally present. Wrapped Data element is present if wrapped data format in PASN Parameters element is nonzero and not reserved. Fragment element is optionally present if any of the elements are fragmented. Tunneled PASN element may be present. PASN ID element is optionally present.
PASN Authentication	2	Status	RSNE is present and PASN Parameters element is present if Status Code field is 0. RSNXE is present if any subfield of the Extended RSN Capabilities field in this element, except the Field Length subfield, is nonzero. Timeout Interval element is optionally present. Wrapped Data element is present if wrapped data format in PASN Parameters element is nonzero and not reserved and Status Code field is 0. PASN Encrypted Data element is optionally present. MIC element is present. Fragment element may be present if any of the elements are fragmented and Status Code field is 0. Tunneled PASN element is optionally present.
PASN Authentication	3	Status	PASN Parameters element is present if Status Code field is 0. Wrapped Data element is present if wrapped data format in PASN Parameters element is nonzero and not reserved; and Status Code field is 0. PASN Encrypted Data element is optionally present. MIC element is present. Fragment element may be present if any of the elements are fragmented and Status Code field is 0.

9.4 Management and Extension frame body components

9.4.1.11 Action field

Insert the following new row into Table 9-81 as shown (header row shown for convenience).

Table 9-81—Category values

Code	Meaning	See subclause	Robust	Group addressed privacy
39	IRM	9.6.36	Yes	No

9.4.2 Elements

9.4.2.1 General

Insert the following new rows in Table 9-130 (header row shown for convenience) as appropriate.

Table 9-130—Element IDs

Element	Element ID	Element ID Extension	Extensible	Fragmentable
Device ID (see 9.4.2.316)	255	138	Yes	No
IRM (see 9.4.2.317)	255	139	Yes	No
PASN Encrypted Data (see 9.4.2.319)	255	140	Subelements	Yes
PASN ID (see 9.4.2.320)	255	144	Yes	No
Measurement ID (see 9.4.2.318)	255	145	No	No

9.4.2.19.7 Beacon request

Insert the following two rows into Table 9-142 after the row of subelement ID 164 (header row shown for convenience) and update the following row as shown.

Table 9-142—Optional subelement IDs for Beacon request

Subelement ID	Name	Extensible
166	IRM Recommendation	No
167	Measurement ID	No
~~165~~168-220	Reserved	

Insert the following paragraphs after the paragraph beginning "The Last Beacon Report Indication Request" as shown.

The IRM Recommendation subelement has the format defined in Figure 9-1074b, with the Length field set to 0. When the IRM Recommendation subelement is included in a Beacon request, it requests the responding STA use an IRM in the Address 2 field in the Probe Request frames the STA transmits. The Measurement ID element has the format defined in Figure 9-1074c. When the Measurement ID element is included in a Beacon request, it requests the responding STA include the provided Measurement ID element in the Probe Request frames the STA transmits.

A Beacon request does not include both an IRM Recommendation subelement and a Measurement ID subelement.

9.4.2.23.3 AKM Suites

Insert the following new row in Table 9-190 (header rows shown for convenience).

Table 9-190—AKM suite selectors

OUI	Suite type	Meaning			Authentication algorithm numbers (see 9.4.1.1)	Cipher suite selector restriction
		Authentication type	Key Management type	Key derivation type		
00-0F-AC	26	PASN with defined key wrap	N/A	N/A	N/A	N/A

9.4.2.240 RSNXE

Insert the following new rows in Table 9-373 (header row shown for convenience).

Table 9-373—Extended RSN Capabilities field

Bit	Information	Notes
16	Device ID Support	A STA sets the Device ID Support field to 1 when dot11DeviceIDActivated is true to indicate that the device ID mechanism is supported. Otherwise, the STA sets the Device ID Support field to 0.
17	IRM Support	A STA sets the IRM Support field to 1 when dot11IRMActivated is true to indicate that the IRM mechanism is supported. Otherwise, the STA sets the IRM Support field to 0.
18	KEK In PASN	The field is set to 1 when dot11KEKPASNActivated is true to indicate support for deriving a KEK when using PASN. Otherwise, the field is set to 0.

Insert the following subclauses after the last subclause in 9.4.2:

9.4.2.316 Device ID element

The format of the Device ID element is shown in Figure 9-1074a.

	Element ID	Length	Element ID Extension	Device ID Length	Device ID Status	Device ID
Octets:	1	1	1	1	0 or 1	variable

Figure 9-1074a—Device ID element format

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1.

The Device ID Length field is set to the number of octets in the Device ID field.

When the element is sent from an AP, the Device ID Status field contains one of the values shown in Table 9-417a.

Table 9-417a—Device ID Status field values

Device ID Status	Name	Meaning
0	Recognized	Indicates that the device ID has been recognized.
1	Not Recognized	Indicates that the device ID has not been recognized.
2	Not Applicable	Indicates that a device ID was not included in the request
3-255	Reserved	

When the Device ID element is sent to an AP, the Device ID Status field is not present.

The Device ID field contains a device ID.

NOTE—The device ID might be constructed as an opaque identifier as described in 12.2.13.1 (Device ID).

9.4.2.317 IRM element

The format of the IRM element is shown in Figure 9-1074b.

	Element ID	Length	Element ID Extension	IRM Status	IRM
Octets:	1	1	1	0 or 1	0 or 6

Figure 9-1074b—IRM element format

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1(General).

When the element is sent to an AP, the IRM Status field is not present.

When the element is sent from an AP, the IRM Status field is defined in Table 9-417b.

Table 9-417b—IRM Status field values

IRM Status	Name	Meaning
0	Recognized	Indicates that the IRM has been recognized.
1	Not Recognized	Indicates that the IRM has not been recognized.
2-255	Reserved	

The IRM field contains a MAC address when sent from a non-AP STA to an AP.

The IRM field is not present when sent from an AP to a non-AP STA.

9.4.2.318 Measurement ID element

The Measurement ID element contains a measurement ID. The format of the Measurement ID element is shown in Figure 9-1074c.

	Element ID	Length	Element ID Extension	Measurement ID
Octets:	1	1	1	variable

Figure 9-1074c—Measurement ID element format

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1.

The Measurement ID field contains a measurement ID.

9.4.2.319 PASN Encrypted Data element

The PASN Encrypted Data element contains encrypted data included in PASN authentication. The format of the PASN Encrypted Data element in Figure 9-1074d.

	Element ID	Length	Element ID Extension	Encrypted Data
Octets:	1	1	1	variable

Figure 9-1074d—PASN Encrypted Data element format

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1.

The Encrypted Data field contains one or more elements encrypted using the KEK (see 12.13.11). The element format is defined in 9.4.2.1. The Element ID field values for the defined elements of the PASN Encrypted Data element are shown in Table 9-417c.

Table 9-417c—Element IDs for Encrypted Data field of the PASN Encrypted Data element

Element ID	Name	Extensible
0	Robust Device ID	No
1	Robust IRM	No
2	Robust PASN ID	No
3-220	Reserved	
221	Vendor Specific	Vendor Defined
222-255	Reserved	

The format of the Robust Device ID element is shown in Figure 9-1074e.

	Element ID	Length	Device ID Status	Device ID
Octets:	1	1	0 or 1	variable

Figure 9-1074e—Robust Device ID element format

The Element ID field is defined in Table 9-417c.

The Length field is defined in 9.4.2.1.

The Device ID Status field and the Device ID field are defined in 9.4.2.316.

The format of the Robust IRM element is shown in Figure 9-1074f.

	Element ID	Length	IRM Status	IRM
Octets:	1	1	0 or 1	variable

Figure 9-1074f—Robust IRM element format

The Element ID field is defined in Table 9-417c.

The Length field is defined in 9.4.2.1.

The IRM Status field and the IRM field are defined in 9.4.2.317.

The format of the Robust PASN ID element is shown in Figure 9-1074g.

	Element ID	Length	PASN ID Status	PASN ID
Octets:	1	1	0 or 1	variable

Figure 9-1074g—Robust PASN ID element format

The Element ID field is defined in Table 9-417c.

The Length field is defined in 9.4.2.1.

The PASN ID Status field and the PASN ID field are defined in 9.4.2.320

9.4.2.320 PASN ID element

The PASN ID element contains a PASN ID. The format of the PASN ID element is shown in Figure 9-1074h.

	Element ID	Length	Element ID Extension	PASN ID Length	PASN ID Status	PASN ID
Octets:	1	1	1	1	0 or 1	variable

Figure 9-1074h—PASN ID element format

The Element ID, Length, and Element ID Extension fields are defined in 9.4.2.1.

The PASN ID Length field contains the length of the PASN ID field.

When the element is sent from an AP, the PASN ID Status field is defined in Table 9-417d.

When the element is sent from a non-AP STA, the PASN ID Status field is not present.

Table 9-417d—PASN ID Status field values

PASN ID Status	Name	Meaning
0	Recognized	Indicates that the PASN ID has been recognized
1	Not Recognized	Indicates that the PASN ID has not been recognized
2	Not Applicable	Indicates that a PASN ID was not included in the request
3-255	Reserved	

The PASN ID field contains a PASN ID.

NOTE—The PASN ID might be constructed as an opaque identifier as described in 12.2.13.1 (Device ID).

Insert the following subclauses after the last subclause in 9.6:

9.6.36 IRM Action frame details

9.6.36.1 General

Two Action frames are defined for IRM purposes. An IRM Action field, immediately after the Category field, differentiates the meanings. The values of the IRM Action field are defined in Table 9-658a.

Table 9-658a—IRM Action field

Action field value	Meaning
0	Duplicate IRM
1	New IRM
2-255	Reserved

9.6.36.2 Duplicate IRM

The format of the Duplicate IRM frame Action field is shown in Figure 9-1322a.

	Category	IRM Action
Octets:	1	1

Figure 9-1322a—Duplicate IRM frame Action field format

The Category field is defined in 9.4.1.11.

The IRM Action field is defined in Table 9-658a in 9.6.36.1.

9.6.36.3 New IRM

The format of the New IRM frame Action field is shown in Figure 9-1322b.

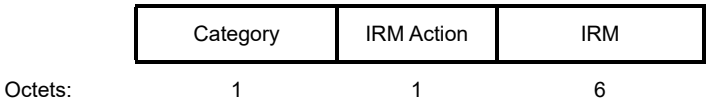

Figure 9-1322b—New IRM frame Action field format

The Category field is defined in 9.4.1.11 (Action field).

The IRM Action field is defined in Table 9-658a in 9.6.36.1.

The IRM field contains a MAC address.

11. MLME

11.3.3 Frame filtering based on STA state

Insert the item as shown to the following list in 11.3.3:

b) Class 1a frames

In an infrastructure BSS when PTKSA from PASN authentication exists

1) Protected Fine Timing frames (9.6.34)
2) SA Query Request and SA Query Response frames sent to an individual address (11.13)
3) IRM Action frame (9.6.36)

11.10 Radio measurement procedures

11.10.9.1.1 General

Change the list after the 7th paragraph as shown:

If dot11RMBeaconActiveMeasurementActivated is true and the measurement mode in the measurement request is Active, the measuring STA shall perform the following procedure (or an equivalent procedure) on the requested channel, if permitted (e.g. the channel is not subject to DFS):

— If the channel is not the operating channel, wait for dot11RMMeasurementNavSync, or until a PHY-RXSTART.indication primitive has been received.

