IEEE P™/D  
Draft for

Sponsor

**Committee**of the **IEEE Computer Society**

NOTE: This amendment is to be applied to the result of original 802.21-2008, 802.21a-2012, and 802.21b-2012.

Approved <XX MONTH 20XX>

**IEEE-SA Standards Board**

Copyright © 2012 by The Institute of Electrical and Electronics Engineers, Inc.

Three Park Avenue

New York, New York 10016-5997, USA

All rights reserved.

This document is an unapproved draft of a proposed IEEE Standard. As such, this document is subject to change. USE AT YOUR OWN RISK! Because this is an unapproved draft, this document must not be utilized for any conformance/compliance purposes. Permission is hereby granted for IEEE Standards Committee participants to reproduce this document for purposes of international standardization consideration. Prior to adoption of this document, in whole or in part, by another standards development organization, permission must first be obtained from the IEEE Standards Association Department (stds.ipr@ieee.org). Other entities seeking permission to reproduce this document, in whole or in part, must also obtain permission from the IEEE Standards Association Department.

IEEE Standards Association Department

445 Hoes Lane

Piscataway, NJ 08854, USA

Abstract: This standard specifies additional IEEE 802® media access independent mechanisms that optimize handovers between possibly heterogeneous IEEE 802 systems and between IEEE 802 systems and cellular systems, to enable improved handover performance for single-radio devices.

Keywords: < management, media independent handover, mobile node, mobility, seamless, point of attachment, point of service, single-radio, preregistration, proactive authentication

[[1]](#footnote-1)•

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

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

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

The existence of an IEEE Standard does not imply that there are no other ways to produce, test, measure, purchase, market, or provide other goods and services related to the scope of the IEEE Standard. Furthermore, the viewpoint expressed at the time a standard is approved and issued is subject to change brought about through developments in the state of the art and comments received from users of the standard. Every IEEE Standard is subjected to review at least every five years for revision or reaffirmation, or every ten years for stabilization. When a document is more than five years old and has not been reaffirmed, or more than ten years old and has not been stabilized, it is reasonable to conclude that its contents, although still of some value, do not wholly reflect the present state of the art. Users are cautioned to check to determine that they have the latest edition of any IEEE Standard.

In publishing and making this document available, the IEEE is not suggesting or rendering professional or other services for, or on behalf of, any person or entity. Nor is the IEEE undertaking to perform any duty owed by any other person or entity to another. Any person utilizing this, and any other IEEE Standards document, should rely upon his or her 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.

Interpretations: Occasionally questions may arise regarding the meaning of portions of standards as they relate to specific applications. When the need for interpretations is brought to the attention of IEEE, the Institute will initiate action to prepare appropriate responses. Since IEEE Standards represent a consensus of concerned interests, it is important to ensure that any interpretation has also received the concurrence of a balance of interests. For this reason, IEEE and the members of its societies and Standards Coordinating Committees are not able to provide an instant response to interpretation requests except in those cases where the matter has previously received formal consideration. A statement, written or oral, that is not processed in accordance with the IEEE-SA Standards Board Operations Manual shall not be considered the official position of IEEE or any of its committees and shall not be considered to be, nor be relied upon as, a formal interpretation of the IEEE. At lectures, symposia, seminars, or educational courses, an individual presenting information on IEEE standards shall make it clear that his or her views should be considered the personal views of that individual rather than the formal position, explanation, or interpretation of the IEEE.

Comments for revision of IEEE Standards are welcome from any interested party, regardless of membership affiliation with IEEE. Suggestions for changes in documents should be in the form of a proposed change of text, together with appropriate supporting comments. Recommendations to change the status of a stabilized standard should include a rationale as to why a revision or withdrawal is required. Comments and recommendations on standards, and requests for interpretations should be addressed to:

Secretary, IEEE-SA Standards Board

445 Hoes Lane

Piscataway, NJ 08854

USA

Authorization to photocopy portions of any individual standard for internal or personal use is granted by The Institute of Electrical and Electronics Engineers, Inc., provided that the appropriate fee is paid to Copyright Clearance Center. To arrange for payment of licensing fee, please contact Copyright Clearance Center, Customer Service, 222 Rosewood Drive, Danvers, MA 01923 USA; +1 978 750 8400. Permission to photocopy portions of any individual standard for educational classroom use can also be obtained through the Copyright Clearance Center.

Notice to users

Laws and regulations

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

Copyrights

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

Updating of IEEE documents

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

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

Errata

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

Patents

Attention is called to the possibility that implementation of this standard may require use of subject matter covered by patent rights. By publication of this standard, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. If a patent holder or patent applicant has filed a statement of assurance via an Accepted Letter of Assurance, then the statement is listed on the IEEE-SA website <http://standards.ieee.org/about/sasb/patcom/patents.html>. Letters of Assurance may indicate whether the Submitter is willing or unwilling to grant licenses under patent rights without compensation or under reasonable rates, with reasonable terms and conditions that are demonstrably free of any unfair discrimination to applicants desiring to obtain such licenses.

Essential Patent Claims may exist for which a Letter of Assurance has not been received. The IEEE is not responsible for identifying Essential Patent Claims for which a license may be required, for conducting inquiries into the legal validity or scope of Patents Claims, or determining whether any licensing terms or conditions provided in connection with submission of a Letter of Assurance, if any, or in any licensing agreements are reasonable or non-discriminatory. Users of this standard are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. Further information may be obtained from the IEEE Standards Association.

Participants

At the time this draft was submitted to the IEEE-SA Standards Board for approval, the Working Group had the following membership:

, *Chair*

, *Vice Chair*

Participant1

Participant2

Participant3

Participant4

Participant5

Participant6

Participant7

Participant8

Participant9

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

***(to be supplied by IEEE)***

Balloter1

Balloter2

Balloter3

Balloter4

Balloter5

Balloter6

Balloter7

Balloter8

Balloter9

When the IEEE-SA Standards Board approved this on <XX MONTH 20XX>, it had the following membership:

***(to be supplied by IEEE)***

**<Name>,** *Chair*

**<Name>,** *Vice Chair*

**<Name>,** *Past Chair*

**<Name>,** *Secretary*

SBMember1

SBMember2

SBMember3

SBMember4

SBMember5

SBMember6

SBMember7

SBMember8

SBMember9

\*Member Emeritus

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

<Name>, *DOE Representative*

<Name>, *NRC Representative*

<Name>

*IEEE Standards Program Manager, Document Development*

<Name>

*IEEE Standards Program Manager, Technical Program Development*

Introduction

This introduction is not part of IEEE P/D, Draft for .

This standard extends the media access independent mechanisms that enable the optimization of handovers between possibly heterogeneous IEEE 802 systems and may facilitate handovers between IEEE 802 systems and cellular systems. The extensions enable mobile devices with single-radio designs to improve handover latencies and avoid packet loss.

Contents

[1. Overview 2](#_Toc361333196)

[1.1 2](#_Toc361333197)

[1.2 2](#_Toc361333198)

[1.3 2](#_Toc361333199)

[1.4 Assumptions 2](#_Toc361333200)

[2. Normative references 2](#_Toc361333204)

[3. Definitions 2](#_Toc361333205)

[4. Abbreviations and Acronyms 3](#_Toc361333206)

[5. General architecture 4](#_Toc361333207)

[5.1 Introduction 4](#_Toc361333208)

[5.1.1 4](#_Toc361333209)

[5.1.2 4](#_Toc361333210)

[5.1.3 4](#_Toc361333211)

[5.1.4 4](#_Toc361333212)

[5.1.5 4](#_Toc361333213)

[5.1.6 4](#_Toc361333214)

[5.1.7 4](#_Toc361333215)

[5.1.8 4](#_Toc361333216)

[5.1.9 4](#_Toc361333217)

[5.1.10 Media independent single radio handover 4](#_Toc361333218)

[5.1.11 Securing Single-Radio messages using PoS 5](#_Toc361333219)

[5.2 General design principles 5](#_Toc361333220)

[5.2.1 5](#_Toc361333221)

[5.2.2 5](#_Toc361333222)

[5.2.3 Single Radio Handover MIHF design principles 5](#_Toc361333223)

[5.3 5](#_Toc361333224)

[5.4 Media independent handover reference framework 5](#_Toc361333225)

[5.4.1 5](#_Toc361333226)

[5.4.2 5](#_Toc361333227)

[5.4.3 5](#_Toc361333228)

[5.4.4 Single Radio MIHF relationship to reference model 5](#_Toc361333229)

[5.5 MIHF reference models for link-layer technologies 6](#_Toc361333230)

[5.5.1 6](#_Toc361333231)

[5.5.2 6](#_Toc361333232)

[5.5.3 6](#_Toc361333233)

[5.5.4 6](#_Toc361333234)

[5.5.5 6](#_Toc361333235)

[5.5.6 6](#_Toc361333236)

[5.5.7 6](#_Toc361333237)

[5.5.8 Single radio handover functional model and signaling flow 6](#_Toc361333238)

[5.6 7](#_Toc361333239)

[5.7 7](#_Toc361333240)

[5.8 Major single radio handover procedures 7](#_Toc361333241)

[5.9 Proxy operations 8](#_Toc361333242)

[5.9.1 Introduction 8](#_Toc361333243)

[5.9.2 Network discovery using proxy Information Server 9](#_Toc361333244)

[5.9.3 Preregistration using proxy PoA 10](#_Toc361333245)

[6. MIH Services 12](#_Toc361333246)

[6.1 12](#_Toc361333247)

[6.2 12](#_Toc361333248)

[6.3 12](#_Toc361333249)

[6.4 Media independent command service 12](#_Toc361333250)

[6.4.1 12](#_Toc361333251)

[6.4.2 12](#_Toc361333252)

[6.4.3 Command List 12](#_Toc361333253)

[6.5 Media independent information service 13](#_Toc361333254)

[6.5.1 13](#_Toc361333255)

[6.5.2 13](#_Toc361333256)

[6.5.3 13](#_Toc361333257)

[6.5.4 Information elements 13](#_Toc361333258)

[7. Service Access Point (SAP) and primitives 14](#_Toc361333259)

[7.1 14](#_Toc361333260)

[7.2 SAPs 14](#_Toc361333261)

[7.2.1 General 14](#_Toc361333262)

[7.2.2 Media dependent SAPs 14](#_Toc361333263)

[7.2.3 MIH\_SAP primitives 14](#_Toc361333264)

[7.3 MIH\_LINK\_SAP primitives 15](#_Toc361333265)

[7.3.1 15](#_Toc361333266)

[7.3.2 15](#_Toc361333267)

[7.3.3 15](#_Toc361333268)

[7.3.4 15](#_Toc361333269)

[7.3.5 15](#_Toc361333270)

[7.3.6 15](#_Toc361333271)

[7.3.7 15](#_Toc361333272)

[7.3.8 15](#_Toc361333273)

[7.3.9 15](#_Toc361333274)

[7.3.10 15](#_Toc361333275)

[7.3.11 15](#_Toc361333276)

[7.3.12 15](#_Toc361333277)

[7.3.13 15](#_Toc361333278)

[7.3.14 15](#_Toc361333279)

[7.3.15 Link\_Prereg\_Ready 15](#_Toc361333280)

[7.4 MIH\_SAP primitives 17](#_Toc361333281)

[7.4.1 17](#_Toc361333282)

[7.4.2 17](#_Toc361333283)

[7.4.3 17](#_Toc361333284)

[7.4.4 17](#_Toc361333285)

[7.4.5 17](#_Toc361333286)

[7.4.6 17](#_Toc361333287)

[7.4.7 17](#_Toc361333288)

[7.4.8 17](#_Toc361333289)

[7.4.9 17](#_Toc361333290)

[7.4.10 17](#_Toc361333291)

[7.4.11 17](#_Toc361333292)

[7.4.12 17](#_Toc361333293)

[7.4.13 17](#_Toc361333294)

[7.4.14 17](#_Toc361333295)

[7.4.15 17](#_Toc361333296)

[7.4.16 17](#_Toc361333297)

[7.4.17 17](#_Toc361333298)

[7.4.18 17](#_Toc361333299)

[7.4.19 17](#_Toc361333300)

[7.4.20 17](#_Toc361333301)

[7.4.21 17](#_Toc361333302)

[7.4.22 17](#_Toc361333303)

[7.4.23 17](#_Toc361333304)

[7.4.24 17](#_Toc361333305)

[7.4.25 17](#_Toc361333306)

[7.4.26 17](#_Toc361333307)

[7.4.27 17](#_Toc361333308)

[7.4.28 18](#_Toc361333309)

[7.4.29 MIH\_Prereg\_Xfer 18](#_Toc361333310)

[7.4.30 MIH\_N2N\_Prereg\_Xfer 22](#_Toc361333311)

[7.4.31 MIH\_Prereg\_Ready 26](#_Toc361333312)

[7.4.32 MIH\_CTRL\_Transfer 27](#_Toc361333313)

[8. Media independent handover protocols 30](#_Toc361333315)

[8.1 30](#_Toc361333325)

[8.2 30](#_Toc361333326)

[8.3 30](#_Toc361333327)

[8.4 30](#_Toc361333328)

[8.5 30](#_Toc361333329)

[8.6 MIH protocol messages 30](#_Toc361333330)

[8.6.1 30](#_Toc361333335)

[8.6.2 30](#_Toc361333336)

[8.6.3 MIH messages for command service 30](#_Toc361333337)

[9. MIH protocol protection 34](#_Toc361333338)

[9.1 34](#_Toc361333340)

[9.2 Key establishment through an MIH service access authentication 34](#_Toc361333341)

[9.2.1 34](#_Toc361333342)

[9.2.2 Key derivation and key hierarchy 34](#_Toc361333344)

[10. Proactive Authentication 35](#_Toc361333345)

[10.1 Media specific proactive authentication 35](#_Toc361333346)

[10.2 Bundling media access authentication with MIH service access authentication 36](#_Toc361333347)

[10.2.1 Media specific key derivation 36](#_Toc361333348)

[10.3 Establishing MIH Security Association between roaming partners 36](#_Toc361333349)

[10.4 Key generation and distribution by OPoS 37](#_Toc361333350)

[10.5 TPoS selection by OPoS 39](#_Toc361333351)

[Annex A Bibliography 40](#_Toc361333352)

[Annex B 40](#_Toc361333353)

[Annex C 40](#_Toc361333354)

[Annex D 40](#_Toc361333355)

[Annex E 40](#_Toc361333356)

[Annex F 41](#_Toc361333357)

[F.1 41](#_Toc361333358)

[F.2 41](#_Toc361333359)

[F.3 Derived data types 41](#_Toc361333360)

[F.3.1 41](#_Toc361333361)

[F.3.2 41](#_Toc361333362)

[F.3.3 41](#_Toc361333363)

[F.3.4 Data types for link identification and manipulation 41](#_Toc361333364)

[F.3.5 42](#_Toc361333365)

[F.3.6 42](#_Toc361333366)

[F.3.7 42](#_Toc361333367)

[F.3.8 Data types for information elements 42](#_Toc361333368)

[F.3.9 42](#_Toc361333369)

[F.3.10 42](#_Toc361333370)

[F.3.11 42](#_Toc361333371)

[F.3.12 42](#_Toc361333372)

[F.3.13 43](#_Toc361333373)