— Using the basic access protocol in 10.3.4.2, send a Probe Request frame to the broadcast address. The BSSID field in the Probe Request frame shall be set to the BSSID field in the measurement request. The SSID element in the Probe Request frame shall be set to the SSID element in the measurement request. If dot11IRMActivated is true and the IRM Recommendation subelement is present in the measurement request, then the Address 2 field in the Probe Request frame shall be set to the IRM. If dot11DeviceIDActivated is true and the Measurement ID element is present in the measurement request, then the Measurement ID element shall be included in the Probe Request frame.

Change the following existing paragraph and insert the following paragraph as shown:

If the BSSID field in the Measurement Request contains a wildcard BSSID, all observed BSSs with the requested SSID shall be reported in a separate Beacon report for each BSSID. If the SSID subelement is not included in the Beacon request, all observed BSSs shall be reported in a separate Beacon report for each BSSID. In active mode, Probe Response frames shall be evaluated regardless of whether the Probe Response frame was triggered by the measuring STA's Probe Request frame.

If dot11RMBeaconActiveMeasurementActivated is true, dot11DeviceIDActivated is true, and the measurement mode in the measurement request is Active, then the Beacon request may include a Measurement ID subelement containing a measurement ID. The measurement ID is copied into the Measurement ID field in the Measurement ID element (see 9.4.2.318) in the measuring STA's Probe Request frame. The AP shall assign a new measurement ID for each measurement exchange.

12. Security

Insert the following new subclauses after 12.2.12 (i.e. immediately before 12.3).

12.2.13 Identifying a non-AP STA with changing MAC address

To mitigate tracking and traffic analysis by third parties, a non-AP STA can randomly change its MAC address while not associated (see 4.5.4.10).

This presents a problem for the network in that it is unable to identify a non-AP STA that previously associated and is not able to apply cached information (shared identity state) from the previous association to the current association (see 12.2.10). Similarly, this presents a problem for the non-AP STA in that it cannot assume the network can recognize the STA as correlated to any cached information from previous association(s). Two mechanisms are defined to alleviate these problems.

The first mechanism, referred to as the device ID mechanism, has the AP provide an identifier to the non-AP STA during association or PASN authentication that the non-AP STA then reports back to the AP during a future association or PASN authentication. The second mechanism, referred to as the IRM mechanism, has the non-AP STA provide a random MAC address (different from the address it is currently using as the TA for its transmissions) to the AP during association or PASN authentication and then use that MAC address as the TA for its own transmissions for identification of the STA during its next pre-association exchanges, next PASN authentication, and/or next association and next associated exchanges with that AP.

The device ID mechanism and the IRM mechanism require that the non-AP-STA supports the MAC privacy enhancements in 12.2.11. A non-AP-STA shall set dot11PrivacyActivated equal to true to use either of these mechanisms. The two mechanisms allow the network to recognize the STA while mitigating the abilities of third parties to do traffic analysis and tracking of the non-AP STA. When the STA receives an indication that it is successfully recognized by the network, it can proceed knowing that its prior shared identity state is established and reused by its applications, higher-layer control plane (such as the network allowing access to the LAN and WAN, etc.), and also for layer 2 control plane (pre-/non-association identity for access and steering, etc.). Alternatively, when the STA fails to be successfully recognized, it knows that where such shared identity state is needed/desired, it will have to be re-established through additional protocol exchanges. Both mechanisms also provide for the non-AP STA to opt-in (typically under user control) to participating in the recognition mechanism, so that sensitive user information can be kept confidential unless the network is trusted.

The two mechanisms may be used concurrently.

Annex AG provides illustrative examples of the usage of device ID and IRM.

NOTE 1—The IRM mechanism and the device ID mechanism are independent. The IRM mechanism allows an AP to recognize a non-AP STA prior to association and while it is associated. The Device ID mechanism allows an AP to identify a non-AP STA while it is associated. A device ID is allocated by an AP, and an IRM is selected by a non-AP STA. If both an AP and a non-AP STA have both IRM and device ID activated, the non-AP STA might provide both an IRM and a device ID during association or PASN authentication.

NOTE 2—The device ID and IRM mechanisms are not specified for use in PBSSs.

12.2.13.1 Device ID

An AP that has dot11DeviceIDActivated equal to true advertises support for the device ID mechanism by setting the Device ID Support field to 1 in the Extended RSN Capabilities field in the RSNXE (see 9.4.2.240) in Beacon and Probe Response frames.

A non-AP STA that has dot11MACPrivacyActivated and dot11DeviceIDActivated equal to true sets the Device ID Support field to 1 in the Extended RSN Capabilities field in the RSNXE to indicate that the

device ID mechanism is supported. The RSNXE with the Device ID Support field equal to 1 is present in either (Re)Association Request frames or the first PASN frame that is sent to an AP that advertises support for the device ID mechanism.

An AP that includes the PASN AKMP as part of the RSNE included in Beacon and Probe Response frames, i.e., when dot11PASNActivated is true, and has dot11DeviceIDActivated equal to true shall set dot11KEKPASNActivated to true.

A non-AP STA that has dot11MACPrivacyActivated and dot11DeviceIDActivated equal to true and uses PASN, i.e., when dot11PASNActivated is true, shall set dot11KEKPASNActivated to true.

An AP that has dot11DeviceIDActivated equal to true and that receives a (Re)Association Request frame or the first PASN frame that includes an Extended RSN Capabilities field with the Device ID Support field equal to 1 shall do one of the following:

— include an Extended RSN Capabilities element in the (Re)Association Response frame with the Device ID Support field set to 1.
— include an Extended RSN Capabilities element in the second PASN frame with the Device ID Support field set to 1.

For correct operation of the device ID mechanism, all APs in an ESS need to have dot11DeviceIDActivated set to true.

NOTE 1—The criteria and mechanism to distribute device IDs to the APs in the ESS is out of scope of this standard.

A STA should not send a frame containing a Device ID element or a PASN ID element to any STA unless the receiving STA has set the Device ID Support field to 1 in the Extended RSN Capabilities field.

When an AP provides a device ID and, if dot11PASNActivated is true, a PASN ID as follows:

1) When using FILS authentication, the AP shall provide a device ID in a Device ID element and, if dot11PASNActivated is true, a PASN ID in a PASN ID element in the Association Response frame.
2) When using PASN authentication, the AP shall provide a device ID in a Robust Device ID element and a PASN ID in a Robust PASN ID element in the second PASN frame.
3) When not using PASN or FILS authentication, the AP shall provide a device ID in a Device ID KDE and, if dot11PASNActivated is true, a PASN ID in a PASN ID KDE in message 3 of the 4-way handshake.

If an AP with dot11DeviceIDActivated equal to true receives an Association Request frame that includes an Extended RSN Capabilities field with the Device ID Support field equal to 1 from a non-AP STA, the AP may provide both a device ID and, if dot11PASNActivated is true, a PASN ID using the procedure described below:

3) When using FILS authentication and the non-AP STA did not provide a device ID in the Device ID element in the Association Request frame, the AP may provide a device ID in the Device ID element setting the Device ID Status field to 2 to indicate Not Applicable and, if dot11PASNActivated is true, a PASN ID in the PASN ID element setting the PASN ID Status field to 2 to indicate Not Applicable in the Association Response frame.
4) When not using PASN or FILS authentication and the non-AP STA did not provide a device ID in the Device ID KDE in message 2 of the 4-way handshake, the AP may provide a device ID in the Device ID KDE setting the Device ID Status field to 2 to indicate Not Applicable and, if dot11PASNActivated is true, a PASN ID in the PASN ID KDE setting the PASN ID Status field to 2 to indicate Not Applicable in message 3 of the 4-way handshake.

NOTE 2—An AP is expected to provide a device ID and a PASN ID in the general case, but the AP might not be able to do that in some cases, e.g. due to not having sufficient resources or access to an external server to generate an identifier that is shared with all the APs in the ESS.

If an AP with dot11DeviceIDActivated equal to true receives from a non-AP STA a first PASN frame that includes an Extended RSN Capabilities field with the Device ID Support field equal to 1 but no PASN ID element, the AP shall provide a device ID in the Robust Device ID element and a PASN ID in the Robust PASN ID element in the second PASN frame.

If a non-AP STA has been provided a device ID by an AP in an ESS, then it may provide that device ID when returning to that ESS. It provides the device ID as follows:

1) When using FILS authentication, in a Device ID element in the Association Request frame.
2) When not using PASN or FILS authentication, in a Device ID KDE in message 2 of the 4-way handshake.

If a non-AP STA has been provided with a device ID and a PASN ID, then it may provide the PASN ID in the PASN ID element in the first PASN frame, when using PASN authentication. An AP shall provide a PASN ID in the Robust PASN ID element in the second PASN frame, when using PASN authentication.

The PASN ID shall be random and not shorter than 6 octets.

A STA may delete either or both of a stored device ID and a stored PASN ID at any point in time for implementation specific reasons.

When a non-AP STA sends a device ID or a PASN ID to an AP, it shall use the device ID or the PASN ID most recently received from any AP belonging to the same ESS.

When an AP with dot11DeviceIDActivated equal to true receives an Association Request frame or message 2 of the 4-way handshake, containing a device ID from a non-AP STA and the AP recognizes the received device ID, the AP shall perform one of the following actions:

1) Set the Device ID Status field of the Device ID KDE or Device ID element to 0 to indicate that the AP recognizes the non-AP STA and set the Device ID field to zero length (indicating the current device ID is maintained) in an Association Response frame or message 3 of the 4-way handshake.
2) Assign a new device ID value in the Device ID field and set the Device ID Status field of the Device ID KDE or Device ID element to 0 and, if dot11PASNActivated is true, assign a new PASN ID value in the PASN ID field and set the PASN ID Status field of the PASN ID KDE or PASN ID element to 2, in an Association Response frame or message 3 of the 4-way handshake.

When an AP with dot11DeviceIDActivated equal to true receives a first PASN frame containing a PASN ID that it recognizes, the AP shall assign a new PASN ID value to the non-AP STA and include this new PASN ID in a Robust PASN ID element in the second PASN frame, setting the PASN ID Status field of the Robust PASN ID element to 0 to indicate Recognized.

When a non-AP STA receives a frame that contains a Device ID Status field in the Device ID KDE or Device ID element equal to 0, or a PASN ID Status field in the Robust PASN ID element equal to 0, indicating Recognized, it proceeds with the assumption that the shared identity state with the AP or ESS (as per the concepts of 12.2.13) is now bound to the MAC address in the Address 2 field in the Association Request frame or the first PASN frame most recently transmitted by the non-AP STA.

If an AP provides a Robust Device ID element or Device ID KDE with the Device ID Status field set to 1, indicating Not Recognized, then the AP may also provide in that same Robust Device ID element or Device ID KDE a new device ID and, in a Robust PASN ID element or PASN ID KDE, a new PASN ID, thus establishing a new shared identity state. An AP shall set a Device ID Status field to 1 indicating Not Recognized if the AP cannot unequivocally identify the non-AP STA shared identity state.