[F.3.14 43](#_Toc361333374)

[F.3.15 43](#_Toc361333375)

[F.3.16 Data type for security 43](#_Toc361333376)

[F.3.17 Data types for delivery of control messages 43](#_Toc361333377)

[Annex G 44](#_Toc361333378)

[Annex H 44](#_Toc361333379)

[Annex I 46](#_Toc361333380)

[Annex J 46](#_Toc361333381)

[Annex K 47](#_Toc361333382)

[Annex L 47](#_Toc361333383)

[Annex M 48](#_Toc361333384)

[Annex N 48](#_Toc361333385)

[N.1 48](#_Toc361333386)

[N.2 48](#_Toc361333387)

[N.3 48](#_Toc361333388)

[N.4 48](#_Toc361333389)

[N.5](#_Toc361333390) ~~[N.6](#_Toc361333390)~~ [Terminating Phase 49](#_Toc361333390)

[N.6 MIH\_Prereg\_Xfer messages for Optimized SA Establishment 49](#_Toc361333391)

[N.6.1 OPoS distributing key derivation key](#_Toc361333392) *[K](#_Toc361333392)* [to TPoS and MN 49](#_Toc361333392)

[N.6.2 OPoS relays additional Preregistration signaling 51](#_Toc361333393)

[N.6.3 OPoS key distribution when OPoS is same as TPoS 52](#_Toc361333394)

[N.6.4 OPoS relay preregistration when OPoS is same as TPoS 53](#_Toc361333395)

[Annex O 54](#_Toc361333396)

[Annex P MN’s Network Access Identifier Format 54](#_Toc361333397)

[Annex Q Network discovery for single radio handover 54](#_Toc361333398)

[Q.1 Network discovery: listening to the target link 54](#_Toc361333399)

[Q.2 Network discovery: using location information 55](#_Toc361333400)

[Annex R Handover Decision 57](#_Toc361333401)

[R.1 Weak SINR of the source link 58](#_Toc361333402)

[R.2 QoS and/or cost check 59](#_Toc361333403)

[R.3 Power consumption comparison of the link interfaces 60](#_Toc361333404)

[Annex S 60](#_Toc361333405)

Draft for

***IMPORTANT NOTICE: This standard is not intended to ensure safety, security, health, or environmental protection. Implementers of the standard are responsible for determining appropriate safety, security, environmental, and health practices or regulatory requirements.***

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

NOTE—The editing instructions contained in this <amendment/corrigendum> 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



   4. Assumptions

***Insert at end of 1.4***



The following assumptions apply during the single radio handover for a device that has two or more radios:

1. The mobile device can transmit on only one radio at a time. The target radio shall not transmit while the originating radio is transmitting.
2. While the originating radio is receiving, the target radio shall not transmit in a manner causing interference to the originating radio receiver.
3. Prior to handover completion, only the originating radio link is used to carry data.
4. Normative references

***Insert references in appropriate order***

IETF RFC 5677 (2009-12) IEEE 802.21 Mobility Services Framework Design (MSFD)

IEEE 802.21a Media Independent Handover Services Amendment 1: Security Extensions to Media Independent Handover Services and Protocol

1. Definitions

*Insert these definitions in appropriate order*

**Information Server:** a server providing information to discover a target network. The information server may be implemented in a Media Independent Information Server but may also be implemented with other standards such as the Access Network Discovery and Selection Function (ANDSF) defined in 3GPP or a server using Access Network Query Protocol (ANQP) defined in IEEE 802.11-2012.

**originating network PoS**: The Point of Service in the network of the Mobile Node’s current Point of Attachment

**originating radio**: the MN’s radio interface that transmits and/or receives over the radio link which the MN currently has established with the originating network

**preregistration:** preparatory handover signaling (possibly including security establishment) which is accomplished before the handover actually occurs.

**proxy Information Server:** A Server that can assist the mobile node to obtain the required information when a query is made via the originating network. To the MN, the Proxy Information Server appears to be an information Server of the originating network.

**proxy PoA**: An entity that provides service to a mobile node and a target point of attachment via the originating network. To the MN, this entity appears to be a point of attachment (PoA) in the target network. It enables such services as preregistration of the MN.

**single radio handover (SRHO)**: A handover among (possibly heterogeneous) radio access technologies during which a mobile node transmits over only one radio link at a time.

**single radio MIH frame**: A packet which may contain the target radio’s PDUs in its payload.

**SRHO-capable node:** An MIHF capable node that implements one or more commands from 7.4.30 through 7.4.33. For instance, a mobile node (MN) or PoA is SRHO-capable if it implements MIH\_Prereg\_Xfer commands.

**target network PoA**: A Point of Attachment in the target network, to which an MN will be attached after a handover has been completed.

**target network PoS**: A Point of Service in the target network of the target Point of Attachment, which will serve a Mobile Node after a handover has been completed.

**target radio**: the MN’s radio interface that will transmit and/or receive over the radio link which, after handover, the MN will have established with the target network.

1. Abbreviations and Acronyms

*Insert these definitions in appropriate order*

ANDSF Access network discovery and selection function

ANQP Access Network Query Protocol

HPoS Home Network Point of Service

OPoS originating network PoS

SRHO single radio handover

TPoA target network PoA

TPoS target network PoS

1. General architecture
   1. Introduction

***Insert 5.1.10 and 5.1.11***

* + 1. Media independent single radio handover

In single radio handover, the opportunities to deliver handover messages are limited. To improve single radio handover performance, it is important to accomplish as much of the handover signaling (including security establishment) before the handover actually occurs; this preparatory signaling is called preregistration. The exact signaling steps included in the preregistration procedure may depend on the requirements of the target network, and can be quite independent of the signaling nature of the originating network. As a general rule, preregistration typically involves one or more of the following steps, which are often needed in general for handovers:

* proactive authentication -- that is, authenticating the MN before it arrives in the target network,
* address allocation -- one or more IP addresses to be used by the MN after it arrives in the target network.
* data path setup -- establishing tunnels and forwarding entries for the MN in the target network
* context establishment -- building all necessary state information such as QoS parameters and access permissions within target core network entities.

Each of these operations can be time-consuming, and if they had to be carried out after the MN had returned to the target network radio access, for most applications seamless session handover would be impossible because of the dead time before packets could start flowing again (break-before-make) via the target network. Moreover, each of the operations must be carried out securely to prevent hijacking attempts or mismanagement of target network resources. As long as handovers occur only between access points within the same operator network, it is often possible to guarantee that signaling packets are never exposed to attack. On the other hand, for access networks belonging to different operators, the data path between neighboring access points of originating and target access networks are more likely to traverse the Internet, potentially exposing preregistration signaling to attack.

* + 1. Securing Single-Radio messages using PoS

Enabling movement between the networks of roaming partners for single-radio smartphones and Internet enabled wireless devices can be facilitated by enabling preregistration via the Point of Service (PoS) and making use of certain functions as developed in 3GPP , 3GPP2 , and WiMAX Forum . Using the PoS, signaling messages related to security information between roaming partners can be exchanged and as a result low-latency optimized session handover can be achieved. Communications between the originating and target networks must be secured. However, authentication has been typically quite time consuming because of reliance on distant authentication agents. A method is defined to establish a secure communication channel between originating and target networks as part of handover preregistration procedures (see 10.3). Improving the security model and reducing authentication delay enables crucial improvements in handover performance, because single-radio systems cannot take advantage of parallel authentication operations.

* 1. General design principles

***Insert 5.2.3***

* + 1. Single Radio Handover MIHF design principles

The following are functional requirements that facilitate single radio handover between possibly heterogeneous radio access technology networks:

1. tunneling mechanism to deliver the preregistration messages
2. control for preregistration states and delivery for preregistration contexts.

   2. Media independent handover reference framework

***Insert 5.4.4***

* + 1. Single Radio MIHF relationship to reference model

To prepare for handover, the MN may exchange link-layer PDUs with the target network PoA through a communication link that is established between MN and the target PoA using the active network connection. These PDUs contain the same information as in the PDUs that would be exchanged if the target links were active. There is no guarantee that the target link is accessible during a single radio handover. A proxy PoA (MIH PoS on a non-PoA network entity in Figure 2) can be used to enable the MN and the target PoA to exchange link-layer PDUs.

During a single radio handover, an L2 frame may be encapsulated in an MIH message, which is then exchanged via an active link between the MIHFs of a local and a remote node using MIH protocol over higher layer transport (TCP or UDP over IP).

* 1. MIHF reference models for link-layer technologies

***Insert 5.5.8***

* + 1. Single radio handover functional model and signaling flow

The functional model for single radio handover is shown in Figure 10a.



Figure 10a Single radio handover functional model.

The services in the originating network are: OPoS (the Originating network PoS) and the proxy Information Server (see 5.9). The services in the target network are: TPoS and the proxy PoA.



***Insert 5.8 and 5.9***

* 1. Major single radio handover procedures

A single radio handover following the reference model in 5.4 may consist of various handover procedures and involve different information elements (Clause 7) and messages (Clause 8). Examples of handover are described in Annex N. Figure 11a shows the single radio handover procedures consisting of five procedures as described below.



Figure 11a –Single radio handover procedures.

The five procedures shown in the Figure 11a are described as follows.

1. **Network discovery**: enables the MN to determine whether or not there is a candidate target network available for handover. Network discovery may involve the following:
   1. The MN may query the Information Server to discover candidate networks and their handover policies. Such information includes whether candidate networks and MN support SRHO or not, and the availability of proxy services on the candidate network. Network discovery also allows the MN to acquire the corresponding system information blocks for candidate PoAs to perform the radio measurements.
   2. The MN may request that the Originating PoS identify one or more candidate target networks.
   3. During idle times when the source radio is not in use, the MN may activate its target radio to scan for one or more reachable TPoAs.
2. The **handover decision** may involve the following:
   1. A handover trigger, which may be a command.
   2. Target network selection.
   3. Proxy services discovery.
   4. Evaluating the handover benefit: the evaluation can be made by the MN or the network, e.g., based on parameters such as signal strength, target QoE, cost, and operator policy.
3. **Preregistration** includes pro-active authentication and establishing context (user identity, security, resource information) at the target network. Possibly with the help of Proxy services, the MN can perform preregistration procedures within the target network while still retaining its data connection with the originating network. Optionally, the preregistration procedure may occur before the handover decision procedure as in the case of WiMAX target networks.
4. During **target link preparation,** the MN and target network prepare the establishment of the target link. This procedure ascertains whether the target network has enough resources to accommodate the new link and may include performing resource reservation or admission control as well as confirming that the signal conditions are favorable enough to establish the target link.
5. Finally, during **SRHO execution**, the source link is disconnected, the target radio is activated, and the target link is established. The association of the network layer address to the link layer address will change from the source link layer address to the target link layer address for IP-based mobility management, and future incoming packets are then routed to the target radio.
   1. Proxy operations
      1. Introduction

Proxy services intermediate the signaling between the MN and the target network via the originating network or between the MN and the Information Server. In single radio handover, the MN may signal to the proxy PoA as if signaling to the target PoA (TPoA), and the TPoA may respond by signaling to the Proxy service as if signaling to the MN. The MN may signal to the proxy Information Server as if signaling to the Information Server, and the Information Server may respond by signaling to the Proxy service as if signaling to the MN.

The L2 control frames are terminated at the proxy PoA, which processes these control frames. Before replying to the control frames, the proxy PoA may communicate with the appropriate network entities in the target network to enable conducting any needed functions requested in the control frame. This proxy in the control plane may therefore execute any control functions in general, including but not limited to preregistration and proactive authentication of the MN.

The network discovery control frames are terminated at the proxy Information Server. Before replying to the control frames, the proxy Information Server may communicate with the appropriate Information Server to enable conducting any needed functions requested in the control frame. Through the proxy Information Server, even though the MN cannot communicate with the Information Server directly, the MN can discover the target network.

In a WiMAX network, the proxy services may be implemented as an extension of the Signal Forwarding Function (SFF) [B5] and may reside at the Access Service Network Gateway (ASN-GW).

In a 3GPP network, the proxy services may be implemented as an extension of the Mobility Management Entity (MME)[B2].

In a 3GPP2 network, the proxy services may be implemented in the High-Rate Packet Data Signal-Forwarding Function (HRPD-SFF) and the existing functions of the Packet Control Function (PCF)[B7].

Signaling between the MN and the proxy service may be accomplished in a media independent manner using the functions of the originating network PoS, and the target network PoS and the signaling messages defined in this specification.

* + 1. Network discovery using proxy Information Server

The MN needs to communicate with the Information Server to discover a target access network. If the MN can directly access the Information Server, it can discover its target network by using MIH\_Get\_Information request and response messages. However, the MN may not always be able to directly access the Information Server. For example, an ANQP server may be used between the MN and WLAN access point (AP). On the other hand, the MN and the Information Server may be located in different networks and in different administrative domains. . For example, the MN may need to query via ANQP messages in an Wi-Fi access network while the information is available in an ANDSF server that is located in a cellular provider’s network. This scenario can be enabled if the Wi-Fi POA is SRHO-capable and an intermediate entity called proxy Information Server is available that can help forwarding the MN’s request to the ANDSF server.

Figure 11b gives an example call flow of the network discovery procedure using proxy Information Server. The goal of the MN is to discover the target network. The steps of the discovery procedure are as follows:

1. The MN requests information about the target network using MIH\_CTRL\_Transfer request or a non-MIH message such as ANQP query.
2. The SRHO-capable PoA transmits MIH\_CTRL\_Transfer request message to the proxy Information Server. In case the SRHO-capable PoA received non-MIH message in “step a,” the SRHO-capable PoA encapsulates the query message into the MIH\_CTRL\_Transfer request message and transmit the message to proxy Information Server (see clause 7.4.33).
3. The proxy Information Server extracts the encapsulated payload message and forwards the MN’s request to another functional entity (a.k.a., MIH User). This entity is responsible to transmit MN’s request to the information server. The interface specification between this functional entity and the information server (i.e., ANDSF server) is out of scope of this document. Note that any translation among different protocols (e.g., ANQP and ANDSF) is performed at the MIH User and is out of the scope of this specification.
4. The proxy Information Server transmits MIH\_CTRL\_Transfer response message to the SRHO-capable PoA by encapsulating the response that is obtained from the functional entity (i.e., MIH User).
5. The SRHO-capable PoA responds to the MN with information about the target network using MIH\_CTRL\_Transfer request or a non-MIH message such as ANQP response. In case the MN did not use MIH as protocol to transmit the original query, the SRHO-capable PoA decapsulates the MIH\_CTRL\_Transfer response message and forwards the content (e.g., ANQP response) to the MN. If the MN used MIH protocol for the initial query, then the MIHF forwards the MIH\_CTRL\_Transfer response message to the MN.



Figure 11b. Network discovery using proxy Information Server.

Use cases of the proxy Information Server are included in Annex S.

* + 1. Preregistration using proxy PoA

Suppose the MN needs to communicate with the target network PoA (TPoA) to prepare for handover by performing a network access procedure with the target access network. The first part of this communication is the transport of TCP or UDP / IP packets to the proxy PoA (Figures 11c and 11d). The second part of this communication depends on whether the TPoA is SRHO-capable (Figure 11c) or whether it is a legacy PoA lacking such capability (Figure 11d). If the target PoA is SRHO-capable, the L2 frame is encapsulated into an MIH frame to be forwarded to the target radio.

Figure 11c shows the transport of the target radio L2 control frame as a payload of a MIH frame between the MN and the proxy PoA via the originating radio interface in the absence of the target link. In Figure 11c, the MN has 2 interfaces (1) and (2). It uses the wireless interface (1) with PHY(1) and L2(1) in its protocol stack to communicate with the corresponding protocol stack PHY(1) and L2(1) at the AP or Base Station. After that, the AP / BS uses some other link, e.g., Ethernet, with protocol stack PHY and L2 to get to the Proxy. The Proxy is usually not using wireless interface. Therefore, the Proxy simply shows PHY and L2 and not PHY(1) and L2(1) in its protocol stack.



Figure 11c: Transport of L2 frame of target interface via MIH using the logical connection at the Target PoS to the SRHO-capable TPoA, showing the resulting protocol stack.

Figure 11d also shows the transport of the target radio L2 control frame as a payload of a MIH frame between the MN and the proxy PoA via the originating radio in the absence the target link. However, the TPoA is not SRHO-capable so that the proxy PoA has to communicate with the TPoA using other control messages in order to proxy between the MN and the TPoA.



Figure 11d. Transport of L2 frame via the proxy PoA, showing the resulting protocol stack.

The procedures of communication between the MN and the TPoA are shown in Figure 11e and are described below.



Figure 11e. Communication between the MN and the TPoA.

1. MN sends a message to the OPoS or directly to the TPoS / proxy PoA with a payload containing a target network L2 handover frame. If the message is directly sent to the TPoS / proxy PoA, the OPoS is bypassed. If the message is sent to the OPoS, then the OPoS will forward the message to the TPoS / proxy PoA.
2. Upon receiving this message from MN, the TPoS / proxy PoA helps to discover a suitable TPoA if not already known. It will determine whether the target PoA is SRHO-capable. If not, the TPoS / proxy PoA will communicate the link-layer frames to the target PoA using a mechanism that is outside the scope of this specification.
   1. TPoS or proxy PoA signals with this TPoA using MIH message if the TPoA is a SRHO-capable node (The target PoA supports MIH\_Prereg\_Xfer messaging.).
   2. Otherwise, proxy PoA may signal with the candidate target PoA using other L2-specific protocol messages. OPoS will relay the reply messages to MN, indicating whether the L2 preregistration signaling is successful. Also, the reply will include an indication for the fact that the messages used for the proxy to PoA signal with the TPoA are outside the scope of this document. L2 frames can be passed to the target PoA either by way of proxy PoA or by MIH\_Prereg\_Xfer commands.

As shown above, MN and target network can exchange link-layer PDUs without using the target PoA’s physical radio channel. The exchanged single-radio control frames are processed by the MIHF which has the assigned transport layer protocol’s port number [B31].

1. MIH Services



   4. Media independent command service


      3. Command List
         1. Link commands

***Insert following row at end of Table 6 in 6.4.3.1***

1. –Link commands

|  |  |  |
| --- | --- | --- |
| Link\_Prereg\_Ready | Request a preregistration on a target link | 7.3.15 |

* + - 1. MIH commands
         1. General

***Insert following rows at the end of Table 7 in 6.4.3.2.1:***

**Table 7 – MIH commands**

|  |  |  |
| --- | --- | --- |
| MIH\_Prereg\_Xfer | Transport parameters and link layer frames | 7.4.29 |
| MIH\_N2N\_Prereg\_Xfer | Transport link layer frames between OPoS and TPoS | 7.4.31 |
| MIH\_ Prereg\_Ready | Check readiness of preregistration on a target link | 7.4.32 |
| MIH\_CTRL\_Transfer | Delivers control messages encapsulated by MIH header | 7.4.33 |

* 1. Media independent information service



     4. Information elements

***Change ordered list element item (c) as follows:***

1. The Information Server provides access to the Point of Service information, the Mobile Node information and the capability for supporting SRHO for each of the available access networks. The PoS sends information elements that include PoS addressing information and tunnel management protocol information.
2. ~~c)~~ Other information that is access network specific, service specific, or vendor/network specific

***Insert information elements in Table 10 as follows:***

**Table 10 –Information elements**

|  |  |  |
| --- | --- | --- |
| Name of information element | Description | Data type |
| PoA-specific higher layer service information elements | | |
| IE\_PoS\_TUNN\_MGMT\_PRTO | Type of tunnel management protocol supported. | IP\_TUNN\_MGMT |
| IE\_PoS\_NAI | NAI of PoS. | NAI |

1. Service Access Point (SAP) and primitives

   2. SAPs
      1. General
      2. Media dependent SAPs
         1. MIH\_LINK\_SAP primitives

***Insert primitives in Table 15 as follows:***

**Table 15 – MIH\_LINK\_SAP primitives (continued)**

|  |  |  |  |
| --- | --- | --- | --- |
| Primitives | Service  category | Description | Defined  in |
| Link\_ Prereg\_Ready | Command | Used by MIHFs at MN and PoS to prepare for preregistration | 7.3.15 |

* + - 1. MIH\_NET\_SAP primitives

***Insert primitives in Table 16 as follows:***

**Table 16 – MIH\_NET\_SAP primitives (continued)**

|  |  |  |  |
| --- | --- | --- | --- |
| Primitives | Service  category | Description | Defined  in |
| MIH\_N2N\_Prereg\_Xfer | Command | Used by MIHFs at OPoS and TPoS for cross-network preregistration operations | 7.4.31 |

* + 1. MIH\_SAP primitives

***Insert primitives in Table 17 as follows:***

**Table 17 – MIH\_SAP primitives (continued)**

|  |  |  |  |
| --- | --- | --- | --- |
| Primitives | Service  category | Description | Defined  in |
| MIH\_Prereg\_Xfer | Command | Used by MIHFs at MN and PoS for preregistration operations | 7.4.30 |
| MIH\_ Prereg\_Ready | Command | Used by MIHFs at MN and PoS to prepare for preregistration | 7.4.32 | |
| MIH\_CTRL\_Transfer | Command | Used by MIHF to deliver control messages | 7.4.33 |

* 1. MIH\_LINK\_SAP primitives

***Insert following 7.3.15***

* + 1. Link\_Prereg\_Ready
       1. Link\_Prereg\_Ready.request
          1. Function

The primitives defined here are used by MIH functions running on MN and PoS to prepare for preregistration for MN on a target Point of Attachment. See Annex R for examples.

* + - * 1. Semantics of service primitive

Link\_Prereg\_Ready.request (

ExecutionDelay

)

|  |  |  |
| --- | --- | --- |
| **Parameter Name** | Data type | Description |
| ExecutionDelay | UNSIGNED\_INT(2) | Time (in ms) to elapse before the action SHOULD be taken. A value of 0 indicates that the action is taken immediately. Time elapsed is calculated from the instance the request arrives until the time when the execution of the action is carried out. |

* + - * 1. When generated

This primitive is generated by the MIHF to prepare preregistration of the target link.

* + - * 1. Effect on receipt

Upon receipt of this primitive, the target link interface prepares preregistration at the time specified by the ExecutionDelay parameter. The L2 messages for preregistration are transmitted to the MIHF for preregistration preparation with the target link layer.

* + - 1. Link\_Prereg\_Ready.confirm
         1. Function

This primitive is used by link-layer technologies to provide an indication of the result of the preregistration preparation on the target link layer.

* + - * 1. Semantics of service primitive

Link\_Prereg\_Ready.confirm (

Status

)

|  |  |  |
| --- | --- | --- |
| Parameter Name | Data type | Description |
| Status | STATUS | Status of the operation. Code 3 (Authorization Failure) is not applicable. (See Table F.3.2) |

* + - * 1. When generated

This primitive is generated in response to Link\_Prereg\_Ready.request operation.

* + - * 1. Effect on receipt

Upon reception of this primitive, the MIHF can know the status of the preregistration on the target link.

* 1. MIH\_SAP primitives

***Insert following 7.4.30 – 7.4.33***

* + 1. MIH\_Prereg\_Xfer

The primitives defined in this clause are used by MIH applications running on the MN and OPoS during preregistration for MN at a target Point of Attachment. See Annex N for examples. For many handovers, the mobile node and the target network may need to exchange layer-2 information, in the same way as they would exchange layer-2 information during a handover not mediated by MIHF. Such layer-2 signaling messages can be provided by the mobile node or the target network within the LLInformation parameter carried by MIH\_Prereg\_Xfer messages.

* + - 1. MIH\_Prereg\_Xfer.request
         1. Function

This primitive is used to transport parameters and link layer frames from the MN’s MIH application to the MIHF running on the MN’s serving PoS (i.e., OPoS) for preregistration signaling, including the establishment of a secure tunnel, between the MN and a target PoS (TPoS) in an appropriate target network.

* + - * 1. Semantics of service primitive

MIH\_Prereg\_Xfer.request (

DestinationIdentifier,

TargetLinkIdentifier,

LLInformation,

TPoSIdentifier,

CandidateLinkList,

CiphersuiteCode,

)

|  |  |  |
| --- | --- | --- |
| Parameter Name | Data type | Description |
| DestinationIdentifier | MIHF\_ID | Identifies an MIHF as the destination of this request. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | (Optional: may be included if the target link is known) Identifies the remote PoA as the corresponding peer of the L2 exchange.[[2]](#footnote-2) |
| LLInformation | LL\_FRAMES | (Optional: included if the target link is known) Carries link layer frames. |
| TPoSIdentifier | MIHF\_ID | (Optional) This identifies the target PoS (TPoS) that will be the destination of the link-layer frames. |
| CandidateLinkList | LIST (LINK\_PoA\_LIST) | (Optional) A list of PoAs, identifying candidate networks to which handover SHOULD be initiated. The list is sorted from most preferred first to least preferred last. The link information can include values and IEs from tables F.10, F.11, F.14, and G.1. |
| CiphersuiteCode | BITMAP(8) | (Optional) CiphersuiteCode is included when MN wishes to request use of a particular algorithm during the establishment of a security association with TPoS for the purposes of preregistration in the target network. |

* + - * 1. When generated

This primitive is generated by an MIH application to preregister with a target PoS. The MN can send this primitive to instruct its serving PoS (i.e., the OPoS) to generate a Security Association with an appropriate TPoS when the OPoS and the TPoS reside on different nodes, for instance so that the MN and the TPoS are able to carry out additional preregistration commands before handover to TPoA. The MN can include whatever information it has about candidate TPoAs, to help OPoS to identify the proper TPoS. If the MN has sufficient information about a TPoA to include link-layer frames, those frames can also be supplied for secure delivery to that TPoA. In this way, the number of round trips for preregistration may be minimized.

* + - * 1. Effect on receipt

If the TargetLinkIdentifier is not included, the OPoS shall use the CandidateLinkList (if included) to identify the appropriate TPoS that can initiate preregistration activities with an appropriate TPoA. In the absence of other information, the OPoS can use available link-type information and location information for the MN to identify an appropriate TPoS. Some location information about the MN may be available by other means, such as associating geographical coordinates with the MN’s current Point of Attachment (i.e., OPoA). After reception of this primitive, the MIHF must generate a MIH\_N2N\_Prereg\_Xfer request message destined to the TPoS, which is expected to relay the link-layer frames transported in this message to the TPoA.

* + - 1. MIH\_Prereg\_Xfer.indication
         1. Function

This primitive is used by the OPoS’s MIHF to notify OPoS’s MIH application about the reception of an MIH\_Prereg\_Xfer request message.

* + - * 1. Semantics of service primitive

MIH\_Prereg\_Xfer.indication (

SourceIdentifier,

TargetLinkIdentifier,

LLInformation,

TPoSIdentifier,

CandidateLinkList,

CiphersuiteCode,

)

|  |  |  |
| --- | --- | --- |
| Parameter Name | Data type | Description |
| SourceIdentifier | MIHF\_ID | Identifies the invoker, an MN in the same network as OPoS. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | (Optional: may be included if the target link is known) Identifies the remote PoA as the corresponding peer of the L2 exchange[[3]](#footnote-3). |
| LLInformation | LL\_FRAMES | (Optional) This carries link layer frames. This attribute may be included if the target link is known. |
| TPoSIdentifier | MIHF\_ID | (Optional) This identifies the target PoS |
| CandidateLinkList | LIST(LINK\_PoA\_LIST) | (Optional) A list of PoAs, identifying candidate networks to which handover SHOULD be initiated. The list is sorted from most preferred first to least preferred last. The link information can include values and IEs from tables F.10, F.11, F.14, and G.1. |
| CiphersuiteCode | BITMAP(8) | (Optional) CiphersuiteCode is included when MN wishes to request use of a particular algorithm during the establishment of a security association with TPoS for the purposes of preregistration in the target network. |

* + - * 1. When generated

This primitive is generated by an MIHF after receiving a MIH\_Prereg\_Xfer Request protocol message.

* + - * 1. Effect on receipt

If TPoSIdentifier is not provided, the MIH application on the OPoS uses the information provided by the MN to identify an appropriate target PoS (TPoS). If the TPoS is hosted remotely (e.g., in a separate target network), the MIH application on the OPoS must generate a MIH\_N2N\_Prereg\_Xfer.request primitive for the TPoS. Otherwise, the MIH application must generate a MIH\_Prereg\_Xfer.response primitive and transmit that response to the MIHF specified by the SourceIdentifier.

* + - 1. MIH\_Prereg\_Xfer.response
         1. Function

OPoS’s MIH application uses this primitive to relay preregistration frames to MN via OPoS’s local MIHF.

* + - * 1. Semantics of service primitive

MIH\_Prereg\_Xfer.response (

DestinationIdentifier,

TargetLinkIdentifier,

LLInformation,

MN\_NAI,

TPoSIdentifier,

SALifeTime,

Status

)

|  |  |  |
| --- | --- | --- |
| Parameter Name | Data type | Description |
| DestinationIdentifier | MIHF\_ID | This identifies an MIHF that will be the destination of this response. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | (Optional: may be included if the target link is known) Identifies the remote PoA as the corresponding peer of the L2 exchange. [[4]](#footnote-4) |
| LLInformation | LL\_FRAMES | (Optional) Carries link layer frames; included if and only if the corresponding MIH\_Prereg\_Xfer.indication contained LLInformation. |
| MN\_NAI | MIHF\_ID | (Optional) Carries the MN’s Network Access Identifier in the case optimized pull key distribution is used. |
| TPoSIdentifier | MIHF\_ID | (Optional) This identifies the target PoS |
| SALifeTime | Lifetime TLV | (Optional) Lifetime of the Security Association |
| Status | STATUS | Status of the preregistration transfer with TPoS. Code 3 (Authorization Failure) is not applicable. (See Table F.3.2) |

* + - * 1. When generated

This primitive is generated by OPoS either: (i) after receiving a MIH\_Prereg\_Xfer.indication primitive if the MIH application that received the corresponding MIH\_Prereg\_Xfer.request primitive did not invoke a MIH\_N2N\_Prereg\_Xfer.request primitive, or (ii) after receiving a MIH\_N2N\_Prereg\_Xfer.confirm primitive. If the OPoS has received a positive confirmation that the TPoS has accepted the Security Association, this will enable MN to complete the establishment of the secure tunnel.