NOTE 3—An AP is expected to provide a device ID and a PASN ID when the AP does not recognize the provided device ID or PASN ID, but the AP might not be able to do that in some cases, e.g. due to not having sufficient resources or access to an external server to generate an identifier that is shared with all APs in the ESS.

If an AP provides a Robust PASN ID element with the PASN ID Status field set to 1, indicating Not Recognized, then the AP may also provide in that same Robust PASN ID element a new PASN ID and in a Robust Device ID element a new Device ID, thus establishing a new shared identity state. An AP may set a PASN ID Status field to 1 indicating Not Recognized if the AP cannot unequivocally identify the non-AP STA shared identity state.

When a non-AP STA receives a frame that contains a Device ID Status field in a Device ID KDE or Robust Device ID element equal to 1, or a PASN ID Status field in a PASN Status field in a Robust PASN ID element equal to 1, indicating Not Recognized, it shall assume that no shared identity state exists with the AP or ESS (as per the concepts of 12.2.13).

NOTE 4—When using PASN authentication, the Robust Device ID element is included in the Encrypted Data field of the PASN Encrypted Data element (see 12.13.11).

An AP may use the procedure in Annex AF, or any other procedure (including nothing if the device ID or PASN ID is encrypted by the AP itself), to keep the device ID or PASN ID content private (opaque) from third parties when sent over the air.

12.2.13.2 Identifiable random MAC address (IRM)

An AP that has dot11IRMActivated equal to true advertises support for the IRM mechanism by setting the IRM Support field to 1 in the Extended RSN Capabilities field in the RSNXE (see 9.4.2.240) in Beacon and Probe Response frames.

A non-AP STA that has dot11MACPrivacyActivated and dot11IRMActivated equal to true indicates that the IRM mechanism is supported by setting the IRM Support field to 1 in the Extended RSN Capabilities field in the RSNXE in either the (Re)Association Request frames or the first PASN frame that it sends to an AP that advertises support for the IRM mechanism.

An AP that has dot11IRMActivated equal to true and that receives a (Re)Association Request frame or the first PASN frame that includes an Extended RSN Capabilities field with the IRM Support field equal to 1 shall do one of the following:

— Include an Extended RSN Capabilities element in the (Re)Association Response frame with the IRM Support field set to 1.
— Include an Extended RSN Capabilities element in the second PASN frame with the IRM Support field set to 1.

An AP that includes the PASN AKMP as part of the RSNE included in Beacon and Probe Response frames, i.e., when dot11PASNActivated is true, and has dot11IRMActivated equal to true shall set dot11KEKPASNActivated to true.

A non-AP STA that has dot11MACPrivacyActivated and dot11IRMActivated equal to true and intends to use PASN, i.e., when dot11PASNActivated is true, shall set dot11KEKPASNActivated to true.

Correct operation of the IRM mechanism depends on all APs in the ESS being configured with dot11IRMActivated set to true. Activation of the IRM mechanism needs to be advertised by all APs in an ESS in Beacons and Probe Response frames.

NOTE 1—The criteria and mechanism to distribute IRMs to the APs in the ESS is out of scope of this standard.

An IRM is a random MAC address that is constructed from the locally administered address space. A non-AP STA shall construct randomized IRMs according to IEEE Std 802®-2014 and IEEE Std 802c™-2017.

When associating for the first time or authenticating using PASN for the first time to an AP in an ESS, the non-AP STA may use any local MAC address or its universal MAC address. Each time the non-AP STA associates with an AP in an ESS, it may provide a new IRM to the AP during association. That IRM may be shared with all the APs in the ESS. The non-AP STA may then use that IRM as its TA the next time it associates with any AP in that same ESS. The non-AP STA shall also use that IRM as its TA for any Probe Request frames, directed or broadcast, public Action frames, Authentication frames, and (Re)Association frames that it transmits when it intends to be identified.

When associating to an AP that advertises activation of the IRM mechanism, the non-AP STA may provide a new IRM to the AP by including an IRM KDE in message 4 of the 4-way handshake or, when using FILS authentication, including the IRM element in the Association Request frame. When using PASN, the non-AP STA may provide a new IRM to the AP by including the IRM element in the third PASN frame.

If a newly provided IRM is already in use by any STA in the ESS, or is identical to an IRM stored by the AP for another STA, then, after association or authentication using PASN, the AP should send a Duplicate IRM frame (see 9.6.36.2) to the non-AP STA that provided the new IRM indicating that the provided IRM is a duplicate. The non-AP STA may then respond with a New IRM frame (see 9.6.36.3), to provide a new IRM to the AP.

The non-AP STA should store the newly allocated IRM as an identifier for use with the APs in that ESS and the APs in that ESS should store the IRM as an identifier for that non-AP STA. The non-AP STA then should use that allocated IRM as its TA when it next associates or uses PASN to preassociate with that same AP or another AP in the same ESS.

A non-AP STA indicates the IRM mechanism is activated in a (Re)Association Request frame or in the first PASN frame and the AP indicates the IRM mechanism is activated in the corresponding (Re)Association Response frame or in the second PASN frame. A non-AP STA may indicate the IRM mechanism is activated in an Association Request frame as part of an initial mobility domain association. If a non-AP STA indicates the IRM mechanism is activated in an Association Request frame or first PASN frame and the AP indicates the IRM mechanism is activated in the corresponding Association Response frame or second PASN frame, then the AP shall support the following options:

— The AP shall include an IRM KDE in message 3 of the 4-way handshake if executing a 4-way handshake.
— The AP shall include an Robust IRM element in the Association Response frame if using FILS authentication.
— The AP shall include an Robust IRM element in the second PASN frame if using PASN authentication.

If the AP recognizes the IRM used as the TA in the received frame(s) from the non-AP STA, the AP shall set the IRM Status field of the IRM KDE or IRM element to Recognized. If the AP does not recognize the IRM, the AP shall set the IRM Status field of the IRM KDE or IRM element to Not Recognized and the IRM field is not present. An AP shall set the IRM Status field to 1 indicating Not Recognized if the AP cannot unequivocally identify the non-AP STA shared identity state.

The non-AP STA, on receipt of an IRM Status field equal to 1, indicating that the AP has not recognized the IRM, shall either continue to associate or authenticate using PASN to the AP and optionally provide a new IRM in an IRM KDE in message 4 of the 4-way handshake or, when using FILS authentication optionally provide an IRM element in the Association Request frame, or when using PASN authentication optionally provide an IRM element in the third PASN frame, else disassociate/deauthenticate.

When a non-AP STA is associating for the first time or authenticating using PASN for the first time to any AP in an ESS, the AP shall set the IRM Status field to 1 in the response frame indicating Not Recognized. In this case, the non-AP STA shall ignore that the IRM Status field is equal to 1 and continue to associate or authenticate using PASN.

NOTE 2—A STA might delete a stored IRM at any point in time for implementation specific reasons.

If a non-AP STA has previously provided an IRM to an AP in an ESS, the APs in the ESS have retained the information, and the non-AP STA sends an Authentication frame using that IRM as the TA to any AP in the ESS, then the AP receiving the Authentication frame can identify the non-AP STA before association is started or completed. A non-AP STA may use that address when actively scanning for any AP in that ESS, such that the AP may identify the non-AP STA. A non-AP STA that has provided an IRM to any AP in an ESS may use that address in a Public Action frame (e.g., a GAS frame) such that APs in that ESS may identify the non-AP STA.

A non-AP STA should change the IRM for each association or PASN authentication.

NOTE 3—When using PASN authentication, the IRM element is included in the Encrypted Data field of the PASN Encrypted Data element (see 12.13.11).

12.7.2 EAPOL-Key frames

Insert new rows in Table 12-10 and change the final row of the table as shown as shown below (header row shown for convenience.)

Table 12-10—KDE selectors

OUI	Data Type	Meaning
00-0F-AC	20	Device ID KDE
00-0F-AC	21	IRM KDE
00-0F-AC	22	PASN ID KDE
00-0F-AC	23 ~~16~~—255	Reserved

Insert the following descriptions of the new KDEs at the end of 12.7.2.

The format of the Device ID KDE is shown in Figure 12-50a.

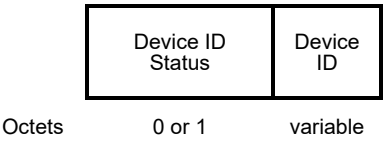

Figure 12-50a—Device ID KDE format

The Device ID Status field is defined in 9.4.2.316.

The Device ID field contains a device ID.

The format of the IRM KDE is shown in Figure 12-50b.

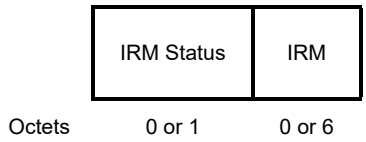

Figure 12-50b—IRM KDE format

The IRM Status and IRM fields are as defined in 9.4.2.317.

The format of the PASN ID KDE is shown in Figure 12-50c.

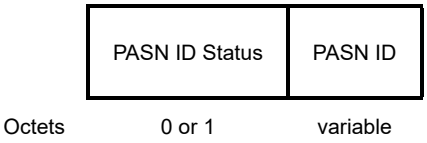

Figure 12-50c—PASN ID KDE format

The PASN ID Status field is defined in 9.4.2.320.

The PASN ID field contains a PASN ID.

12.7.3 EAPOL-Key PDU construction and processing

Change or insert the following rows in Table 12-11 as shown below (header row shown for convenience).

Table 12-11—Integrity and key wrap algorithms

AKM	Integrity algorithm	KCK_bits	Size of MIC (octets)	Key wrap algorithm	KEK_bits	KCK2_bits	KEK2_bits
00-0F-AC:21	See NOTE	N/A	N/A	~~N/A~~ As defined by Base AKMP in Table 12-11 if Base AKMP is not 00-0F-AC:21, NIST EAS Key Wrap if Base AKMP is 00-0F-AC:21.	~~N/A~~ As defined by Base AKMP in Table 12-11 if Base AKMP is not 00-0F-AC:21, 128 if Base AKMP is 00-0F-AC:21.	N/A	N/A
00-0F-AC:26	See NOTE	N/A	N/A	AES-SIV-256	256	N/A	N/A

12.7.4 EAPOL-Key PDU notation

Insert the following text after OCI (shown for reference).

OCI	is the OCI KDE
Device ID	is the Device ID KDE, described in 9.4.2.316
IRM	is the IRM KDE, described in 9.4.2.317
PASN ID	is the PASN ID KDE, described in 9.4.2.320

12.7.6 4-way handshake

12.7.6.1 General

Change the following text as shown.

RSNA defines a protocol using EAPOL-Key PDUs called the *4-way handshake*. The handshake completes the IEEE 802.1X authentication process. The information flow of the 4-way handshake is as follows:

Message 1: Authenticator → Supplicant: OCI(0 or 1, 0, 1, 0, P, 0, 0, ANonce, 0, {PMKID})

Message 2: Supplicant → Authenticator: EAPOL-Key(0 or 1, 1, 0, 0, P, 0, 0, SNonce, MIC, {RSNE [, RSNXE] [, OCI] [, Device ID]})

Message 3: Authenticator→Supplicant: EAPOL-Key(1, 1, 1, 1, P, 0, RSC, ANonce, MIC, {RSNE [, RSNXE] [, OCI], GTK(N) [, IGTK(M, IPN)] [, BIGTK(Q, BIPN)] [, WIGTK(R, WIPN)] [, SSID] [,Device ID] [IRM] [,PASN ID]})

Message 4: Supplicant → Authenticator: EAPOL-Key(1, 1, 0, 0, P, 0, 0, 0, MIC, {[IRM]}).