* + - * 1. Effect on receipt

The local MIHF generates a MIH\_Prereg\_Xfer Response protocol message in order to provide the MN with the information previously requested in MIH\_N2N\_Prereg\_Xfer Request.

* + - 1. MIH\_Prereg\_Xfer.confirm
         1. Function

This primitive is used to notify the MN’s MIH application about the reception of a MIH\_Prereg\_Xfer Response message.

* + - * 1. Semantics of service primitive

MIH\_Prereg\_Xfer.confirm (

SourceIdentifier,

TargetLinkIdentifier,

LLInformation,

MN\_NAI,

TPoSIdentifier,

*K*,

SALifeTime,

Status

)

|  |  |  |
| --- | --- | --- |
| Parameter Name | Data type | Description |
| SourceIdentifier | MIHF\_ID | This identifies the invoker, which is an MIHF. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | This identifies the remote PoA that is the corresponding peer of the L2 exchange. [[5]](#footnote-5) |
| LLInformation | LL\_FRAMES | (Optional) Carries link layer frames |
| MN\_NAI | MIHF\_ID | (Optional) Carries the Network Access Identifier assigned for use by the MN after movement to the target network |
| TPoSIdentifier | MIHF\_ID | (Optional) Identifies the target PoS |
| *K* | ENCR\_BLOCK | (Optional) A key derivation key encrypted in a way recoverable by TPoS |
| SALifeTime | Lifetime | (Optional) Lifetime of the Security Association |
| Status | STATUS | Status of the preregistration transfer with TPoS. Code 3 (Authorization Failure) is not applicable. (See Table F.3.2) |

* + - * 1. When generated

The MN’s MIHF generates this primitive after receiving a MIH\_Prereg\_Xfer Response protocol message. If the MN included CiphersuiteCode with the MIH\_Prereg\_Xfer Request message, then the optional key derivation key *K* will be included in the MIH\_Prereg\_Xfer Response message so that MN can compute the keys necessary for communication with TPoS and TPoA.

* + - * 1. Effect on receipt

The MIH application on the MN may generate another MIH\_Prereg\_Xfer.request primitive -- for example if preregistration procedures are not completed. If *K* is present, the MN derives the key hierarchy according to clause 9.2.2 and Figure 47.

* + 1. MIH\_N2N\_Prereg\_Xfer

The primitives defined in 7.4.31 are used by MIH functions running on OPoS and TPoS to enable preregistration for MN on a target Point of Attachment. See Annex N for examples. The primitives provide the ability to transport link-layer frames for the target link over the MIH protocol between the originating PoS and the target PoS. Preregistration is conducted between the MN and the target PoA. As part of preregistration, media-specific authentication may be conducted with an authenticator deployed in the target PoA.

* + - 1. MIH\_N2N\_Prereg\_Xfer.request
         1. Function

OPoS generates this primitive to deliver link layer frames to the target PoS.

* + - * 1. Semantics of Service Primitive

MIH\_N2N\_Prereg\_Xfer.request (

DestinationIdentifier,

TargetLinkIdentifier,

LLInformation,

MNID,

CandidateLinkList,

CiphersuiteCode

)

|  |  |  |
| --- | --- | --- |
| Parameter Name | Data type | Description |
| DestinationIdentifier | MIHF\_ID | This identifies a remote MIHF that will be the destination of this request. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | (Optional) Identifies the remote PoA as the corresponding peer of the L2 exchange; [[6]](#footnote-6) shall be included if the target link is known. |
| LLInformation | LL\_FRAMES | (Optional) Carries link layer frames; shall be included if the target link is known. |
| MNID | MIHF\_ID | (Optional) MIHF\_ID of the MN to identify the MN’s Media Independent Root Key to be transferred to the target PoS. |
| CandidateLinkList | LIST (LINK\_PoA\_LIST) | (Optional) A list of PoAs, identifying candidate networks to which handover SHOULD be initiated. The list is sorted from most preferred first to least preferred last. This attribute shall not be included if the target link is known. |
| CiphersuiteCode | BITMAP(8) | (Optional) CiphersuiteCode is included when MN wishes to request use of a particular algorithm during the establishment of a security association with TPoS for the purposes of preregistration in the target network. |

* + - * 1. When generated

OPoS’s MIH application generates this primitive after receiving an MIH\_Prereg\_Xfer.indication primitive, to relay preregistration signaling to the target PoS. OPoS may do this to relay link-layer frames, or to establish a security association derived from key derivation key *K*. In order to allow OPoS and TPoS to exchange the key derivation key *K*, MIHF of OPoS first produces *K*, and another random number Nonce-N. Then OPoS’s MIHF encrypts *K* using the mechanism specified in clause 10, and transmits the result to TPoS along with Nonce-N and Nonce-T, where Nonce-T is the value received from MN in the MIH\_Prereg\_Xfer protocol message.

* + - * 1. Effect on receipt

The local MIHF shall generate a MIH\_N2N\_Prereg\_Xfer request message to the remote MIHF.

* + - 1. MIH\_N2N\_Prereg\_Xfer.indication
         1. Function

This primitive is used by the MIHF of the TPoS to notify its MIH application of the reception of a MIH\_N2N\_Prereg\_Xfer request message.

* + - * 1. Semantics of service primitive

MIH\_N2N\_Prereg\_Xfer.indication (

SourceIdentifier,

TargetLinkIdentifier,

MNID,

*K*,

LLInformation

)

|  |  |  |
| --- | --- | --- |
| Parameter Name | Data type | Description |
| SourceIdentifier | MIHF\_ID | This identifies the invoker, which is a remote MIHF. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | (Optional)This identifies the remote PoA that is the corresponding peer of the L2 exchange. [[7]](#footnote-7) This attribute shall be included if the target link is known. |
| LLInformation | LL\_FRAMES | (Optional) carries link layer frames. This attribute shall be included only the target link is known. |
| MNID | MIHF\_ID | ID of the MN, used to index and compute the MN’s Media Independent Root Key to be established the target PoS |
| *K* | ENCR\_BLOCK | A key derivation key encrypted in a way recoverable by TPoS |

* + - * 1. When generated

TPoS’s MIHF generates this primitive upon receiving a MIH\_N2N\_Prereg\_Xfer Request protocol message.

* + - * 1. Effect on receipt

The TPoS MIHF recovers *K* according to the formula in 10.3.1. MIHF then passes *K* to the MIH application, which then derives the key hierarchy, installing keys as necessary in the target AAA. The TPoS also must generate appropriate messages to the TPoA to install a media-specific pair-wise master key (MSPMK, defined in 10.2.1.2) also derived from *K*, which will be used by MN as necessary when MN connects to the target network. The MSPMK will be distributed to the target PoA using media-specific key distribution described in 10.2.2.

The MIH application must generate an MN\_NAI associated with the MNID provided; the two IDs are allowed to be the same.

The MIH application must subsequently generate a MIH\_N2N\_Prereg\_Xfer.response primitive and include MN\_NAI.

***Subclauses 10.2.1.2 and 10.2.2 are defined in IEEE 802.21a-2012.***

* + - 1. MIH\_N2N\_Prereg\_Xfer.response
         1. Function

This primitive is used by TPoS’s MIH application to supply preregistration frames to TPoS’s MIHF.

* + - * 1. Semantics of service primitive

MIH\_N2N\_Prereg\_Xfer.response (

DestinationIdentifier,

TargetLinkIdentifier,

LLInformation,

MN\_NAI,

SALifeTime,

Status

)

|  |  |  |
| --- | --- | --- |
| Parameter Name | Data type | Description |
| DestinationIdentifier | MIHF\_ID | This identifies a remote MIHF that will be the destination of this response. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | This identifies the remote PoA that is the corresponding peer of the L2 exchange. [[8]](#footnote-8) |
| LLInformation | LL\_FRAMES | (Optional) Carries link layer frames |
| MN\_NAI | MIHF\_ID | (Optional) Carries the MN’s temporary Network Access Identifier assigned by the target network. |
| SALifeTime | Lifetime TLV | (Optional) Lifetime of the Security Association |
| Status | STATUS | Status of the preregistration transfer with TPoS. Code 3 (Authorization Failure) is not applicable. (See Table F.3.2) |

* + - * 1. When generated

This primitive is generated after receiving a MIH\_N2N\_Prereg\_Xfer.indication primitive.

* + - * 1. Effect on receipt

The MIHF at the TPoS shall generate a MIH\_N2N\_Prereg\_Xfer Response protocol message in order to provide the required information until the authentication is finished.

* + - 1. MIH\_N2N\_Prereg\_Xfer.confirm
         1. Function

This primitive is used to notify OPoS’s MIH application about the reception of a MIH\_N2N\_Prereg\_Xfer Response protocol message.

* + - * 1. Semantics of service primitive

MIH\_N2N\_Prereg\_Xfer.confirm (

SourceIdentifier,

TargetLinkIdentifier,

LLInformation,

MN\_NAI,

SALifeTime,

Status

)

|  |  |  |
| --- | --- | --- |
| Parameter Name | Data type | Description |
| SourceIdentifier | MIHF\_ID | This identifies the invoker, which is a remote MIHF. |
| TargetLinkIdentifier | LINK\_TUPLE\_ID | This identifies the remote PoA that is the corresponding peer of the L2 exchange. [[9]](#footnote-9) |
| LLInformation | LL\_FRAMES | (Optional) This carries link layer frames. |
| MN\_NAI | MIHF\_ID | (Optional) This carries the MN’s Network Access Identifier |
| SALifeTime | Lifetime TLV | (Optional) Lifetime of the Security Association |
| Status | STATUS | Status of the preregistration transfer with TPoS. Code 3 (Authorization Failure) is not applicable. Code 6 (TPoS is identical to OPoS), is not applicable. (See Table F.3.2) |

* + - * 1. When generated

This primitive is generated by the remote MIH application after receiving a MIH\_N2N\_Prereg\_Xfer response message.

* + - * 1. Effect on receipt

The OPoS MIH application generates a MIH\_Prereg\_Xfer.response primitive with the information obtained from this primitive. The OPoS also retrieves its stored value for *K* which had previously been sent to the TPoS MIHF, encrypting it according to clause 10.4 for use in the MIH\_ Prereg\_Xfer Response protocol message.

* + 1. MIH\_Prereg\_Ready

The primitives defined in 7.4.32 are used by the MIHF at MN to select a target network interface for preregistration. After the target network interface receives MIH\_Prereg\_Ready.request, the target network interface responds with MIH\_Prereg\_Ready.response. See Annex R for examples.

* + - 1. MIH\_Prereg\_Ready.request
         1. Function

This primitive is used by an MIH application of MN MIHF to request preparation for preregistration on a target link interface of the MN.

* + - * 1. Semantics of service primitive

MIH\_Prereg\_Ready.request (

DestinationIdentifier,

LinkType

)

|  |  |  |
| --- | --- | --- |
| Parameter Name | Data type | Description |
| DestinationIdentifier | MIHF\_ID | This identifies the MIHF that will be the destination of this request. |
| LinkType | LINK\_TYPE | This identifies the link type of the link for which preregistration is desired. |

* + - * 1. When generated

This primitive is generated by the MIHF user to prepare preregistration of the target link.

* + - * 1. Effect on receipt

If the Destination Identifier is the MIHF-ID of the local MIHF, the local MIHF invokes an IF\_Prereg\_Ready.request primitive to the specified lower layer link(s). Otherwise, the local MIHF generates and sends a MIH\_Prereg\_Ready request message to the remote MIHF identified by the Destination Identifier. The remote MIHF issues Link\_Prereg\_Ready.request(s) to the specified lower layer link(s).

* + - 1. MIH\_Prereg\_Ready.confirm
         1. Function

This primitive is used by the MIHF to confirm that the target link is ready for preregistration signaling.

* + - * 1. Semantics of service primitive

MIH\_Prereg\_Ready.confirm (

SourceIdentifier,

Status,

LinkType

)

|  |  |  |
| --- | --- | --- |
| Parameter Name | Data type | Description |
| SourceIdentifier | MIHF\_ID | This identifies the MIHF invoking of this primitive. |
| Status | STATUS | Status of the preregistration transfer with TPoS. Code 3 (Authorization Failure) is not applicable. (See Table F.3.2) |
| LinkType | LINK\_TYPE | This identifies the link type for which preregistration is desired. |

* + - * 1. When generated

This primitive is generated by the MIHF on receiving a MIH\_Prereg\_Ready response message from a peer MIHF.

* + - * 1. Effect on receipt

Upon receipt of this primitive, the MIHF user can know success of preregistration preparation on the target link. If Status does not indicate “Success,” the recipient performs appropriate error handling.

* + 1. MIH\_CTRL\_Transfer

The primitives defined in 7.4.33 are used by the MIHF of MN or PoS to transfer control messages encapsulated by MIH header. 5.9.3 shows the use of MIH\_CTRL\_Transfer message. See Annex S for examples.

* + - 1. MIH\_CTRL\_Transfer.request
         1. Function

This primitive delivers control messages encapsulated by MIH header. The control messages are not only MIH specific control messages but may include other messages, such as ANQP and ANDSF control messages.

* + - * 1. Semantics of service primitive

MIH\_CTRL\_Transfer.request (

DestinationIdentifier,

CTRLmessage,

)

|  |  |  |
| --- | --- | --- |
| Parameter Name | Data type | Description |
| DestinationIdentifier | MIHF\_ID | Identifies an MIHF as the destination of this request. |
| CTRLmessage | CTRL\_PROT\_MSGS | Delivers control messages. |

* + - * 1. When generated

This primitive is generated by an MIH application to deliver control messages such as ANQP and ANDSF messages.

* + - * 1. Effect on receipt

After reception of this primitive, the MIHF of MN at PoSmust generate a MIH\_CTRL\_Transfer request message destined to the MIHF of proxy Information Server.

* + - 1. MIH\_CTRL\_Transfer.indication
         1. Function

This primitive is used by the MIHF to notify the local MIH application about the reception of a MIH\_CTRL\_Transfer request message.

* + - * 1. Semantics of service primitive

MIH\_CTRL\_Transfer.indication (

SourceIdentifier,

CTRLmessage,

)

|  |  |  |
| --- | --- | --- |
| Parameter Name | Data type | Description |
| SourceIdentifier | MIHF\_ID | Identifies the invoker, typically a remote MIHF. |
| CTRLmessage | CTRL\_PROT\_MSGS | This delivers control messages. |

* + - * 1. When generated

This primitive is generated by an MIHF after receiving a MIH\_CTRL\_Transfer request message.

* + - * 1. Effect on receipt

The MIH application must generate a MIH\_CTRL\_Transfer.response primitive.

* + - 1. MIH\_CTRL\_Transfer.response
         1. Function

This primitive is used by an MIH application to provide control messages to the local MIHF.

* + - * 1. Semantics of service primitive

MIH\_CTRL\_Transfer.response (

DestinationIdentifier,

CTRLmessage,

Status

)

|  |  |  |
| --- | --- | --- |
| Parameter Name | Data type | Description |
| DestinationIdentifier | MIHF\_ID | This identifies a remote MIHF that will be the destination of this response. |
| CTRLmessage | CTRL\_PROT\_MSGS | Delivers control messages. |
| Status | STATUS | Status of the preregistration transfer with TPoS. Code 3 (Authorization Failure) is not applicable. (See Table F.3.2) |

* + - * 1. When generated

This primitive is generated by the local MIHF after receiving a MIH\_CTRL\_Transfer.indication primitive.

* + - * 1. Effect on receipt

The local MIHF may generate a MIH\_CTRL\_Transfer response message.

* + - 1. MIH\_CTRL\_Transfer.confirm
         1. Function

This primitive is used to notify the local MIH application about the reception of a MIH\_CTRL\_Transfer response message.

* + - * 1. Semantics of service primitive

MIH\_CTRL\_Transfer.confirm (

SourceIdentifier,

CTRLmessage,

Status

)

|  |  |  |
| --- | --- | --- |
| Parameter Name | Data type | Description |
| SourceIdentifier | MIHF\_ID | This identifies the invoker, which is a remote MIHF. |
| CTRLmessage | CTRL\_PROT\_MSGS | Delivers control messages. |
| Status | STATUS | Status of the preregistration transfer with TPoS. Code 3 (Authorization Failure) is not applicable. (See Table F.3.2) |

* + - * 1. When generated

This primitive is generated by the local MIHF after receiving a MIH\_CTRL\_Transfer response message.

* + - * 1. Effect on receipt

The MIH application on the MN may generate a MIH\_CTRL\_Transfer.request primitive.



1. Media independent handover protocols














   15. MIH protocol messages






       7. MIH messages for command service

***Insert 8.6.3.24 through 8.l6.3.31***

* + - 1. MIH\_Prereg\_Xfer Request

MN’s MIHF sends this message so that OPoS transmits link layer frames to expedite preregistration with an appropriate TPoS, particularly to initiate proactive authentication for the establishment of a security association. The corresponding primitive is defined in 7.4.30.1. Nonce-T is included if MN is requesting OPoS to establish a security association with TPoS. CandidateLinkList is included if MN has information available about the desired target link. Nonce-T is generated by MN’s MIHF.

|  |
| --- |
| MIH Header Fields (SID=3, Opcode=1, AID=13) |
| **Source Identifier** = sending MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID  (Destination MIHF ID TLV) |
| TargetLinkIdentifier (optional)  (Link Identifier TLV) |
| LLInformation (optional)  (Link Layer Information TLV) |
| TPoSIdentifier (optional)  (TPoS Identifier TLV) |
| CandidateLinkList (optional)  (Link identifier list TLV) |
| CiphersuiteCode (optional) (Ciphersuite Code TLV) |
| Nonce-T (optional) (Nonce TLV) |

*(Note to editor: Nonce TLV is defined in IEEE 802.21a-2012.)*

* + - 1. MIH\_Prereg\_Xfer Response

This message is used by the MIHF running on OPoS to complete the establishment of a security association between an MN and an appropriate TPoS. The corresponding primitive is defined in 7.4.30.3. SALifetime, *K*, and Nonce-N are not sent unless MN sent Nonce-T in the MIH\_Prereg\_Xfer Request. *K* is encrypted as described in 10.4.

|  |
| --- |
| MIH Header Fields (SID=3, Opcode=2, AID=13) |
| **Source Identifier** = sending MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID  (Destination MIHF ID TLV) |
| TargetLinkIdentifier (optional) (Link Identifier TLV) |
| LLInformation (optional) (Link Layer Information TLV) |
| MN\_NAI (optional) (Network Access Identifier TLV) |
| TPoSIdentifier (optional) (TPoS Identifier TLV) |
| Encrypted key derivation key *K* (optional) (ENCR\_BLOCK TLV) |
| Nonce-N (optional) (Nonce TLV) |
| SALifeTime (optional) (Lifetime TLV) |
| Status (Status TLV) |

*(Note to editor: Lifetime TLV is defined in IEEE 802.21a-2012.)*

* + - 1. MIH\_N2N\_Prereg\_Xfer Request

An MIHF sends this message to relay link layer frames during preregistration. The corresponding primitive is defined in 7.4.31.1. Nonce-T, Nonce-N, and the encrypted key derivation key *K* must all be present, or must all be absent; MIHF generates Nonce-N and the encrypted key derivation key *K* as specified in 9.2.2. The method for encrypting *K* is specified in 10.4.

*Note to editor: 9.2.2 is defined in IEEE 802.21a-2012.*

|  |
| --- |
| MIH Header Fields (SID=3, Opcode=1, AID=14) |
| **Source Identifier** = sending MIHF ID (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID (Destination MIHF ID TLV) |
| TargetLinkIdentifier (optional) (Link Identifier TLV) |
| LLInformation (optional) (Link Layer Information TLV) |
| MNID (optional) (Mobile node MIHF ID TLV) |
| CiphersuiteCode (optional) (Ciphersuite Code TLV) |
| Encrypted key derivation key *K* (optional) (ENCR\_BLOCK TLV) |
| Nonce-T (optional) (Nonce TLV) |
| Nonce-N (optional) (Nonce TLV) |
| SALifeTime (optional) (Lifetime TLV) |

* + - 1. MIH\_N2N\_Prereg\_Xfer Response

An MIHF sends this message to complete the establishment of a security association between itself and the preregistering MN, or to accomplish other layer-2 signaling. The corresponding primitive is defined in 7.4.31.3. The SALifeTime may be included if specified by the TPoS for the requested security association. The TPoS may also include the MN\_NAI parameter if the MNID parameter of the MIH\_N2N\_Prereg\_Xfer Request message is not appropriate for use in the target network.

|  |
| --- |
| MIH Header Fields (SID=3, Opcode=2, AID=14) |
| **Source Identifier** = sending MIHF ID (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID (Destination MIHF ID TLV) |
| TargetLinkIdentifier (Link Identifier TLV) |
| LLInformation (optional) (Link Layer Information TLV) |
| MN\_NAI (Network Access Identifier TLV)(optional) |
| SALifeTime (optional) (Lifetime TLV) |
| Status (Status TLV) |

* + - 1. MIH\_Prereg\_Ready request

The corresponding MIH primitive of this message is defined in 7.4.32.1.

This message is transmitted to the MIHF to perform preparation of preregistration.

|  |
| --- |
| MIH Header Fields (SID=3, Opcode=1, AID=15) |
| **Source Identifier** = sending MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID  (Destination MIHF ID TLV) |
| LinkType  (Link type TLV) |

* + - 1. MIH\_Prereg\_Ready response

The corresponding MIH primitive of this message is defined in 7.4.32.2.

This message returns the result of a MIH\_Prereg\_Ready request.

|  |
| --- |
| MIH Header Fields (SID=3, Opcode=2, AID=15) |
| **Source Identifier** = sending MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID  (Destination MIHF ID TLV) |
| Status ( Status TLV) |
| LinkType  (Link type TLV |

* + - 1. MIH\_CTRL\_Transfer request

This message is used to deliver control messages such as ANQP and ANDSF message. The delivery of control messages is described in 12.3. The corresponding MIH primitive of this message is defined in 7.4.33.1.

|  |
| --- |
| MIH Header Fields (SID=3, Opcode=1, AID=16) |
| **Source Identifier** = sending MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID  (Destination MIHF ID TLV) |
| CTRLmessage  (Control Information TLV) |

* + - 1. MIH\_CTRL\_Transfer response

This message is used to respond to MIH\_CTRL\_Transfer request message. Moreover, this message can deliver control messages such as ANQP and ANDSF message. The delivery of control messages is described in 12.3. The corresponding MIH primitive of this message is defined in 7.4.33.3.

|  |
| --- |
| MIH Header Fields (SID=3, Opcode=2, AID=16) |
| **Source Identifier** = sending MIHF ID  (Source MIHF ID TLV) |
| **Destination Identifier** = receiving MIHF ID  (Destination MIHF ID TLV) |
| CTRLmessage  (Control Information TLV) (optional) |

1. MIH protocol protection


   3. Key establishment through an MIH service access authentication

***Replace text in the first paragraph of 9.2.2 with the following:***

* + 1. Key derivation and key hierarchy

Upon a successful MIH service access authentication, the authenticator (i.e., the serving PoS) obtains a master session key (MSK), a re-authentication master session key (rMSK) via EAP to generate a root key *K* shared between the MN and the serving PoS. Alternatively, the root key *K* may be securely exchanged with the serving PoS from another trusted PoS (e.g., OPoS) using the transfer mechanism specified in 10.4. In the latter case, the MIHF identifier of the MN, Nonce-T, generated by the MN and Nonce-N, generated by the OPoS are also transferred together with *K*. Nonce-T is generated as follows: Nonce-T = PRF(Nonce-T’ || MN\_MIHF\_ID), where Nonce-T’ is provided by the MN and MN\_MIHF\_ID is the MN’s MIHF identity. Similarly, PoS generates Nonce-N by first generating a random number Nonce-N’. Then Nonce-N = PRF(Nonce-N’ || POS\_MIHF\_ID), where POS\_MIHF\_ID is the PoS’s MIHF identity.

The keys derived from *K* include a 128 bit authentication key (MIAK) used to generate a value AUTH, the session keys determined by the ciphersuite code *c* agreed upon between the MN and the serving PoS. If no ciphersuite code is specified by the MN, the default ciphersuite code is used as specified in Table 25. The session keys used for MIH message protection consist of an encryption key (MIEK) only, an integrity key (MIIK) only, or both an encryption key (MIEK) and an integrity key (MIIK). The concatenation of MIAK, MIEK and MIIK is called the media independent session key (MISK). The length, *L*, of the MISK is specified in 9.2.3. When (D)TLS is not used to establish the MIH security association between MN and TPoS, the default SALifeTime for MISK and derived keys is 65,536 seconds (slightly over 18 hours). This value may be overridden by passing a preferred value as the SALifeTime parameter in relevant MIH primitives.

***Replace the definition of the key derivation key K, in 9.2.2 of 802.21a, with the following:***

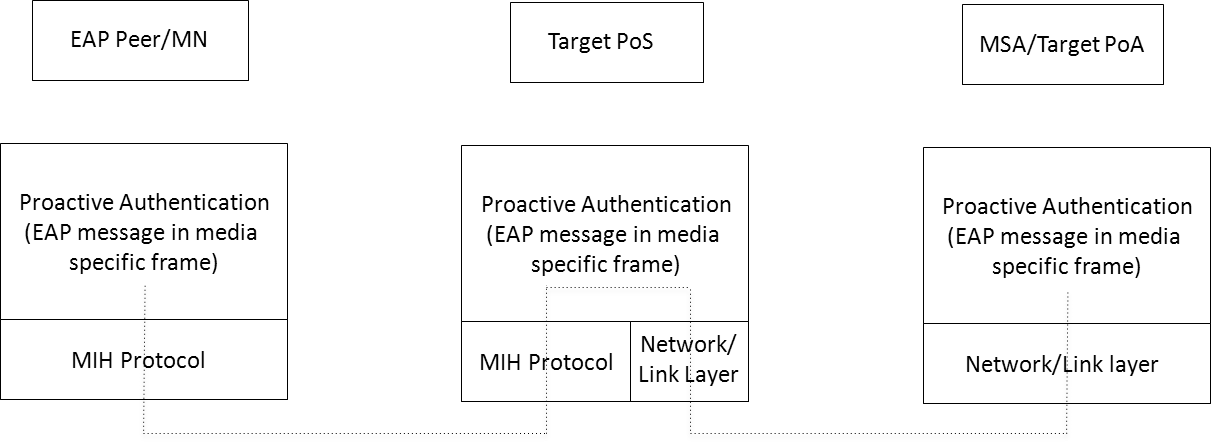
*K* - key derivation key. It is truncated from a master session key (MSK) or re-authentication MSK (rMSK), or obtained by key exchange with another trusted PoS (e.g see 10.3). The length of *K* is determined by the pseudorandom function (PRF) used for key derivation. If HMAC-SHA-1 or HMAC-SHA-256 is used as a PRF, then the full MSK or rMSK is used as the key derivation key *K*. If CMAC-AES is used as a PRF, then the first 128 bits of MSK or rMSK are used as the key derivation key *K*.

1. Proactive Authentication
   1. Media specific proactive authentication

***Change first paragraph of 10.1 as follows:***

In a media access proactive authentication, a Target PoS passes authentication messages between the mobile node and a media specific authenticator (MSA). The protocol stacks in each interface are illustrated in Figure 46 and Figure 47. In scenarios where MSA/Target PoA is reachable via same media as MN and TPoS, EAP messages received at TPoS are directly forwarded to the target PoA. In an optimized pull key distribution, OPoS passes authentication messages between the mobile node, the target PoS and a media specific authenticator (MSA).

***Replace Figure 46 as follows:***



***Insert figure, renumber existing figure 47 to Figure 48***

Figure 47—Protocol Stack for MIH Supported optimized pull key distribution with two Points of Service.

***Insert second paragraph of 10.1 below Figure 47 as follows:***

Figure 47 illustrates the protocol stacks and message passing when the Originating PoS is in a different network than the TPoS.

* 1. Bundling media access authentication with MIH service access authentication
     1. Media specific key derivation

        2. Derivation of media specific pairwise master keys (MSPMKs)

***Change Figure number 47 in 10.2.1.2 to Figure number 48***

Figure ~~47~~ 48 —Key Hierarchy for Bundle Case

***Insert 10.3 and 10.4 and 10.5***

* 1. Establishing MIH Security Association between roaming partners

The PoS is a convenient and natural place to locate security services, and roaming partners have in place agreements that can be used to beneficially establish the needed security agreements between different PoS modules in partner networks. It is expected that the PoS functions in partner networks must often communicate by data paths that traverse the external Internet; in such cases, a secure communication channel must exist or must be established between the partners. It is out of scope for this document to specify exactly how the secure communication channel should be established, but this can be done by configuration when the partners enter into their roaming agreement. It can also be done on demand by using IKEv2 [IETF RFC 5996]. The following overview describes in more detail the circumstances enabling dynamic establishment of security association between OPoS and TPoS.



Figure 49: MN handover signaling for preregistration using OPoS.

MIH\_Prereg\_Xfer and MIH\_N2N\_Prereg\_Xfer messages exchanged between OPoS and TPoS may require security protection. Furthermore, TPoS may reject these messages from an unauthorized originating PoS. To protect the link between OPoS and TPoS, several approaches are possible.

An MIH SA (Security Association) (see clause 3)[IEEE 802.21a] can be used for protecting the communications between OPoS and TPoS. In this case, OPoS acts as the initiating end-point of an MIH SA and TPoS as the other end-point of the MIH SA. The MIH SA can be established using (D)TLS over MIH or EAP over MIH (see clause 9.2) [IEEE 802.21a].

Other mechanisms for providing message integrity and confidentiality, such as IPSec and TLS over TCP can also be used for protecting the communications between OPoS and TPoS.

* 1. Key generation and distribution by OPoS

Except for the initial network attach, by the time an MN enters a network, it can also have a security relationship with the PoS in that network by using MIH\_Prereg\_Xfer commands. For each newly visited network, this security relationship can be created on demand, enabled by signaling from another PoS. The PoS creating the visited security relationship can either be the MN's home PoS (HPoS, a PoS in MN's home network), or the PoS in the network previously visited by the MN. When the MN first attaches to one of the partner networks of the roaming partners, it is either the MN's home network, or a visited network. If the first attachment is to the MN's home network, then the MN is expected to already have a security association with HPoS; otherwise, the MN can bootstrap this security association with the assistance of HPoS, IKEv2 or standard AAA mechanisms or other proprietary means.