12.7.6.3 4-way handshake message 2

Change the following text as shown to the list beginning "Key Information:".

Key Information:

...

Encrypted Key Data = 1 when using an AEAD cipher or if the Device ID KDE is included, or 0 otherwise

Reserved = 0 – unused by this protocol version

Insert the following text as shown to the list beginning "Key Data =".

Key Data =

— ...

— Additionally, contains an OCI KDE when dot11RSNAOperatingChannelValidationActivated is true on the Supplicant.

— Additionally, may include a Device ID KDE subject to the conditions in 12.2.13.1.

— The RSNXE that the Supplicant sent in its (Re)Association Request frame, if this element is present in the (Re)Association Request frame that the Supplicant sent.

12.7.6.4 4-way handshake message 3

Insert the following text as shown to the list beginning "Key Data =".

Key Data =

- ...
- Additionally, contains an OCI KDE when dot11RSNAOperatingChannelValidationActivated is true on the Authenticator.
- Additionally, may include a Device ID KDE, subject to the conditions in 12.2.13.1.
- Additionally, may include a PASN ID KDE.
- Addtionally, may include an IRM KDE subject to the conditions in 12.2.13.2.
- The RSNXE that the Authenticator sent in its Beacon or Probe Response frame, if this element is present in the Beacon or Probe Response frame that the Authenticator sent.

12.7.6.5 4-way handshake message 4

Change the following text as shown.

Key Data Length = length of Key Data field in octets

Key Data = includes an IRM KDE when dot11IRMActivated is true, otherwise, none required; RSNEs and Multi-band elements shall not be included

12.13.2 Discovery of a PASN capable AP

Change the following text as shown.

An AP indicates it is capable of performing PASN authentication by including the PASN AKMP as part of the RSNE included in Beacon and Probe Response frames. When PASN AKMP is advertised, the AP shall also include at least one additional AKMP in the RSNE unless it allows PTKSA derivation without authentication using the ephemeral keys exchanged during PASN authentication. When the PASN AKMP is advertised, an AP with dot11KEKPASNActivated equal to true shall also include 00-0F-AC:26 if AES-SIV is supported as the key wrap algorithm for KEK.

12.13.3 Key establishment with PASN authentication

12.13.3.2 PASN frame construction and processing

Change the following text as shown.

If non-AP STA chooses to initiate PASN authentication, it first selects the following authentication parameters:

- Base AKMP from among AKMPs advertised by the AP or provisioned by a higher layer (applicable for STAs co-located with NGV STAs (see 31.4 (NGV ranging)) if RSNA authentication is desired.

Otherwise, if dot11NoAuthPASNActivated is true, Base AKMP chosen is the PASN AKMP or PASN with defined key wrap AKMP, indicating that PTKSA is to be established without mutual authentication, that is, without a corresponding PMKSA.

Insert the following text as shown at the end of the list that begins: "The first PASN authentication frame (see 9.3.3.11) of the exchange is constructed as follows:"

— If dot11DeviceIDActivated is true, including a PASN ID element as defined in 9.4.2.320, if required per the procedure in 12.2.13.1.

Change the following text as shown in the list below "Upon receiving the first PASN frame, the AP:"

— Verifies the public key as specified in 5.6.2.3 of NIST SP 800-56A R2. If verification fails, the processing status is set to INVALID_PUBLIC_KEY. Verifies that a PMKSA named via a PMKID in the RSNE exists for the specified Base AKMP, or the Base AKMP is set to PASN AKMP or PASN with defined key wrap AKMP or Base AKMP data exists in the frame to allow a PMK to be established. If Base AKMP is equal to PASN AKMP or PASN with defined key wrap AKMP, verifies that dot11NoAuthPASNActivated is set to true. Otherwise processing status is set to REFUSED.

NOTE 1—If dot11DeviceIDActivated is true, it processes the device ID in a Device ID element following the rule defined in 12.2.13.1.

Insert the following text as shown in the list that begins: "— Derives the PTKSA; see 12.13.8." just before the list element beginning "A MIC element"

— If dot11DeviceIDActivated is true, including a PASN ID element and optionally a Device ID element as defined in 9.4.2.320 and 9.4.2.316 in the PASN Encrypted Data element, if required per the procedure in 12.2.13.1. The PASN Encrypted Data element shall be encrypted as defined in 12.13.11

— if dot11IRMActivated is true, including an IRM element as defined in 9.4.2.317 in the PASN Encrypted Data element, if required per the procedure in 12.2.13.2. The PASN Encrypted Data element shall be encrypted as defined in 12.13.11.

Change the following text as shown in the list below "Upon receiving the second PASN frame, the non-AP STA:"

— Verifies that a PMKSA named via a PMKID in the RSNE exists for the specified Base AKMP, or the Base AKMP is set to PASN AKMP or PASN with defined key wrap AKMP or Base AKMP data exists in the frame to allow a PMK to be established. If base AKMP is equal to PASN AKMP or PASN with defined key wrap AKMP, verifies that dot11NoAuthPASNActivated is set to true.

— If dot11DeviceIDActivated is true and the PASN frame is from an AP that indicated support for the device ID mechanism in its Beacon or Probe Response frame(s), it validates that a PASN Encrypted Data element is present and checks the decryption operation result. If the decryption operation returns failure, the non-AP STA silently discards the second PASN frame.

NOTE 2—The device ID in the Device ID element is processed by following the rule defined in 12.2.13.1.

— If dot11IRMActivated is true, it validates that a PASN Encrypted Data element is present and checks the decryption operation result. If the decryption operation returns failure, the non-AP STA silently discards the second PASN frame.

NOTE 3—The IRM in the IRM element is processed by following the rule defined in 12.2.13.2.

Insert the following text as shown in the list that begins: "Otherwise the STA begins the construction of the third PASN frame as follows:" just before the list element beginning "A MIC element"

— If dot11IRMActivated is true and the PASN frame is from an AP that indicated support for the IRM mechanism in its Beacon or Probe Response frame(s), including an IRM element as defined in 9.4.2.317 in a PASN Encrypted Data element, if required per the procedure in 12.2.13.2. The PASN Encrypted Data element shall be encrypted as defined in 12.2.13.

Insert the following text to the end of the list that begins "Upon receiving the third PASN frame, the AP:"

— If dot11DeviceIDActivated is true and the PASN frame is from an AP that indicated support for the device ID mechanism in its Beacon or Probe Response frame(s), it validates that a PASN Encrypted Data element is present and checks the decryption operation result. If the decryption operation returns failure, the AP silently discards the third PASN frame.

NOTE 4—The device ID in the Device ID element is processed by following the rule defined in 12.2.13.1.

— If dot11IRMActivated is true and the PASN frame is from an AP that indicated support for the IRM mechanism in its Beacon or Probe Response frame(s), it validates that a PASN Encrypted Data element is present and checks the decryption operation result. If the decryption operation returns failure, the AP silently discards the third PASN frame.

NOTE 5—The IRM in the IRM element is processed by following the rule defined in 12.2.13.2.

12.13.8 PTKSA derivation with PASN authentication

Change the following text as shown.

For PTKSA key derivation, the inputs to the PRF are the PMK of the PMKSA, a constant label and a concatenation of non-AP STA's MAC address, AP's BSSID and the DH shared secret from the ephemeral exchange.

PTK = KDF-HASH-NNN (PMK, "PASN PTK Derivation", SPA || BSSID || DHss)

where

PMK	is the pairwise master key for the base AKMP if the AKMP is ~~other than~~ neither PASN AKMP nor PASN with defined key wrap AKMP; see 9.4.2.23.3. Otherwise, if the base AKMP is PASN AKMP or PASN with defined key wrap AKMP, that is, the PASN PTKSA is being setup without mutual authentication in a non-RSN, the PMK shall be set to the string "PMKz" padded with 28 0s. NOTE—The PMK for the derivation can come from a cached PMKSA for the AKMP or from the PMKSA established with PASN by tunneling Wrapped Data or Authentication frames.
DHss	is the shared secret derived from the PASN ephemeral key exchange encoded as an octet string (12.4.7.2.2).
KDF-HASH-NNN	is the key derivation function defined in 12.7.1.6.2 using the hash algorithm defined for the base AKMP; see Table 9-190. When there is no base AKMP, the hash algorithm is selected based on the pairwise Cipher Suite provided in the RSNE provided by the AP in the second PASN frame. SHA-256 is used as the hash algorithm, except for the ciphers 00-0F-AC:9 and 00-0F-AC:10 for which SHA-384 is used.
NNN	is the number of b~~B~~its required for KCK, KEK, TK and KDK depending on the pairwise cipher and whether a KEK and a KDK ~~is~~ are derived.

When dot11KEKPASNActivated is not true, orwhen dot11KEKPASNActivated is true and the KEK In PASN field in the RSNXE from the peer is 0, a PTK is composed of the Key Confirmation Key (KCK), the Temporal Key (TK) and the Key Derivation Key (KDK) which are derived as follows:

Insert the following text at the end of 12.13.8 as shown.

When dot11KEKPASNActivated is true and the KEK In PASN field in the RSNXE from the peer is 1, a PTK is composed of the KCK, the KEK, the TK and the KDK which are derived as follows (see Table 12-11):

KCK = ExtractBits(PTK, 0, 256)

KEK = ExtractBits(PTK, 256, KEK_bits)

The KEK is used to provide encryption for the PASN Encrypted Data element in PASN frames, as defined in 12.13.3.2. Its length is defined in Table 12-11.

TK = ExtractBits(PTK, 256 + KEK_bits, TK_Length_Bits)

The TK is the transient key whose length is the same as a key for the pairwise cipher in the RSNE provided by the AP in the second PASN frame. TK_Length_Bits is the TK_bits in Table 12-8 (Cipher suite key lengths).

KDK = ExtractBits(PTK, 256 + KEK_bits + TK_Length_Bits, KDK_bits)

The KDK is of bit length KDK_bits which has the value 256 if a KDK is derived (see 12.7.1.3) or 0 otherwise.

The KDK shall be derived if dot11SecureLTFImplemented is true and the peer STA has indicated Secure HE-LTF support capability in its Extended RSN Capabilities field.

The Key ID in the PTKSA (see 12.6.1.1.6) resulting from PASN authentication shall be 0.

Insert the following new subclause after 12.13.10 (i.e. immediately before 12.14)

12.13.11 Encrypting the Encrypted Data field for PASN

The Encrypted Data field of the PASN Encrypted Data element shall be encrypted in the second PASN frame (if present) and in the third PASN frame (if present).

The KEK, as derived from the PTK (see 12.13.8), shall be used with the negotiated key wrap algorithm to encrypt the Encrypted Data field of the PASN Encrypted Data element.

If the size of the Encrypted Data field is larger than 254 octets, then the Encrypted Data field shall be encrypted first, then element fragmentation as defined in 10.28.11 shall be performed.

If the Encrypted Data field uses the NIST AES key wrap, then the Encrypted Data field shall be padded before encrypting if the length of the Encrypted Data field is nonzero and less than 16 octets, or if it is not a multiple of 8 octets. The padding consists of appending a single octet 0xdd followed by zero or more 0x00 octets. When processing a received PASN Encrypted Data element, the receiver shall ignore this trailing padding.

If the Encrypted Data field uses an AEAD cipher, the Encrypted Data field shall not be padded and the AAD for the encipherment operation shall not be used and the number of AAD components is zero.

13. Fast BSS Transition

13.4.2 FT initial mobility domain association in an RSN

Change the following text as shown.

The R1KH and S1KH then perform an FT 4-way handshake. The EAPOL-Key PDU notation is defined in 12.7.4 (EAPOL-Key PDU notation).

R1KH->S1KH: EAPOL-Key(0, 0, 1, 0, P, 0, 0, ANonce, 0, {})
S1KH->R1KH: EAPOL-Key(0, 1, 0, 0, P, 0, 0, SNonce, MIC, {RSNE(PMKR1Name) [, RSNXE], MDE, FTE [, Device ID]})
R1KH->S1KH: EAPOL-Key(1, 1, 1, 1, P, 0, 0, ANonce, MIC, {RSNE(PMKR1Name) [, RSNXE], [, OCI], MDE, FTE, TIE(ReassociationDeadline), TIE(KeyLifetime), GTK(N) [, IGTK(M, IPN)] [, BIGTK(Q, BIPN)] [, WIGTK(R, WIPN)] [, Device ID] [, IRM] [, PASN ID]})
S1KH->R1KH: EAPOL-Key(1, 1, 0, 0, P, 0, 0, 0, MIC, {[IRM]})

Annex B

(normative)

Protocol Implementation Conformance Statement (PICS) proforma

B.2 Abbreviations and special symbols

B.2.2 General abbreviations for Item and Support columns

Insert the following entry in alphabetical order:

ID identifier

IRM identifiable random MAC address

B.4 PICS proforma—IEEE Std 802.11-2020[6]

B.4.3 IUT Configuration

Insert two new entries in the table (header row shown for convenience):

Item	IUT configuration	References	Status	Support
CFDID	Device ID	12.2.13.1	PC34 AND CFAP:O PC34 AND CFSTAofAP: O	Yes ☐ No ☐
CFIRM	IRM	12.2.13.2	PC34 AND CFAP:O PC34 AND CFSTAofAP: O	Yes ☐ No ☐

[6]*Copyright release for PICS proforma:* Users of this standard may freely reproduce the PICS proforma in this annex so that it can be used for its intended purpose and may further publish the completed PICS.

B.4.4.2 MAC frames

Insert two new entries in the table (header row shown for convenience):

Item	MAC frame	References	Status	Support
FT74	IRM Action	9.6.36	CFIRM:O	Yes ☐ No ☐
FR75	IRM Action	9.6.36	CFIRM:O	Yes ☐ No ☐

Annex C

(normative)

ASN.1 encoding of the MAC and PHY MIB

C.3 MIB detail

Insert the following entries to the end of the "Dot11StationConfigEntry" of the "dot11StationConfig TABLE" as follows:

```
…,
       dot11KEKPASNActivated                    TruthValue,
       dot11DeviceIDActivated                   TruthValue,
       dot11IRMActivated                        TruthValue

}
```

Insert the following elements at the end of the dot11StationConfigTable element definitions:

```
dot11KEKPASNActivated OBJECT-TYPE
   SYNTAX TruthValue
   MAX-ACCESS read-write
   STATUS current
   DESCRIPTION
      "This is a control variable. It is written by an external management
      entity or the SME. Changes take effect as soon as practical in the
      implementation.
      This attribute, when true, indicates support for deriving KEK in PASN."
   DEFVAL { false }
   ::= { dot11StationConfigEntry 235 }

dot11DeviceIDActivated OBJECT-TYPE
   SYNTAX TruthValue
   MAX-ACCESS read-write
   STATUS current
   DESCRIPTION
      "This is a control variable. It is written by an external management
      entity or the SME. Changes take effect as soon as practical in the
      implementation.
      This attribute, when true, indicates that the device ID mechanism is
      supported."
   DEFVAL { false }
   ::= { dot11StationConfigEntry 236 }


dot11IRMActivated OBJECT-TYPE
   SYNTAX TruthValue
   MAX-ACCESS read-write
   STATUS current
   DESCRIPTION
      "This is a control variable. It is written by an external management
      entity or the SME. Changes take effect as soon as practical in the
      implementation. This attribute, when true, indicates that the IRM
      mechanism is supported."
   DEFVAL { false }
   ::= { dot11StationConfigEntry 237 }
```

Insert the following Annexes after Annex AE.

Annex AF

(informative)

Example of an opaque identifier scheme

AF.1 General

This annex provides an example scheme for generating opaque identifiers suitable for use in the PASN ID field of the PASN ID element (see 9.4.2.320) as used in the procedure defined in 12.2.13.1. These procedures require that the identifier precludes tracking by third parties. In addition to satisfying this requirement, this scheme also provides for countermeasures to deal with traffic analysis, precludes cutting-and-pasting of identities into conversations, prevents the same identifier from being used on multiple ESSs, and has an acceptable security level based on the birthday paradox. It uses symmetric cryptography for speed and DoS resistance. It imposes minimal overhead on each frame that contains a PASN ID, imposes minimal state retention requirements on an ESS (a single secret), and establishes a binding of each unwrapped identity assigned to a STA and the current opaque identifier provided to it.

Opaque identifiers are generated and processed by APs. To a non-AP STA they are indistinguishable from a random string and have no significance.

AF.2 Generation of opaque identifiers

The identifier generation scheme takes a unique identifier as input and uses AES-SIV in deterministic mode to wrap the identifier to produce output.

There is a single symmetric secret, k, shared by all APs in an ESS. The length of k is 256 bits if AES-SIV-256 is used or 512 bits if AES-SIV-512 is used. In either case, the procedure is to prepend the identifier with a single octet indicating the number of random octets of padding that follow. The amount of random padding to add varies and its variability determines the resistance to traffic analysis that this scheme provides. For example, if there are 4 octets of padding added to mitigate traffic analysis, the identifier, *id*, might be padded as:

padded-id = 0x04 0xc8 0x34 0x9a 0x70 <id>

If there is no padding, a single zero octet is prepended to the identifier.

The *padded-id* is prepended with a variable length input comprised of random octets called a tweak. The length of the tweak in bits, n, determines the baseline security of the scheme such that the probability of a duplicate identifier being generated, assuming a worst case of no padding, would be $1/2^{(n/2)}$. Padding of the tweaked identifier increases the security of the scheme.

The overhead of the scheme is 17 octets (1 for the pad indicator and 16 for the SIV tag) plus padding and plus the size of the tweak. Device identifiers that are greater than 233 octets cannot be made opaque using this scheme.

NOTE—233 octets is the maximum size of a device ID with no padding and no tweak minus the overhead. The resulting opaque identifier needs to fit in a Device ID KDE.

For example, an 8 octet tweak would provide collision resistance of at least $1/2^{32}$ (in addition to that provided by the padding) and the *tweaked-padded-id* would be constructed as (assuming the values of the tweak are generated according to Annex J.5):

tweaked-padded-id = 0x7e 0x17 0x54 0x82 0xf1 0xd0 0xaa 0x52 0x04 0xc8 0x34 0x9a 0x70 <id>

The *tweaked-padded-id* is then passed to AES-SIV in deterministic mode as plaintext using *k* as a key to produce the opaque identifier.

AF.3 Processing of opaque identifiers

All APs in an ESS need to use the same tweak length for all opaque identifiers that are generated and parsed.

APs that receive opaque identifiers using the procedures described in 12.2.13 (Identifying a non-AP STA with changing MAC address), pass the opaque identifier to AES-SIV with key *k*. If AES-SIV returns FAIL, the protocol using the opaque identifier fails. If AES-SIV returns a plaintext, the (known-length) tweak is removed and the next octet, the pad length, is inspected to determine how many additional octets are removed to recover the original identifier, *id*. This identifier is checked to validate that the received opaque identifier is the current one associated with the identifier. If so, the unwrapped identity is passed up to the protocol using the scheme with an indication of success. If not, the protocol using the opaque identifier is notified of the failure and no identifier is passed up.

AF.4 Using opaque identifiers

An AP that receives an opaque identifier extracts the original identity and generates a new opaque identifier for the STA. A new opaque identifier is generated with a pad length that differs from the pad length of the previously wrapped identifier.

The AP associates the new opaque identifier with the non-AP STA’s identity.

AF.5 Security of scheme

The security guarantees of AES-SIV mean that it is computationally infeasible for an adversary to generate a valid opaque identifier that could be processed by an AP and it is computationally infeasible for an adversary to decrypt a valid opaque identifier.

Assuming the combination of tweak and pad are never repeated for a given identifier, the probability of a given identity producing an opaque device identity that has been used already is at least $1/2^{(n/2)}$ where *n* is the number of bits of tweak. The AP might use different amounts of padding each time an identity is wrapped.

The overhead added to each frame by the scheme is 16 octets of AES-SIV tag plus length of tweak plus one octet of padding indication plus padding.

Annex AG

(informative)

Examples of device ID and IRM usage

AG.1 Examples of device ID usage

Figure AG-1 shows an example of a device ID exchange when a non-AP STA authenticates and associates to APs (AP-1 and AP-2 belonging to the same ESS) using a 4-way handshake.

AP-1 and AP-2 advertise their support of device ID in the RSNXE in beacons and probe responses.

The non-AP STA with a MAC address of MAC1 initiates the first connection with AP-1, i.e., the non-AP STA does not have a device ID for that ESS.

After the authentication frame exchange, the non-AP STA indicates its activation of device ID by setting the Device ID Support field in the RSNXE to 1 in the association request. Similarly, AP-1 indicates its activation of device ID by setting the Device ID Support field in the RSNXE to 1 in the association response. In 4-way handshake message 3, AP-1 includes a Device ID KDE and PASN ID KDE and assigns a device ID (devID) and a PASN ID (pasnID1) to the non-AP STA. The non-AP STA, AP-1, and AP-2 store devID and pasnID1.

Later, the non-AP STA terminates the connection with AP-1.

The non-AP STA then returns to that same ESS using a different MAC address (MAC2), again indicating activation of device ID in the Association Request/Response frame exchange. The non-AP STA then provides the previously assigned device ID (devID) to AP-2 in a Device ID KDE in 4-way handshake message 2.

AP-2 identifies the non-AP STA from the device ID (devID) despite the non-AP STA using a randomized MAC address (MAC2). AP-2 then sends a Device ID KDE in 4-way Handshake Message 3 with the Device ID Status field set to 0 indicating that the device ID has been recognized.

AP-2 does not allocate a new device ID in the Device ID KDE sent in 4-way handshake message 3, implying that the same device ID (devID) will be used subsequently.