After initial attachment, there is signaling defined so that at all times the MN has a security association with the PoS in the network at its current point of attachment, i.e. OPoS. As the MN moves from one partner network to the next target network, the MN establishes or renews a security association with the PoS in the target network, TPoS. When handover is completed, TPoS naturally begins to play the role of the MN’s serving PoS, and subsequently when a handover is required, TPoS plays the role of OPoS.

In order to enable a wider application of high-performance handovers and in particular preregistration signaling, security must be guaranteed for the control traffic. As described above, this signaling traffic is mediated by the PoS in each target network, which may be unknown to the MN until the need for handover has been determined. In such cases, for secure signaling, the MN needs to establish a security association with TPoS. The procedure of establishing such a security association can be quite time consuming and often expensive in processor cycles as well. This clause specifies a fast, straightforward method for providing security associations as needed between the MN and TPoS in any target network within the networks covered by the roaming partners.

This specifies one algorithm to allow OPoS to distribute a key derivation key *K* to the MN and to its desired TPoS. The key derivation key is then used to derive other keys that are used as the basis for a secure communications channel between the MN and the TPoS, enabling further secure preregistration activities. The notation used in this clause for PoS-based handover keys is listed in Table 26.

Table 26 — Notation for OPoS-based exchange of key derivation key *K*

|  |  |
| --- | --- |
| *K* | Key derivation key |
| *K*opos | Encryption key (i.e., MIAK (MN, OPoS)) between MN and OPoS |
| *K*otpos | Encryption key between OPoS and TPoS |
| PRFopos | pseudo-random function between MN and OPoS |
| PRFotpos | pseudo-random function between OPoS and TPoS |

Because of previous protocol operations (e.g., derivation of MIAK upon arrival in the originating network), the MN has a current security association with OPoS. This security association is bidirectional and based on a shared key *K*opos.

Suppose the MN determines to move to a new network, the target network; for preregistration, the MN needs to use the PoS in target network, i.e., TPoS. Before it can do this, it needs to discover the address of TPoS and establish a security association with TPoS by exchanging MISK as described in clause 9.2.2.

For this purpose, MN can make use of its existing security association with OPoS, because OPoS either already has, or can readily establish, a security association with TPoS; suppose OPoS already has the required security association with TPoS. Then, when MN begins forwarding preregistration traffic to TPoS via OPoS, OPoS will provide MN and TPoS with a key derivation key, *K*, for use to derive MIAK which can be used to protect the remainder of the MN's signaling traffic with TPoS. OPoS thus forwards the initial traffic to TPoS on behalf of the MN; the OPoS uses its own security relationship with TPoS to protect this initial preregistration signaling, and it also supplies the value of *K* to TPoS by adding a new extension to the preregistration traffic.

To send *K* to TPoS, OPoS provides the following payload within the TLVs of MIH\_N2N\_Prereg\_Xfer Request (see clause 7.4.31.1):

Payload = MNID, Nonce-T, Nonce-N, [*K* ⊕ PRFotpos (MNID, Nonce-T, Nonce-N)]

Upon receiving this payload, TPoS calculates PRFotpos (MNID, Nonce-T, Nonce-N) and XORs the result to the third parameter of the payload to recover *K*.

Similarly, to send *K* to MN, OPoS provides the following payload as a parameter to MIH\_Prereg\_Xfer Response (see clause 7.4.30.3):

Payload = TPoSIdentifier, Nonce-N, [*K* ⊕ PRFopos (TPoSIdentifier, Nonce-N)]

Upon receiving the payload, MN calculates PRFopos (TPoSIdentifier, Nonce-T, Nonce-N) and XORs the result to the third parameter of the payload to recover *K*.

Alternatively, for either of these messages, OPoS could encrypt the entire contents by using *K*otpos or *K*opos, the keys OPoS has available with TPoS and MN respectively. MN is allowed to send more signaling information to TPoS via OPoS even after OPoS distributes the keys; OPoS continues to forward traffic back and forth between MN and TPoS as needed until both endpoints have used *K* to derive the required security associations. For best performance and least likelihood of congestion at OPoS, MN and TPoS should begin to use direct signaling as soon as possible and thus bypass OPoS. Other structures for the message payloads are also possible, depending on requirements.

Once the handover is completed, TPoS "becomes" OPoS and the handover cycle can begin anew whenever MN determines the need for the next handover.

* 1. TPoS selection by OPoS

It is possible for OPoS to take a more active role to promote smooth handover. When the MN determines the need for handover, but does not already know the address of the TPoS for the intended target network, the MN can start the preregistration sequence by sending all the known information to the OPoS. If OPoS has access to information about each surrounding networks, and information about the MIH PoS in each such surrounding network, OPoS can make a determination about which target network may best be able to provide connectivity and service to the MN. This also depends on OPoS having access to location and configuration information about the MN – for example which radio access technologies (RATs) are configured for operation on the MN. When the candidate TPoS is in another operator’s network, it may be also important the OPoS should have a security relationship with a candidate TPoS, in order to avoid interference from malicious nodes. This would typically mean that the operators are also roaming partners.

Subsequently, the OPoS will provide the address of the TPoS to the MN along with *K*, as described above. The exact nature of the information about TPoS provided by the MN is dependent on the radio access technology type (RAT) of the target network, and is outside the scope of this document.

# Bibliography

(informative)

***Insert these informative references in appropriate order.***

1. IEEE 802 standard, “IEEE Draft Standard for Local and metropolitan Area Networks: overview and Architecture”, P802-D1.4, June 2012.
2. 3GPP, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access,” TS23.401.
3. 3GPP, “3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture enhancements for non-3GPP accesses,” TS23.402
4. WiMAX Forum Network Architecture: Stage 3 Detailed Protocols and Procedures T33-001-R015
5. WiMAX Forum, “Single radio interworking between Non-WiMAX and WiMAX Access Networks,” WMF-T37-011-R016v01, Nov 30, 2011.
6. WiMAX Forum, “WiFi-WiMAX Interworking,” WMF-T37-010-R016v01.
7. 3GPP2, “WiMAX-HRPD Interworking: Core network aspects,” X.S0058.
8. IETF RFC 6153 (2011-02), DHCPv4 and DHCPv6 Options for Access Network Discovery and Selection Function (ANDSF) Discovery

***Change the informative reference [B31] as follows:***  [B31] IETF ~~Internet Draft~~ RFC 5677 (~~draft-ietf-mipshop-mstp-solution-04.txt, 2008-05~~2009-12), Mobility Services Framework Design (MSFD).

# 

# 

# 

# 

***Insert following Data Type to Table E.1.***

|  |  |  |  |
| --- | --- | --- | --- |
| MIH\_LINK\_SAP\_primitive | | IEEE Std 802.16 C\_SAP | IEEE Std 802.16 M\_SAP |
| Link\_Action | Link\_RX\_ON | N/A | N/A |

# 

## 

## 

## Derived data types

### 

### 

***Change the following row in Table F.2:***

|  |  |  |
| --- | --- | --- |
| STATUS | ENUMERATED | The status of a primitive execution.  0: Success  1: Unspecified Failure  2: Rejected  3: Authorization Failure  4: Network Error  5: Authentication Failure  6:TPoS is identical to OPoS, use *K*opos  7: Requested CiphersuiteCode Not Available |

### 

### Data types for link identification and manipulation

(normative)

***Insert number 5 in the description of LINK\_PARAM\_GEN in Table F.4 in F3.4***

|  |  |  |
| --- | --- | --- |
| Data type name | Derived form | Description |
| LINK\_PARAM\_GEN | UNSIGNED\_INT(1) | 5: Average power consumption in active state- the parameter value is represented as an UNSIGNED\_INT(2). Its measure is mW. See Annex R.3 for examples.  Value Range: 0 – 216-1 mW  6-255: (Reserved) |

***Insert Following Data Type to Table F.5 in F3.5***

|  |  |
| --- | --- |
| Action name | Description |
| Link\_RX\_ON | Turn on only the receiver of the radio |

### 

### 

### 

### Data types for information elements

***Change Table F.13 in F3.8 as follows:***

**Table F.13 – Data types for information elements**

|  |  |  |
| --- | --- | --- |
| Data type name | Derived from | Definition |
| NET\_CAPS | BITMAP(32) | These bits provide high level capabilities supported on a network.  Bitmap Values:  Bit 0: Security – Indicates that some level of security is supported when set.  Bit 1: QoS Class 0 – Indicates that QoS for class 0 is supported when set  Bit 2: QoS Class 1 – Indicates that QoS for class 1 is supported when set  Bit 3: QoS Class 2 – Indicates that QoS for class 2 is supported when set; Otherwise, no QoS for class 2 support is available.  Bit 4: QoS Class 3 – Indicates that QoS for class 3 is supported when set; Otherwise, no QoS for class 3 support is available.  Bit 5: QoS Class 4 – Indicates that QoS for class 4 is supported when set; Otherwise, no QoS for class 4 support is available.  Bit 6: QoS Class 5 – Indicates that QoS for class 5 is supported when set; Otherwise, no QoS for class 5 support is available.  Bit 7: Internet Access – Indicates that Internet access is supported when set; Otherwise, no Internet access support is available.  Bit 8: Emergency Services – Indicates that some level of emergency services is supported when set; Otherwise, no emergency service support is available.  Bit 9: MIH Capability – Indicates that MIH is supported when set; Otherwise, no MIH support is available.  Bit 10: SRHO Capability – Indicates that SRHO is supported when set; Otherwise, no SRHO support is available.  Bit ~~10~~ 11–31: (Reserved) |
| IP\_TUNN\_MGMT | BITMAP(16) | Indicates the supported tunnel management protocol on PoS.  Bitmap Values:  Bit 0: IPSec  Bit 1–15: (Reserved) |

### 

### 

### 

### 

***Change MIH\_CMD\_LIST data type definition as follows.***

|  |  |  |
| --- | --- | --- |
| MIH\_CMD\_LIST | BITMAP(32) | A list of MIH commands.  Bitmap Values:  Bit 0: MIH\_Link\_Get\_Parameters  Bit 1: MIH\_Link\_Configure\_Thresholds  Bit 2: MIH\_Link\_Actions  Bit 3: MIH\_Net\_HO\_Candidate\_Query  MIH\_Net\_HO\_Commit  MIH\_N2N\_HO\_Query\_Resources  MIH\_N2N\_HO\_Commit  MIH\_N2N\_HO\_Complete  Bit 4: MIH\_MN\_HO\_Candidate\_Query  MIH\_MN\_HO\_Commit  MIH\_MN\_HO\_Complete  Bit 5: MIH\_Prereg\_Xfer  MIH\_Prereg\_Ready  MIH\_N2N\_Prereg\_Xfer  MIH\_CTRL\_Transfer  Bit 6~~5~~–31: (Reserved) |

### 

### 

### 

### Data type for security

***Change following Data Types into Table F.24 in F.3.16 [802.21a]***

|  |  |  |
| --- | --- | --- |
| Data | Derived from | Definition |
| LL\_FRAMES | OCTET\_STRING | ~~Represents the information needed to carry out a key installation.~~ One or more link-layer frame(s). |

***Insert F.3.17 after F.3.16:***

### Data types for delivery of control messages

***Insert Table F.25 as follows:***

**Table F.25- Data types for delivery of control messages**

|  |  |  |
| --- | --- | --- |
| Data type name | Derived form | Definition |
| CTRL\_PROT\_MSGS | SEQUENCE(  CTRL\_TYPE,  CTRL\_MSGS  ) | Represent which control messages are delivered. CTRL\_TYPE represents a type of control messages. CTRL\_MSGS represents control messages to be delivered. |
| CTRL\_TYPE | UNSIGNED\_INT(1) | Indicates the type of the control message.  0: Reserved  1: ANQP  2: ANDSF  3..127: Reserved for other control message types  128..255: Reserved for vendor-specific message types |
| CTRL\_MSGS | OCTET\_STRING | Represents control messages to be delivered. |

# 

(normative)

***Insert following Information element identifiers values into Table G.1***

**Table G.1—Information element identifier values**

|  |  |
| --- | --- |
| Name of information element or container | IE Identifier |
| IE\_PoS\_TUNN\_MGMT\_PRTO | 0x10000209 |
| IE\_PoS\_NAI | 0x1000020A |

# 

***Change the following text in IEEE 802.21a-2012 shown:***

<owl:Class rdf:ID="POA">

<rdfs:subClassOf>

<owl:Restriction>

<owl:onProperty rdf:resource="#ie\_poa\_mac\_addr"/>

<owl:cardinality rdf:datatype="&xsd;nonNegativeInteger">1

</owl:cardinality>

</owl:Restriction>

</rdfs:subClassOf>

<rdfs:subClassOf>

<owl:Restriction>

<owl:onProperty rdf:resource="#ie\_poa\_location"/>

<owl:cardinality rdf:datatype="&xsd;nonNegativeInteger">1

</owl:cardinality>

</owl:Restriction>

</rdfs:subClassOf>

<rdfs:subClassOf>

<owl:Restriction>

<owl:onProperty rdf:resource="#ie\_poa\_channel\_range"/>

<owl:cardinality rdf:datatype="&xsd;nonNegativeInteger">1

</owl:cardinality>

</owl:Restriction>

</rdfs:subClassOf>

<rdfs:subClassOf>

<owl:Restriction>

<owl:onProperty rdf:resource="#ie\_poa\_system\_info"/>

<owl:cardinality rdf:datatype="&xsd;nonNegativeInteger">1

</owl:cardinality>

</owl:Restriction>

</rdfs:subClassOf>

<rdfs:subClassOf>

<owl:Restriction>

<owl:onProperty rdf:resource="#ie\_poa\_subnet\_info"/>

<owl:minCardinality rdf:datatype="&xsd;nonNegativeInteger">1

</owl:minCardinality>

</owl:Restriction>

</rdfs:subClassOf>

<rdfs:subClassOf>

<owl:Restriction>

<owl:onProperty rdf:resource="#ie\_poa\_ip\_addr"/>

<owl:minCardinality rdf:datatype="&xsd;nonNegativeInteger">1

</owl:minCardinality>

</owl:Restriction>

</rdfs:subClassOf>

<rdfs:subClassOf>

<owl:Restriction>

<owl:onProperty rdf:resource="#ie\_authenticator\_link\_addr"/>

<owl:cardinality rdf:datatype="&xsd;nonNegativeInteger">1

</owl:cardinality>

</owl:Restriction>

</rdfs:subClassOf>

<rdfs:subClassOf>

<owl:Restriction>

<owl:onProperty rdf:resource="#ie\_authenticator\_ip\_addr"/>

<owl:minCardinality rdf:datatype="&xsd;nonNegativeInteger">1

</owl:minCardinality>

</owl:Restriction>

</rdfs:subClassOf>

<rdfs:subClassOf>

<owl:Restriction>

<owl:onProperty rdf:resource="#ie\_pos\_ip\_addr"/>

<owl:minCardinality rdf:datatype="&xsd;nonNegativeInteger">1

</owl:minCardinality>

</owl:Restriction>

</rdfs:subClassOf>

<rdfs:subClassOf>

<owl:Restriction>

<owl:onProperty rdf:resource="#ie\_pos\_tunnel\_mgmt\_prto"/>

<owl:minCardinality rdf:datatype="&xsd;nonNegativeInteger">1

</owl:minCardinality>

</owl:Restriction>

</rdfs:subClassOf>

<rdfs:subClassOf>

<owl:Restriction>

<owl:onProperty rdf:resource="#ie\_pos\_nai"/>

<owl:minCardinality rdf:datatype="&xsd;nonNegativeInteger">1

</owl:minCardinality>

</owl:Restriction>

</rdfs:subClassOf>

***Insert the following prior to </rdf:RDF>:***

<owl:ObjectProperty rdf:ID="ie\_pos\_tunnel\_mgmt\_prto">

<mihbasic:ie\_type\_identifier>0x10000209</mihbasic:ie\_type\_identifier>

<rdfs:domain rdf:resource="#POA"/>

<rdfs:range rdf:resource="#bit\_number"/>

<rdfs:comment>

The range of #bit\_number is 0-15.