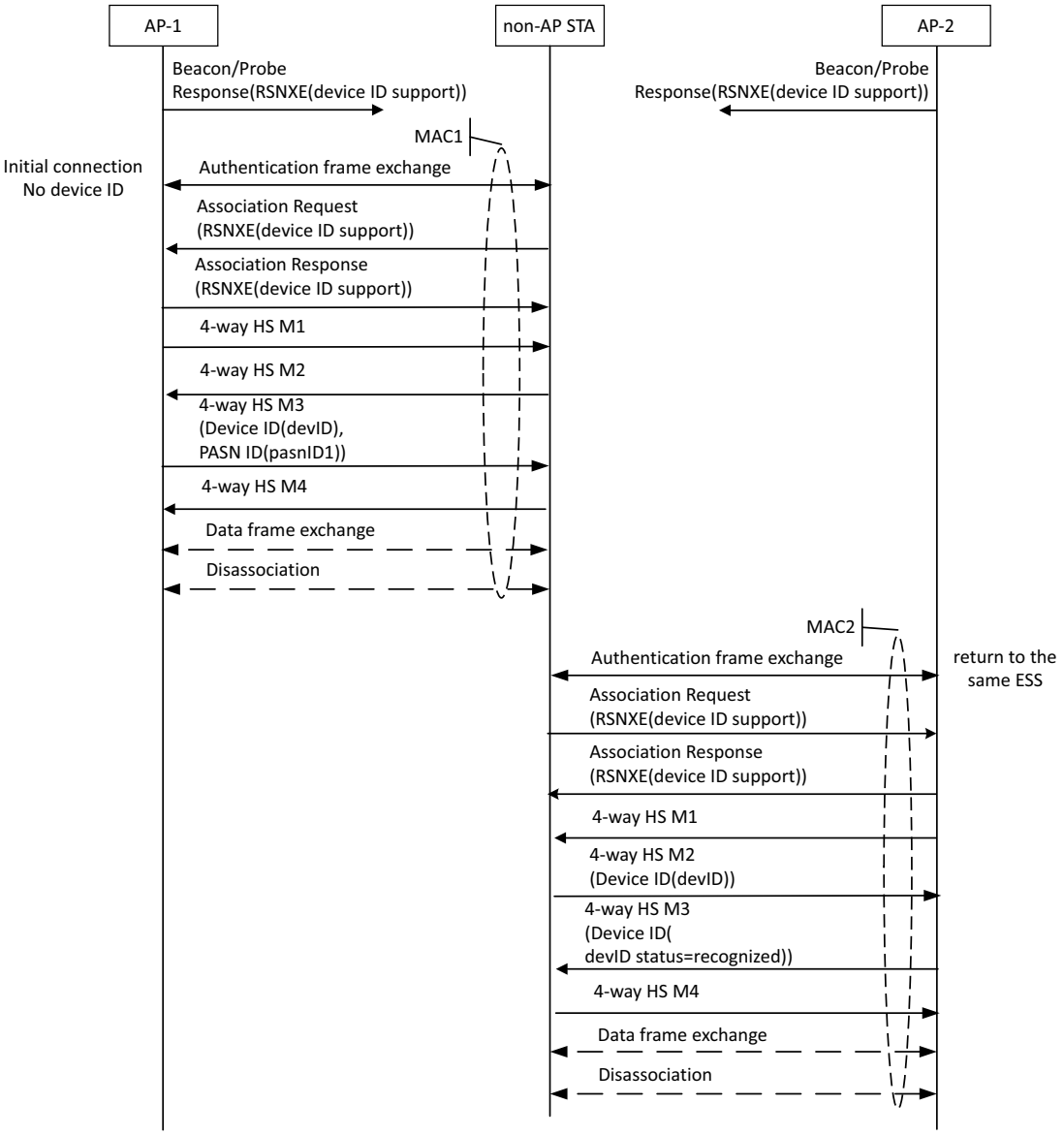

Figure AG-1—Example of device ID exhanges in PASN

Figure AG-2 shows an example of a device ID exchange when a non-AP STA associates to APs (AP-1 and AP-2 belonging to the same ESS) using FILS public key with PFS.

AP-1 and AP-2 advertise their support of device ID in the RSNXE in beacons and probe responses.

The non-AP STA with a MAC address of MAC1 initiates the first connection with AP-1. The non-AP STA does not have a device ID for that ESS. After the FILS authentication frame exchange, the non-AP STA indicates its activation of device ID by setting the Device ID Support field in the RSNXE to 1 in the association

request. Similarly, the AP-1 indicates its activation of device ID by setting the Device ID Support field in the RSNXE to 1 in the association response.

In the association response, AP-1 includes a Device ID element and a PASN ID element and assigns a device ID (devID1) and a PASN ID (pasnID1) to the non-AP STA. The non-AP STA, AP-1, and AP-2 store devID1 and pasnID1.

Later, the non-AP STA terminates the connection with AP-1.

The non-AP STA then returns to that same ESS using a different MAC address (MAC2), again indicating activation of device ID in the association request.

The non-AP STA then provides the previously assigned device ID (devID1) to AP-2 in a Device ID element in the association request. Because of devID1, AP-2 identifies the non-AP STA from the device ID (devID1) despite the non-AP STA using a randomized MAC address (MAC2).

AP-2 then sends a Device ID element in the association response with the Device ID Status field set to 0 indicating that the device ID has been recognized. (Notice the device ID activation from AP-2 via the Association Response frame as well).

In the Figure AX-2, AP-2 optionally allocates a new device ID (devID2) and a PASN ID (pasnID2) in the Device ID element and in the PASN ID element sent in the association response.

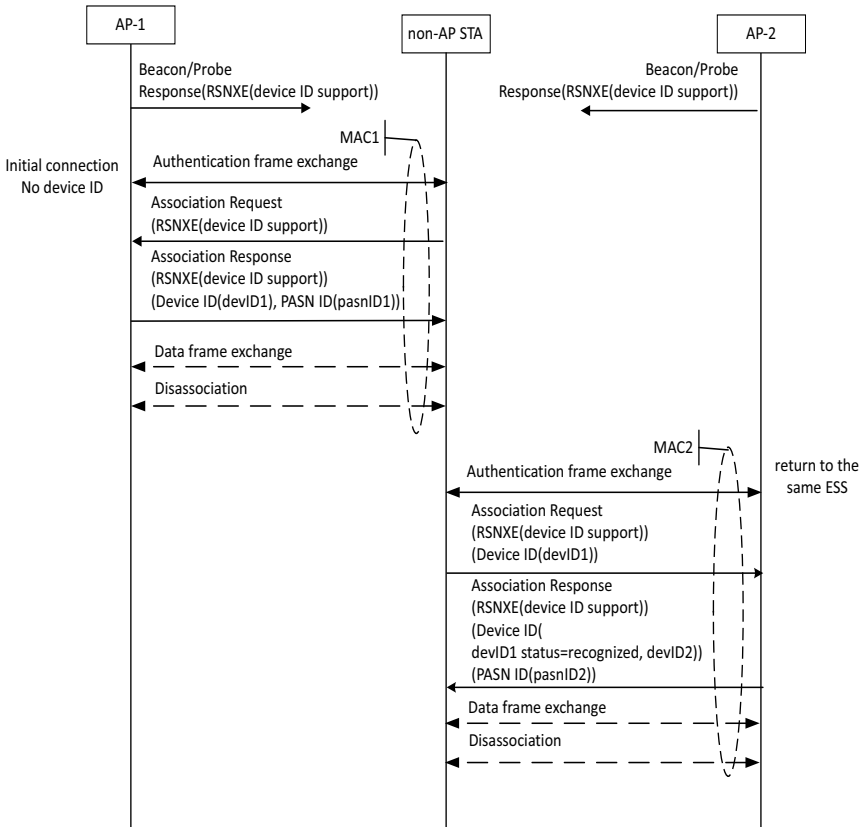

Figure AG-2—Example of device ID exchange in FILS

Figure AG-3 shows an example of a device ID and PASN ID exchange in PASN. The example illustrates a non-AP STA performing PASN to establish FTM session(s) in an ESS containing AP-1 and AP-2.

AP-1 and AP-2 advertise their support of device ID in the RSNXE in beacons and probe responses.

The non-AP STA with a MAC address of MAC1 first initiates a connection with AP-1 by sending the first PASN frame with the Device ID Support field in the RSNXE set to 1 but does not include a PASN ID.

Upon receiving the first PASN frame, AP1 indicates its activation of device ID by setting the Device ID Support field and PASN ID Active in the RSNXE to 1. AP-1 then assigns a device ID (devID) and a PASN ID (pasnID1) and sends them to the non-AP STA in the Device ID field in the Device ID element and in the PASN ID field in the Robust PASN ID element in the PASN Encrypted Data element in the second PASN frame. The non-AP STA, AP-1 and AP-2 store devID and pasnID1.

The non-AP STA then continues to establish an FTM session with AP-1.

When the non-AP STA, now using a MAC address of MAC2 (the non-AP STA changing its MAC address from MAC1 to MAC2), performs PASN with AP-2 to establish another FTM session, the non-AP STA sends the previously assigned PASN ID (pasnID1) to AP-2 in the PASN ID field in an PASN ID element in the first PASN frame.

AP-2 identifies the non-AP STA from the PASN ID (pasnID1) despite the non-AP STA using a randomized MAC address (MAC2). Upon receiving the PASN ID (pasnID1) in the first PASN frame, AP-2 sends a Robust PASN ID element in the PASN Encrypted Data element in the second PASN frame with the PASN ID Status field set to 0, indicating that the PASN ID has been recognized. AP-2 then assigns another PASN ID (pasnID2) and sends it to the non-AP STA in the PASN ID field in the Robust PASN ID element included in the PASN Encrypted Data element in the second PASN frame.

The non-AP STA then proceeds to establish the FTM session.

Similarly, when the non-AP STA with a MAC address of MAC3 returns to AP-1, it sends the previously assigned PASN ID (pasnID2) and is assigned another PASN ID (pasnID3) that will be used in the subsequent PASN for another FTM session.