</rdfs:comment>

</owl:ObjectProperty>

<owl:DatatypeProperty rdf:ID="ie\_pos\_ip\_nai">

<mihbasic:ie\_type\_identifier>0x1000020a</mihbasic:ie\_type\_identifier>

<rdfs:domain rdf:resource="#POA"/>

<rdfs:range rdf:resource="&xsd;string"/>

</owl:DatatypeProperty>

# 

# 

***Change the following text in IEEE 802.21a-2012 as shown:***

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

-- \* MODULE IDENTITY

-- \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

ieee802dot21 MODULE-IDENTITY

LAST-UPDATED "201306082200Z~~201105161205Z~~"

ORGANIZATION "IEEE 802.21"

CONTACT-INFO

"WG E-mail: stds-802-21@ieee.org

Chair: Subir Das

Advanced Communication Sciences~~Telcordia Technologies~~

E-mail: sdas@appcomsci.com~~subir@research.telcordia.com~~

Editor: David Cypher

E-mail: david.cypher@nist.gov"

DESCRIPTION

"The MIB module for IEEE 802.21 entities.

iso(1).std(0).iso8802(8802).ieee802dot21(21)"

REVISION "201306082200Z~~201105161205Z~~"

DESCRIPTION

"The latest version of this MIB module."

::= { iso std(0) iso8802(8802) ieee802dot21(21) }

***Change the following text in IEEE 802.21-2008 as shown:***

Dot21CommandList ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

"This attribute represents a list of supported commands."

REFERENCE "IEEE Std 802.21, 2008 Edition, F.3.12"

SYNTAX BITS

{ mihGetLinkParameters(0),

mihLinkConfigureThresholds(1),

mihLinkActions(2),

mihNetworkHandoverCommands(3),

mihMobileHandoverCommands(4),

mihSingleRadioHandoverCommands(5) }

***Change the following text in IEEE 802.21a-2012 as shown:***

Dot21ISQueryTypeList ::= TEXTUAL-CONVENTION

STATUS current

DESCRIPTION

" This attribute will be a set of supported MIH IS query types."

REFERENCE "IEEE Std 802.21, 2008 Edition, F.3.12"

SYNTAX BITS

{ binary(0),

rdfData(1),

rdfSchemaUrl(2),

rdfSchema(3),

typeIeNetworkType(4),

typeIeOperatorIdentifier(5),

typeIeServiceProviderIdentifier(6),

typeIeCountryCode(7),

typeIeNetworkIdentifier(8),

typeIeNetworkAuxiliaryIdentifier(9),

typeIeRoamingPartners(10),

typeIeCost(11),

typeIeNetworkQos(12),

typeIeNetworkDataRate(13),

typeIeNetworkRegulatoryDomain(14),

typeIeNetworkFrequencyBands(15),

typeIeNetworkIpConfigurationMethods(16),

typeIeNetworkCapabilities(17),

typeIeNetworkSupportedLcp(18),

typeIeNetworkMobilityManagementProtocol(19),

typeIeNetworkEmergencyServiceProxy(20),

typeIeNetworkImsProxyCscf(21),

typeIeNetworkMobileNetwork(22),

typeIePoaLinkAddress(23),

typeIePoaLocation(24),

typeIePoaChannelRange(25),

typeIePoaSystemInformation(26),

typeIePoaSubnetInformation(27),

typeIePoaIpAddress(28),

typeIeAuthenticatorLinkAddress(29),

typeIeAutheticatorIpAddress(30),

typeIePosIpAddress(31),

typeIeTunnMgmtPrto (32),

typeIePosNai (33)

# 

# 

(normative)

***Insert the following rows to Table L.1***

|  |  |
| --- | --- |
| MIH messages | AID |
| MIH messages for Command Service | |
| MIH\_Prereg\_Xfer | 13 |
| MIH\_N2N\_Prereg\_Xfer | 14 |
| MIH\_Prereg\_Ready | 15 |
| MIH\_CTRL\_Transfer | 16 |

***Insert the following TLVs to Table L.2***

|  |  |  |
| --- | --- | --- |
| TLV type Name | TLV type value | Data type |
| TPoS Identifier TLV | 78 | MIHF\_ID |
| Ciphersuite Code TLV | 79 | BITMAP(8) |

# 

***Insert the following row to Table M.3***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| M.8.3.10 | Is optimized single-radio handover supported? | 5.2.3, 5.4.4, 5.5.8, 5.8, 5.9 | O | Yes [] No [] | MC10 |
| M.8.3.11 | Is Key Generation supported? | 9.2.2 | O | Yes [ ] No [ ] | MC11 |

***Insert the following rows to Table M.4***

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| M.8.4.43 | MIH\_Prereg\_Xfer request | 8.6.3.24 | O | Yes [ ] No [ ] | PDU43 |
| M.8.4.44 | MIH\_Prereg\_Xfer response | 8.6.3.25 | O | Yes [ ] No [ ] | PDU44 |
| M.8.4.45 | MIH\_N2N\_Prereg\_Xfer request | 8.6.3.26 | O | Yes [ ] No [ ] | PDU45 |
| M.8.4.46 | MIH\_N2N\_Prereg\_Xfer response | 8.6.3.27 | O | Yes [ ] No [ ] | PDU46 |
| M.8.4.47 | MIH\_Prereg\_Ready request | 8.6.3.28 | O | Yes [ ] No [ ] | PDU47 |
| M.8.4.48 | MIH\_Prereg\_Ready response | 8.6.3.29 | O | Yes [ ] No [ ] | PDU48 |
| M.8.4.49 | MIH\_CTRL\_Transfer request | 8.6.3.30 | O | Yes [ ] No [ ] | PDU49 |
| M.8.4.50 | MIH\_CTRL\_Transfer response | 8.6.3.31 | O | Yes [ ] No [ ] | PDU50 |

# 

(informative)

## 

## 

## 

## 

***Change the Annex number N.6[802.21a] to N.5***

## ~~N.6~~ Terminating Phase

***Insert new Annex N.6***

## MIH\_Prereg\_Xfer messages for Optimized SA Establishment

### OPoS distributing key derivation key *K* to TPoS and MN



Figure N.7 -- OPoS distributing key derivation key *K* to TPoS and MN

The signaling diagram illustrated in Figure N.7 shows the following steps

1. MIH\_Prereg\_Xfer.request: the MN user application asks to initiate preregistration to a suitable target PoA (TPoA)
2. MIH\_Prereg\_Xfer Request: MN’s MIHF transmits request to Originating PoS (OPoS)
3. MIH\_Prereg\_Xfer.indication: OPoS presents MN’s Request to OPoS MIH application.
4. MIH\_N2N\_Prereg\_Xfer.request: issued by OPoS MIH application containing information to enable TPoS to compute *K*
5. MIH\_N2N\_Prereg\_Xfer Request: relayed by OPoS to TPoS, possibly encapsulated with IPSec
6. MIH\_ N2N\_Prereg\_Xfer.indication: presented to TPoS MIH application for extraction of *K* and computation of MNmsrk (i.e., MSPMK between MN and TPoA).
7. TPoS MIH application provides MIAK and any other appropriate keys to AAA for future authentication purposes
8. TPoS MIH application computes MNmsrk from *K* and sends appropriate LL frames to TPoA for key distribution and any other preregistration tasks.
9. MIH\_N2N\_Prereg\_Xfer.response: TPoS MIH application initiates message for OPoS MIH application containing MN\_NAI.
10. MIH\_N2N\_Prereg\_Xfer Response: TPoS relays message to OPoS containing MN\_NAI.
11. MIH\_N2N\_Prereg\_Xfer.confirm: OPoS presents message to OPoS MIH application containing MN\_NAI.
12. MIH\_Prereg\_Xfer.response: OPoS MIH application initiates message to MN user application via OPoS containing MN\_NAI, *K*.
13. MIH\_Prereg\_Xfer Response: OPoS relays message to MIHF running on MN containing MN\_NAI, *K*.
14. MIH\_Prereg\_Xfer. confirm: MIHF running on MN relays message to MN user application containing MN\_NAI, *K*.
15. MN user application extracts *K*, computes MNmsrk, continues any necessary preregistration activities
16. MN continues with additional preregistration signaling

The call flow illustrated in Figure N.7 shows how the identity is bootstrapped by TPoS, how *K* is sent by OPoS to TPoS and how the MSPMK is installed into the TPoA (AAA). Notice that the PoA in the originating network does not conceptually play any role in the signal handling, even though signals exchanged between the MN and the OPoS are transmitted by way of the originating PoA.

### OPoS relays additional Preregistration signaling



Figure N.8 -- OPoS relays additional Preregistration signaling

The signaling diagram illustrated in Figure N.8 shows the following steps

1. MIH\_Prereg\_Xfer.request: the MN user application asks to continue preregistration to a suitable target PoA (TPoA)
2. MIH\_Prereg\_Xfer Request: MN’s MIHF transmits request to Originating PoS
3. MIH\_Prereg\_Xfer.indication: OPoS presents MN’s Request to OPoS MIH application.
4. MIH\_N2N\_Prereg\_Xfer.request: issued by OPoS MIH application relaying MN additional preregistration signaling to TPoS
5. MIH\_N2N\_Prereg\_Xfer Request: relayed by OPoS to TPoS, possibly encapsulated with IPSec
6. MIH\_ N2N\_Prereg\_Xfer.indication: presented to TPoS MIH application for continuation of preregistration signaling
7. TPoS relays preregistration signaling to TPoA
8. TPoA contacts AAA for authentication
9. TPoA responds with additional preregistration signaling for MN
10. TPoS MIH application relays preregistration signaling from TPoA, possibly including LL frames, to be transmitted to OPoS.
11. MIH\_N2N\_Prereg\_Xfer.response: TPoS MIH application transmits message for OPoS MIH application.
12. MIH\_N2N\_Prereg\_Xfer.confirm: OPoS presents message to OPoS MIH application.
13. MIH\_Prereg\_Xfer.response: OPoS MIH application transmits message to MN user application.
14. MIH\_Prereg\_Xfer Response: OPoS relays message to MIHF running on MN.
15. MIH\_Prereg\_Xfer. confirm: MIHF running on MN relays message to MN user application.
16. MN user application continues any necessary preregistration activities based on signaling received from TPoA.

In Figure N.8, the authentication between the MN and the TPoA is depicted. MNmsrk is as previously installed on the TPoS, shown in the bootstrap procedure in the first figure; TPoA holds the MNmsrk and uses it for media-specific authentication. Therefore, another MNmsrk transfer is not needed.

### OPoS key distribution when OPoS is same as TPoS

Figure N.9 OPoS key distribution when OPoS is same as TPoS.

The signaling diagram illustrated in Figure N.9 shows the following steps.

1. MIH\_Prereg\_Xfer.request: the MN user application asks to initiate preregistration to a suitable target PoA (TPoA)
2. MIH\_Prereg\_Xfer Request: MN’s MIHF relays request to Originating PoS (OPoS)
3. MIH\_Prereg\_Xfer.indication: OPoS presents MN’s request to OPoS MIH application.
4. OPoS MIH application provides MIAK and any other appropriate keys to AAA for future authentication purposes at TPoA
5. OPoS MIH application computes MNmsrk from *K* and sends appropriate LL frames to TPoA for key distribution and any other preregistration tasks.
6. MIH\_Prereg\_Xfer.response: OPoS MIH application initiates message to MN user application via OPoS containing MN\_NAI, *K*. The response message informs MN that TPoS is the same as OPoS.
7. MIH\_Prereg\_Xfer Response: OPoS relays message to MIHF running on MN containing MN\_NAI, *K*.
8. MIH\_Prereg\_Xfer. confirm: MIHF running on MN relays message to MN user application containing MN\_NAI, *K*.
9. MN user application extracts *K*, computes MNmsrk, continues any necessary preregistration activities

When the MN can directly contact the TPoS (this case is the same as when OPoS and TPoS are the same entity), Figure N.9 and the numbered steps apply for authentication at the TPoA.

### OPoS relay preregistration when OPoS is same as TPoS



Figure N.10 OPoS relay preregistration when OPoS is same as TPoS

Finally when the OPoS and TPoS are the same entity and the MIH\_Prereg\_Xfer is used to exchange L2 frames, but no authentication messaging is required, the diagram shown in Figure N.10 can be applied. The signaling diagram illustrated in Figure N.10 shows the following steps.

1. MIH\_Prereg\_Xfer.request: the MN user application asks to initiate preregistration to a suitable target PoA (TPoA)
2. MIH\_Prereg\_Xfer Request: MN’s MIHF relays request to Originating PoS (OPoS)
3. MIH\_Prereg\_Xfer.indication: OPoS presents MN’s request to OPoS MIH application.
4. OPoS MIH application sends appropriate LL frames to TPoA for preregistration tasks such as datapath setup, context transfer, etc.
5. OPoS MIH application receives corresponding LL frames from TPoA to complete preregistration tasks initiated in the previous step.
6. MIH\_Prereg\_Xfer.response: OPoS MIH application initiates message to MN user application via OPoS containing MN\_NAI, *K*. The response message informs MN that TPoS is the same as OPoS.
7. MIH\_Prereg\_Xfer Response: OPoS relays message to MIHF running on MN containing MN\_NAI, *K*.
8. MIH\_Prereg\_Xfer. confirm: MIHF running on MN relays message to MN user application containing MN\_NAI.

# 

***Insert Annex P and Annex Q and Annex R and Annex S***

# MN’s Network Access Identifier Format

(Informative)

An MN\_NAI attribute (of type MIHF\_ID), which is optionally contained in MIH\_Prereg\_Xfer.response, MIH\_Prereg\_Xfer.confirm, MIH\_N2N\_Prereg\_Xfer.response, and MIH\_N2N\_Prereg\_Xfer.confirm primitives, is assigned by the target PoS to the MN such that the MN can use the value of this attribute as the EAP peer identity for subsequent reactive pull key distribution or optimized pull key distribution from the target PoS. The username part of the MIHF\_ID carried in this attribute may contain the identifier of the MSRK used between the MN and the target PoS, and the realm part of the MIHF\_ID may contain a Fully Qualified Domain Name of the target PoS.

# Network discovery for single radio handover

(Informative)

The purpose of Annex Q is to introduce network discovery for single radio handover (SRHO). As shown in clause 1.4, the SRHO has restrictions on the use of radio interfaces to reduce interference between source and target radio interfaces and power consumption of mobile nodes. A mobile node is not free to use the target radio when the originating radio is operating. Annex Q shows methods of network discovery under the restrictions of SRHO.

## Network discovery: listening to the target link

The first method is listening to the target link. When the mobile node can listen to the target link and signal strength of the source link decreases, the mobile node can scan candidate links and then can find the target link. Moreover, periodic scanning for the target link can support network discovery. This method serves the accurate detection of the target links, but the mobile node may follow the assumptions in 1.4.



Figure Q.1- Network discovery listening to the target link.

Figure Q.1 shows the case for network discovery listening to the target link with extended Link\_Action. In (0) and (1), MIHF turns on only the receiver of the candidate radio using Link\_Action message with newly defined action name which is LINK\_RX\_ON. In (2), the candidate link listens to network detection related messages, such as the beacon in an IEEE 802.11 network. In (3), candidate link informs detection of a new link using Link\_Detected message. This method serves the accurate detection of the target links, but the mobile node may follow the assumptions in 1.4.

## Network discovery: using location information

The second method is network discovery based on the location information of the mobile node. This mechanism finds the target network using GPS (Global Positioning System) location information and interacting with the Information Server explained in 5.4.4. This mechanism will avoid the interference explained above. Although location information from global positioning system (GPS) can enhance network detection, the GPS also dissipates power in the mobile node which is often limited by the power capability of its battery. Also, the GPS systems performance is often degraded with the weak signals in an indoor environment. In the event of GPS signal loss, such as when entering a building, the last known location could be used. Moreover, it can be a huge load to the network to invoke a network information repository to support network discovery for the mobile nodes which are equipped with the GPS.



Figure Q.2- Network discovery using location information.

Figure Q.2 shows the case for network discovery using location information of the MN with QUERIER\_LOC. In (1), the MN MIHF sends the location information (QUERIER\_LOC) of the MN through MIH\_Get\_Information request message. In (2), the IR MIHF responds with network access information elements, such as IE\_NETWORK\_TYPE and IE\_NET\_FREQUENCY\_BANDS.

Moreover, scheduled location information can be used for network discovery. The multi-radio MN (i.e., an MN equipped with multiple radio network interfaces) can possess a lightweight software that includes schedule program, e.g., Google calendar, and many users are already managing their schedule through the use of a schedule program such as Google calendar. The schedule program usually shows the user’s location at the dedicated time. Based on user’s location information, the multi-radio MN can determine its available networks and the target radio.

The network discovery using scheduled location information can improve network discovery in indoor environments and reduce the network load. The GPS does not work correctly indoors. The network discovery using the MN’s geo-location information using GPS is not appropriate indoors. Moreover, periodical update of location information results in network load. The scheduled location information is not affected by indoor environment and does not need periodical update of location information. Thus, the network discovery using scheduled location information can be more efficient at indoor and network load than the conventional location information.

A usage of network discovery with the scheduled information is the same as follows. If Mr. Sam is scheduled to stay meeting room from 9AM to 11AM, the Mr. Sam’s multi-radio MN can discover a WLAN AP at the meeting room. In order to enhance this network discovery mechanism, the scheduled information can include the network information including information about link type, link identifier, link availability, link quality as defined in this standard. Using the network information, the mobile node can perform network discovery. If the MN knows the network information, it can try to connect to the network using that information.

In addition, records of user’s network access can enhance network discovery with or without the Information Server. For example, if Mr. Sam had visited “Room #1” and accessed WLAN at some time. When Mr. Sam is scheduled to visit “Room #1” again, the recorded network information will show that Mr. Sam’s MN can connect the WLAN using the recorded WLAN access information.



Figure Q.3- Network discovery using user schedule information.

Figure Q.3 shows the case for network discovery using location information of the MN with QUERIER\_LOC. In (1), the MN MIHF sends the scheduled location information (QUERIER\_LOC) of the MN through MIH\_Get\_Information request message. In (2), the IR MIHF responds with network access information elements, such as IE\_NETWORK\_TYPE and IE\_NET\_FREQUENCY\_BANDS.

# Handover Decision

(Informative)

To decide handover, three representative criteria are considered for handover decision. Criteria to decide handover can be weak SINR (Signal to Interference plus Noise Ratio), QoS and/or cost, and the power consumption of the source link.

## Weak SINR of the source link



Figure R.1- HO decision caused by weak SINR of the source link.

Figure R.1 shows the case for weak SINR of the source link. Through Link\_Going\_Down.indication, the source link interface reports its weak SINR. Afterwards, the MIHF orders the target link interface to initiate preregistration through Link\_Prereg\_Ready.req. Link\_Prereg\_Ready is needed, because preregistration is different from regular registration. While the L2 messages for regular registration are transmitted through the target link, the L2 messages for preregistration are transmitted through higher layer (TCP or UDP/IP) and the source link. After the target link interface prepares preregistration, the target link interface responds with Link\_Prereg\_Ready.confirm.

## QoS and/or cost check



Figure R.2- HO decision caused by QoS and/or cost.

Figure R.2 shows the case of QoS and/or cost check for HO decision. The OPoS consults the QoS and/or cost with TPoS through MIH\_Get\_Information. After OPoS recommends the MN to perform handover, the OPoS transmits MIH\_Prereg\_Ready request message. The MIHF of the MN orders the target link to preregister through Link\_Prereg\_Ready.

## Power consumption comparison of the link interfaces



Figure R.3- HO decision caused by comparison of power consumption.

Figure R.3 shows the HO decision to reduce power consumption of the MN. The MIHF of the MN asks power consumption of each link interface through Link\_Get\_Parameters.request with new LINK\_PARAM\_GEN value, which is 5, and thus the source link interface and the target link interface answers its average power consumption through Link\_Get\_Parameters.confirm. Afterwards, the MIHF of the MN decides to perform handover through Link\_Prereg\_Ready.request, and then the target link interface responds with Link\_Prereg\_Ready.confirm.

# 

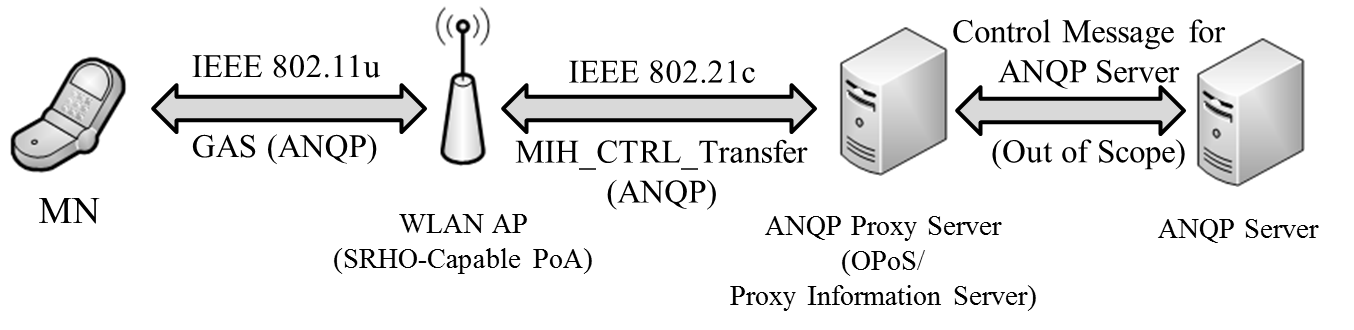
*(Informative)*

**Practical uses of proxy Information Server**

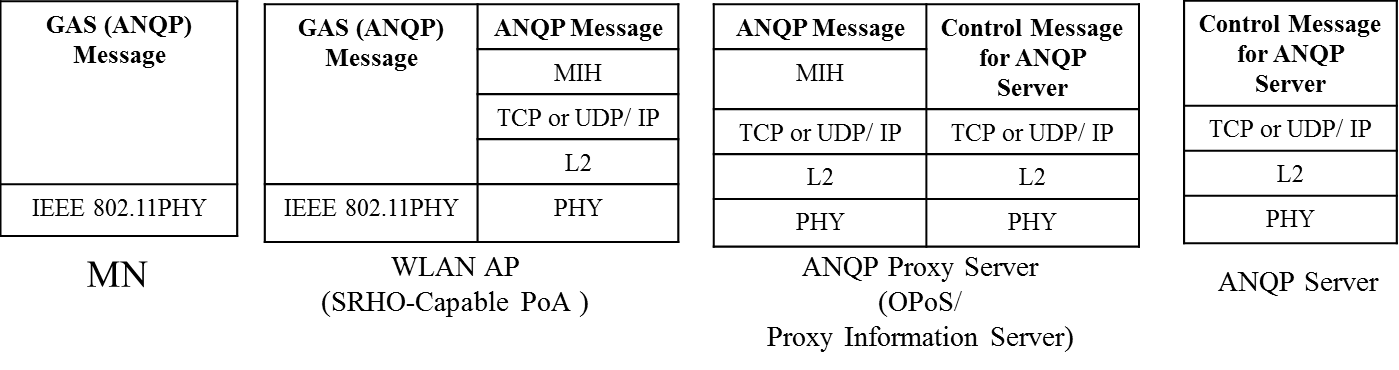
IEEE 802.11u defines a mechanism for the AP to contact an external information service upon receiving an ANQP query from an MN. The functionality of proxy Information Server can be used to simplify the interaction of the AP with heterogeneous information services such as MIIS or ANDSF.

Figure S.1 (a) presents a diagram of the functionality provided by the proxy Information Server. First the MN queries the AP using ANQP. The AP encapsulates this query in a MIH\_CTRL\_Transfer message as shown in Figure S.1 (b), and forwards it to the proxy Information Server. Upon reception of the message, the MIHF at the proxy Information Server decapsulates the message and forwards the ANQP query to the MIH User in charge of the translation function. The MIH User then performs the translation between ANQP and any other protocol used to contact the desired Information Server (e.g., OMA-DM for ANDSF) and it also performs the communication with the external Information Server. The translation and communication functionalities used by the MIH User to contact the external Information Server are out of the scope of this specification.

Once the response is received from the external Information Server, the process is reverted. The MIH User at the proxy Information Server translates the information into an ANQP response and forwards it to the MIHF which encapsulates it in an MIH\_CTRL\_Transfer message and sends it to the AP. The AP then decapsulates the message and forwards the ANQP response to the MN as shown in Figure S.1 (b).



(a) ANQP Message Transfer using proxy Information Server.



(b) Protocol Stacks for ANQP Transfer.

**Figure S. 1 Proxy Information Server for ANQP Transfer.**

Figure S.2 shows proxy Information Server for control message conversion. If the Information Server does not support control messages that the MN can use, MIH User at the proxy Information Server converts the control message (Control Message A) for the MAN into other control message (Control Message B) for the Information Server. The proxy Information Server operates as a proxy of the Information Server to the MN. To the Information Server, the proxy Information Server behaves like the MN that can communicate with the Information Server.

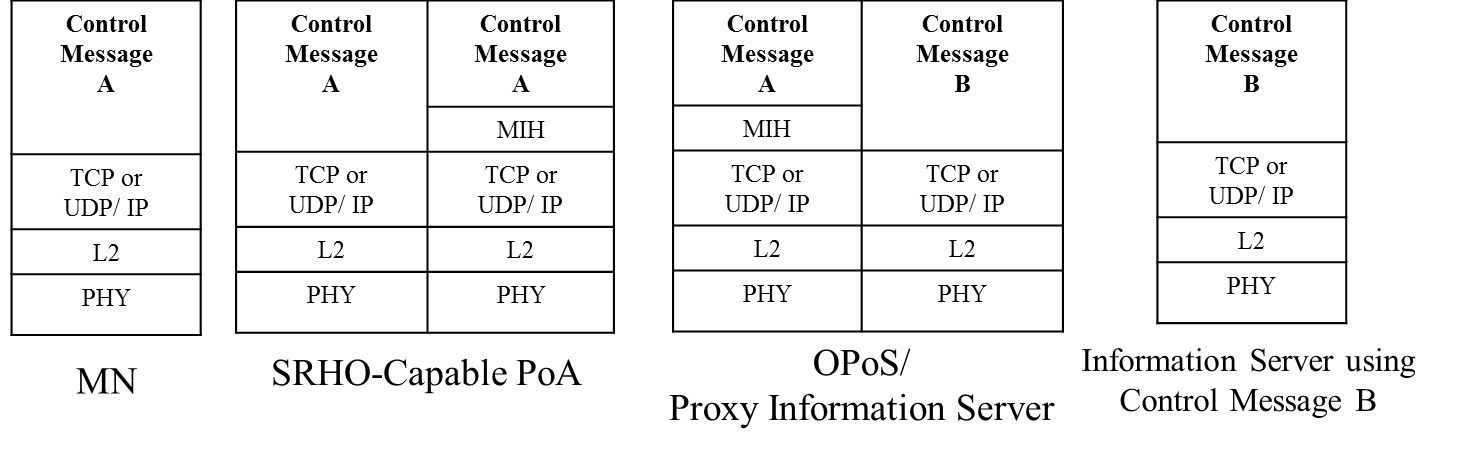


Figure S.2 Proxy Information Server for Control Message Conversion.

If the MN uses ANQP messages but the Information Server uses the other control messages such as ANDSF messages, MIH User at the proxy Information Server needs to convert ANQP messages to the other control messages. For this case, the WLAN AP as the SRHO-capable PoA only encapsulates ANQP messages of the MN into MIH\_CTRL\_Transfer messages and decapsulates MIH\_CTRL\_Transfer messages of information server, as shown in Figure S.3 (a). MIH User at proxy Information Server converts the ANQP messages from the WLAN AP to the other control messages and vice versa. Hence, the MN can communicate with Information Server by using the WLAN AP and the proxy Information Server. To explain the ANQP conversion, the protocol stacks for MN, WLAN AP, Proxy, and Information Server are shown in Figure S.3 (b).



(a) ANQP Message Conversion using the proxy Information Server.



(b) Protocol Stacks for ANQP Conversion

Figure S.3 Proxy Information Server for ANQP Conversion.

1. The Institute of Electrical and Electronics Engineers, Inc.

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

   Copyright © 20XX by the Institute of Electrical and Electronics Engineers, Inc.

   All rights reserved. Published <XX MONTH 20XX>. Printed in the United States of America.

   IEEE is a registered trademark in the U.S. Patent & Trademark Office, owned by the Institute of Electrical and Electronics   
   Engineers, Incorporated.

   **PDF: ISBN 978-0-XXXX-XXXX-X STDXXXXX**

   **Print: ISBN 978-0-XXXX-XXXX-X STDPDXXXXX**

   *IEEE prohibits discrimination, harassment and bullying. For more information, visit* [*http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html*](http://www.ieee.org/web/aboutus/whatis/policies/p9-26.html)*.*

   *No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of the publisher.*  [↑](#footnote-ref-1)
2. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-2)
3. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-3)
4. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-4)
5. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-5)
6. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-6)
7. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-7)
8. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-8)
9. Note that LINK\_TUPLE\_ID includes the LINK\_ID of both sides of the link, the MN and the PoA. [↑](#footnote-ref-9)