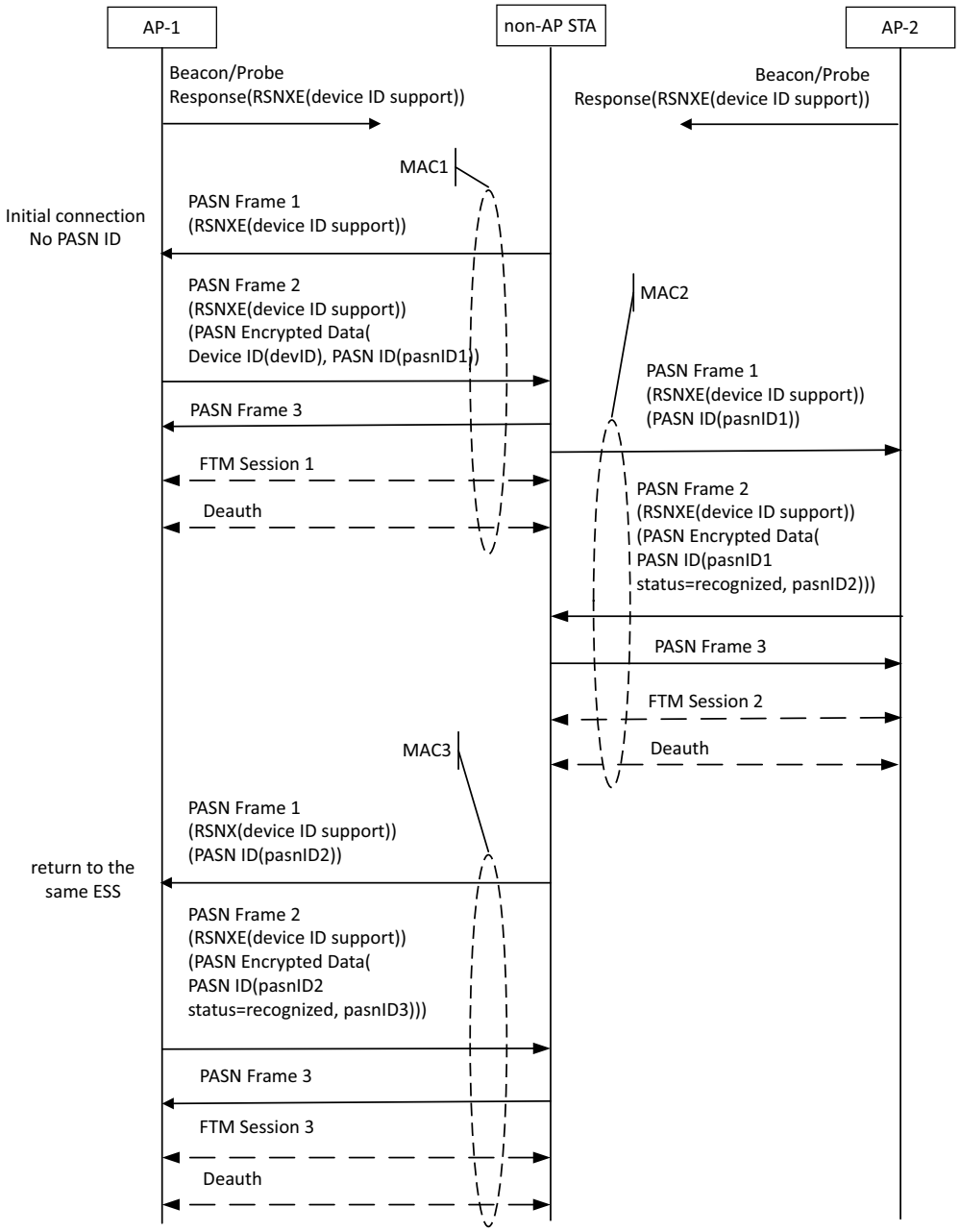

Figure AG-3—Example of device ID and PASN ID exchange in PASN

AG.2 Examples of IRM Usage

Figure AG-4 shows an example of an IRM exchange when a non-AP STA authenticates and associates to APs (AP-1 and AP-2 belonging to the same ESS) using 4-way handshake.

AP-1 and AP-2 advertise their support of IRM in the RSNXE in beacons and probe responses.

The non-AP STA with a MAC address of MAC1 initiates a first connection with AP-1. The non-AP STA has not previously provided an IRM to that ESS. After the authentication frame exchange, the non-AP STA indicates its activation of IRM by setting the IRM Support field in the RSNXE to 1 in the association request. Similarly, AP-1 indicates its activation of IRM by setting IRM Support field in the RSNXE to 1 in the association response. In 4-way handshake message 4, the non-AP STA includes an IRM KDE and provides an IRM (IRM1) to AP-1. The non-AP STA, AP-1, and AP-2 store that IRM (IRM1).

Later, the non-AP STA terminates the connection with AP-1.

When non-AP STA returns to that same ESS, the non-AP STA uses IRM1 as its MAC address. AP-2 identifies the non-AP STA from the stored IRM1. AP-2 then sends an IRM KDE in 4-way handshake message 3 with the IRM Status field set to 0 indicating that the IRM has been recognized. The non-AP STA then provides another IRM (IRM2) to AP-2 in an IRM KDE in 4-way handshake message 4.

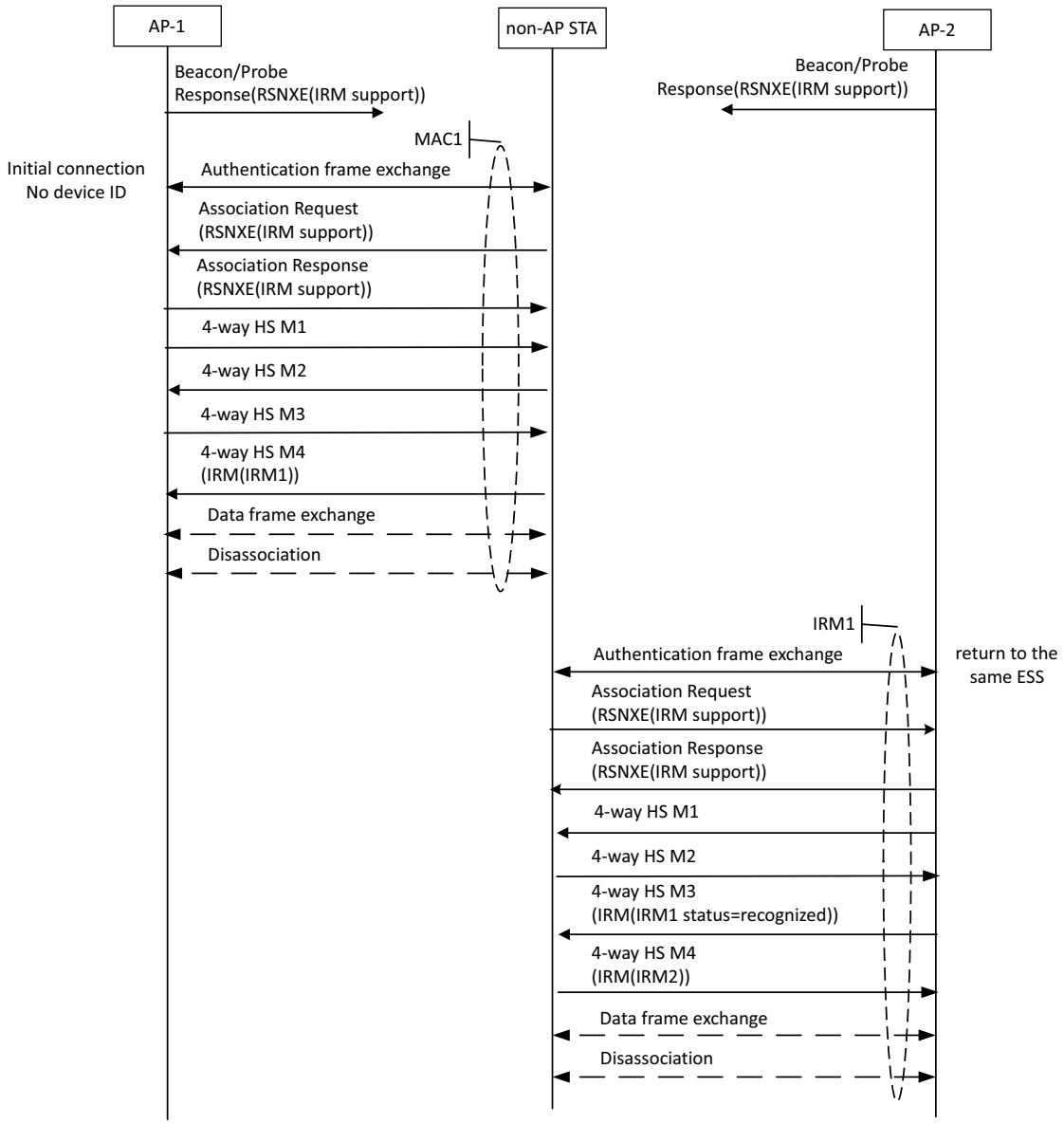

Figure AG-4—Example of IRM exchange in 4-way handshake

Figure AG-5 shows an example of an IRM exchange when a non-AP STA associates to APs (AP-1 and AP-2 belonging to the same ESS) using FILS public key with PFS.

AP-1 and AP-2 advertise their support of IRM in the RSNXE in Beacons or Probe Responses.

The non-AP STA with a MAC address of MAC1 initiates a first connection with AP-1. The non-AP STA has not previously provided an IRM to that ESS. After the FILS authentication frame exchange, the non-AP STA indicates its activation of IRM by setting the IRM Support field in the RSNXE to 1 in the association request. In an association request, the non-AP STA assigns an IRM (IRM1) to itself in an IRM element. AP-1 also indicates its activation of IRM by setting the IRM Support field in the RSNXE to 1 in the association response. The non-AP STA, AP-1, and AP-2 store IRM1.

Later, the non-AP STA terminates the connection with AP-1.

When non-AP STA returns to that same ESS, the non-AP STA uses IRM1 as its MAC address. AP-2 identifies the non-AP STA from the stored IRM1. AP-2 then sends an IRM element in the association response with the IRM Status field set to 0 indicating that the IRM has been recognized. The non-AP STA then provides another IRM (IRM2) to AP-2 in an IRM element in association request.

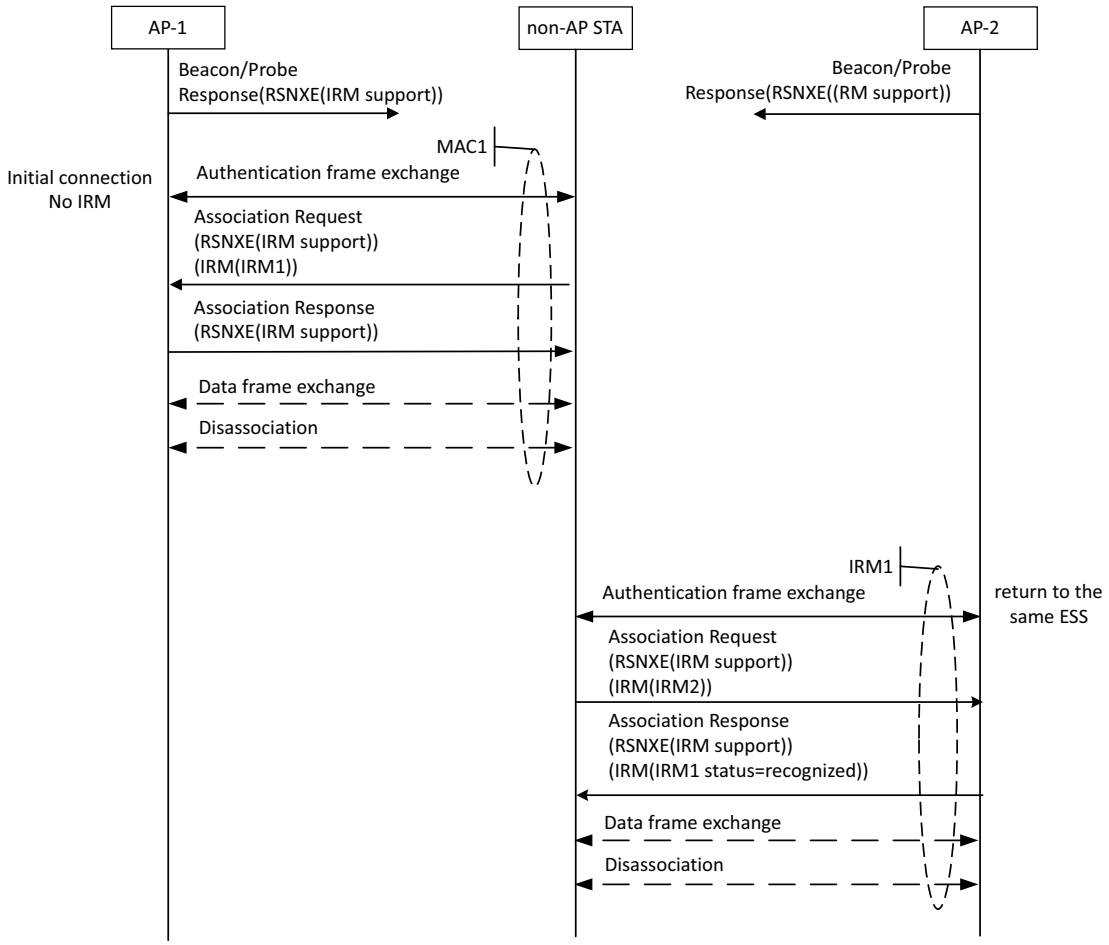

Figure AG-5—Example of IRM exchange in FILS

Figure AG-6 shows an example of a IRM exchange in PASN. The example illustrates a non-AP STA performing PASN to establish FTM session(s) in an ESS containing AP-1 and AP-2.

AP-1 and AP-2 advertise their support of IRM in the RSNXE in beacons and probe responses.

The non-AP STA with a MAC address of MAC1 first initiates the connection with AP-1 by sending the first PASN frame with the IRM Support field in the RSNXE set to 1.

Upon receiving the first PASN frame, AP-1 indicates its activation of IRM by setting the IRM Support field in the RSNXE to 1. In the third PASN frame, the non-AP STA provides an IRM (IRM1) to AP-1 sending it to AP1 in the IRM field in an Robust IRM element in the PASN Encrypted Data element. The non-AP STA, AP-1 and AP-2 store IRM1. The non-AP STA then continues to establish an FTM session with AP-1. [

When the non-AP STA performs PASN with AP-2 to establish another FTM session, the non-AP STA uses IRM1 as its MAC address. AP-2 identifies the non-AP STA from the stored IRM1. Upon receiving IRM1 in the first PASN frame, AP-2 may send a Robust IRM element in the PASN Encrypted Data element in the second PASN frame with the IRM Status field set to 0, indicating that the IRM has been recognized. The non-AP STA then provides another IRM (IRM2) to AP-2 in the IRM field in a Robust IRM element in PASN Encrypted Data element in the third PASN frame.

Similarly, when the non-AP STA returns to AP-1, it uses the previously assigned IRM (IRM2) as its MAC address and provides another IRM (IRM3) that will be used in the subsequent PASN for another FTM session.

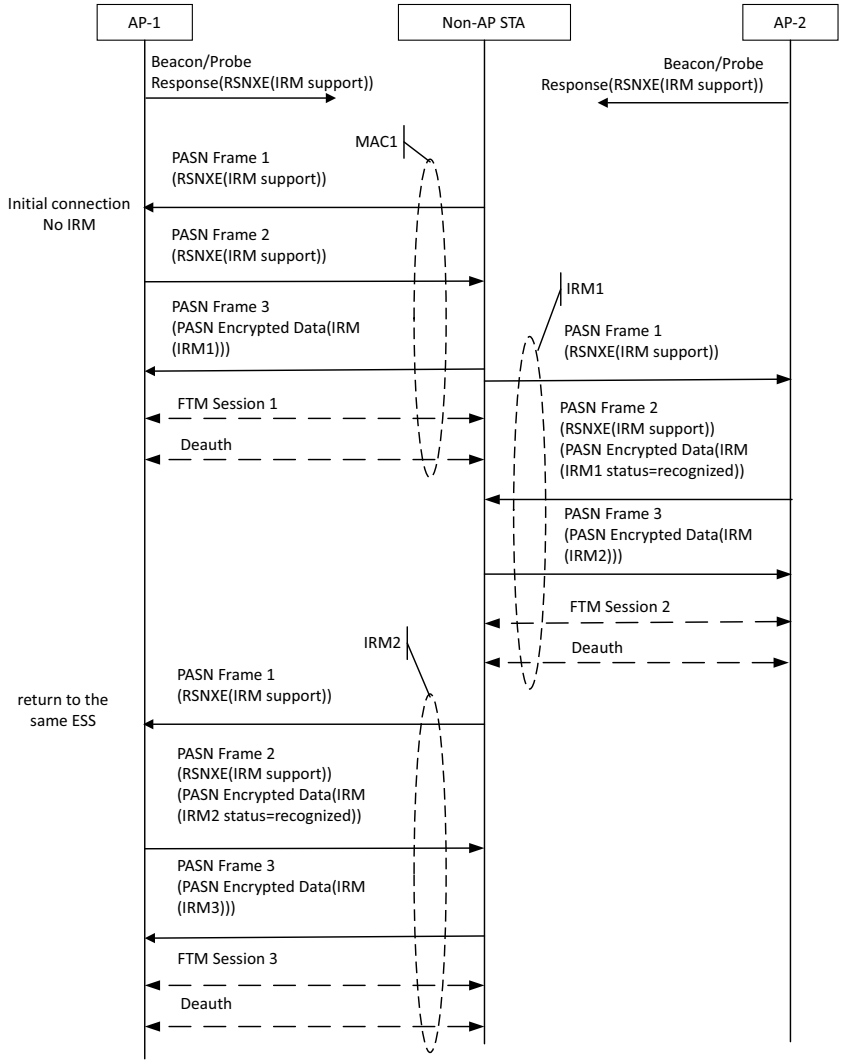

Figure AG-6—Example of IRM exchange in PASN

AG.3 Example of device ID and IRM usage

Figure AG-7 shows an example of a simultaneous exchange of device ID and IRM in 4-way handshake for APs (AP-1 and AP-2 belonging to the same ESS).

AP-1 and AP-2 advertise their support of device ID and IRM in the RSNXE in beacons and probe responses.

The non-AP STA with a MAC address of MAC1 initiates the first connection with AP-1. The non-AP STA does not have a device ID and IRM for that ESS. After the authentication frame exchange, the non-AP STA indicates its activation of device ID and IRM by setting the Device ID Support field and IRM Support field in the RSNXE to 1 in the association request. Similarly, the AP-1 indicates its activation of device ID and IRM by setting the Device ID Support field and IRM Support field in the RSNXE to 1 in the association response.

In 4-way handshake message 3, AP-1 includes a Device ID KDE and PASN KDE and assigns a device ID (devID) and PASN ID (pasnID1) to the non-AP STA. In 4-way handshake message 4, the non-AP STA includes an IRM KDE and provides an IRM (IRM1) to AP-1. The non-AP STA, AP-1, and AP-2 store devID, pasnID1, and IRM1.

Later, the non-AP STA terminates the connection with AP-1.

When the non-AP STA returns to that same ESS, the non-AP STA uses IRM1 as its MAC address. AP-2 identifies the non-AP STA from the stored IRM1. The non-AP STA then provides the previously assigned device ID (devID) to AP-2 in a Device ID KDE in 4-way handshake message 2. AP-2 then sends an IRM KDE in 4-way handshake message 3 with the IRM Status field set to 0 indicating that the IRM has been recognized and sends a Device ID KDE with the Device ID Status field set to 0 indicating that the device ID has been recognized. The non-AP STA then provides another IRM (IRM2) to AP-2 in an IRM KDE in 4-way handshake message 4.

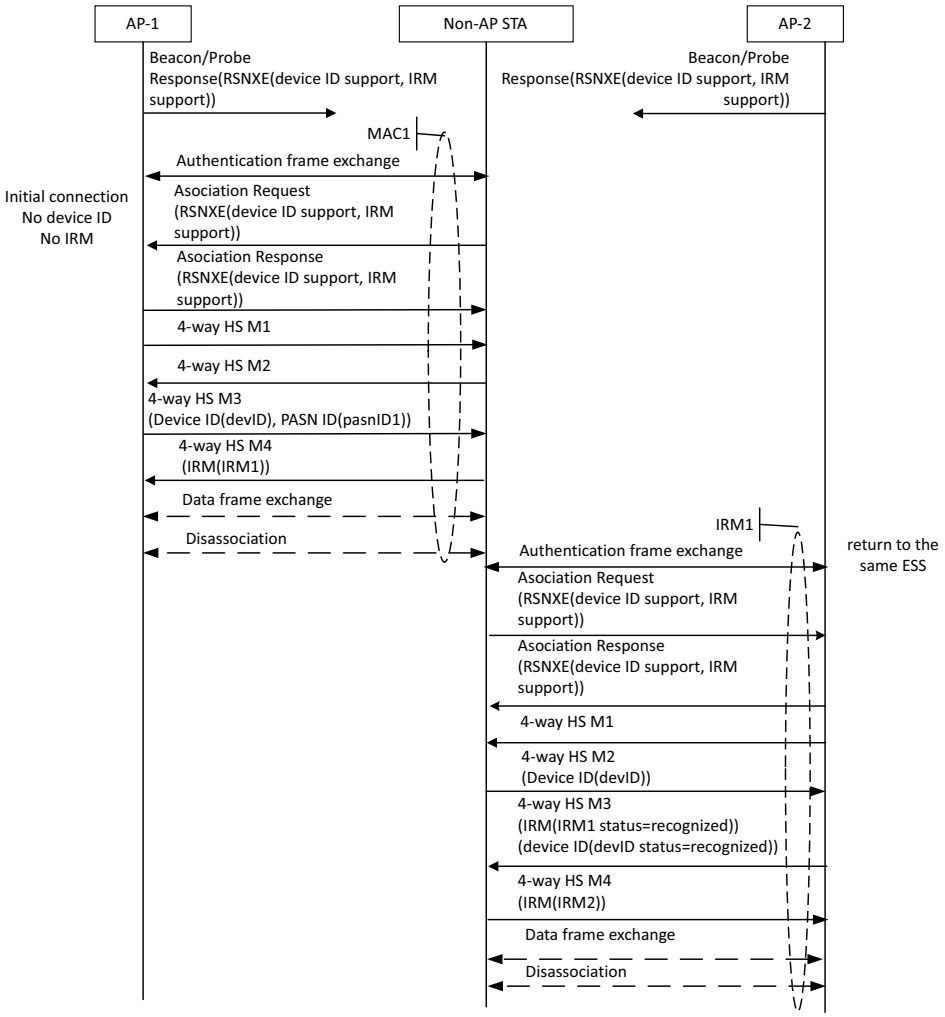

Figure AG-7—Example of device ID exchange and IRM exchange in 4-way handshake

IEEE SA
STANDARDS ASSOCIATION

RAISING THE WORLD'S STANDARDS

Connect with us on:

Facebook: facebook.com/ieeesa
LinkedIn: linkedin.com/groups/1791118
Beyond Standards blog: beyondstandards.ieee.org
YouTube: youtube.com/ieeesa

standards.ieee.org
Phone: +1 732 981 0060

IEEE