Minutes IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IEEE 802.11 TGbh Meeting Minutes, November 8, 2022  Randomized and Changing MAC addresses (RCM) | | | | |
| Date: 2022-11-8 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Stephen Orr | Cisco | New York |  | sorr@cisco.com |
|  |  |  |  |  |

Abstract

This document contains the minutes of the IEEE 802.11bh telecon meeting of November 8, 2022.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting November 8, 2022 9:30 a.m. to 11:30 a.m. ET**

**Chair: Mark Hamilton (Ruckus/CommScope)**

**Vice Chair: Peter Yee (NSA-CSD/AKAYLA)**

**Vice Chair: Stephen Orr (Cisco)**

**Secretary: Peter Yee**

**Editor: Carol Ansley (Cox)**

**The teleconference was called to order by the Chair at 9:32 a.m. EDT.**

Agenda slide deck HYPERLINK "https://mentor.ieee.org/802.11/dcn/22/11-22-2084-00-00bh-agenda-tgbh-2022-dec-1.pptx"11-22/1735r00

1. **Policies and procedures were presented by the chair. (Slides 4 to 14)**

There were no Patent declarations.

Copyright policy slides were presented (Slides 10 and 11)

1. **Agenda:**

* **Attendance, noises/recording, meeting protocol reminders**
* **Policies, duty to inform, participation rules**
* **Organization topics (see Backup slides)**
  + Sept to Nov teleconferences: Tuesdays, every other week, 9:30-11:30 am ET (this time slot)
  + Timeline reminder (slide 20)
* **Issues Tracking:** [**11-21/0332r37**](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* **Results of Comment Collection on D0.2:** [**11-22/0973r13**](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-13-00bh-cc41-comments-against-d0-2.xlsx)
* **Continue discussion on resolutions of ones that are NOT on topics: Opt-in, Pre/un-association, Non-AP STA-generated ID**
  + [11-22/1665r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1665-00-00bh-deviceid-renaming-discussion.pptx) – Device ID renaming discussion (Antonio de la Oliva) (any updates?)
  + [11-22/1588r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1588-00-00bh-resolution-comment-32-11bhd0-2.docx) – Resolution comment 32 (Antonio de la Oliva)
  + [11-22/1599r3](https://mentor.ieee.org/802.11/dcn/22/11-22-1599-03-00bh-revisions-to-rsn-extension-element.docx) – Revisions to RSN Extension element (Kurt Lumbatis) (ready for motion)
  + [11-22/1329r6](https://mentor.ieee.org/802.11/dcn/22/11-22-1329-06-00bh-cid-resolutoins-for-12-2-11.docx) – CID resolutions for 12.2.11 (Kurt Lumbatis)
  + Walk-through CIDs status
  + ~1 hour
* **Contributions on topics: Opt-in, Pre/un-associated, Non-AP STA-generated ID (slide 16)**
  + ~1 hour
* **WBA liaison response**

Any comments?

Q- For the last 2 contributions can you swap the order? Enhancement for RRCM and CR for STA generated ID

1. No objection

Any objections to agenda? [None] – Approved

1. **Resolution for CID19 and CID 20** [**11-22/1732r1**](https://mentor.ieee.org/802.11/dcn/22/11-22-1732-01-00bh-resolution-for-cid19-and-cid20.pptx)

* PASN and FTM
  + Slide 4-5 – recap of PMK and PTK generation for PASN
  + Slide 6 – FTM associated and unassociated STA discussion
  + Possible solutions for CID 19
    - Unencrypted Solution
      * Slide 10 – uses Opaque ID
    - Encrypted v1 – Slide 12
      * AP assigns DevID in Auth Msg2 encrypted
      * Non-AP STA sends Device ID to AP in Auth Msg3 encrypted
    - Encrypted v2 Slide 14
      * AP assigns Device ID in Auth Msg2 Encrypted
      * Non-AP STA send Opaque ID unencrypted
  + CID 20 Slide 16
    - Same as CID 19 but assing a Device ID for each FTM session in ESS
    - A Device ID will be assigned per session in an ESS
  + Review Text of the solutions [**11-22/1806r0**](https://mentor.ieee.org/802.11/dcn/22/11-22-1806-00-00bh-cr-for-pasn.docx)
  + Option 1
    - When using PASN authentication for un-associated STA, the non-AP STA sends the identifier, if it has one and opts-in to using it, in the first PASN frame and the AP sends a new identifier in the second PASN frame.

Q: Can PASN be done by an associated non-AP STA

A: PASN can only be done by an unassociated non-AP STA

C: PASN works in a similar way to FILS (based on a previous association).Text seems confusing on the clarity on when they get exchanged.

A: Text written based on current draft (12.2.11)

C: We need to clarify “the identifier” in the first sentence.

C: The proposal follows the baseline – does not reference the PMK cache

Q: You can’t get a PMK without a full association at some point. The only way a non-AP STA gets a PMK is if it does a full association and a 4WH

A: In PASN it is possible – PMK is generated. Cached PMK and generation a new one.

Q: Through the Public Key Exchange

A: Need to double check

C: Limited number of ways to derive the PMK for PASN (cached or Public Key)

A: Correct

C: Both of those required prior association or a trusted 3rd party

C: The identifier is coming from somewhere – the security and privacy depends on how the identifier is created and shared.

C: This could be a brand new identifier that was just created

C: Then you can’t use PASN

C: Need to check with PASN experts

C: We don’t have consensus on whether the device ID can be validated

C: In order for security mapping to occur – it should be coupled to a previous known shared secret. If it’s a random identifier – none of this security overlay can work

C: Lets table the PASN discussion until we can confer with a PASN epxert

A: Agree

1. [**11-22/1802r0**](https://mentor.ieee.org/802.11/dcn/22/11-22-1802-00-00bh-enhancement-of-rrcm.pptx) **– Enhancement of RRCM (Okan Mutgan)**

* Recap of RRCM Slide 3

Q: The Counter – this could be a potential DoS attack on the AP. If the non-AP STA sets the counter to a large value, this will force the AP to keep state on all RCM for every STA. May be ok in a residential deployment – but could consume significant resources on the AP in an enterprise deployment.

A: The STA sets the counter – however this could be modified.

Q: Is .11be in scope of .11bh?

A: We should keep the impact of MLO for 11be in mind

Q: PMF in an MLO is it per link or one for all links in the MLO

A: Need to check

Q: Question on storing keys – more keys that need to be stored.

C: This could be a way to protect ANQP frames

Q: Some of these topics are already being discussed in TGbi. TGbh was supposed to be a “quick solution” – this may be easier to roll into TGbi and coordinate. Maybe have a joint TGbh/bi meeting to discuss who is addressing what.

Chair: The chairs can coordinate to make sure both groups are not overlapping

C: Scope of this idea is really broad. Sometimes one group will define something and another group can use it. Things can be used in other groups.

Chair: Maybe TGbh could start with proposing something and TGbi could leverage it and enhance.

1. **WBA liaison response**

We will come back to this when we have something substantive to tell them.

**Meeting adjoined at 11:09 a.m. EDT.**

**Attendance**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 11/8 | Ansley, Carol | Cox Communications Inc. |
| TGbh | 11/8 | Chng, Shi Baw | BAWMAN LLC |
| TGbh | 11/8 | DeLaOlivaDelgado, Antonio | InterDigital, Inc. |
| TGbh | 11/8 | Haasz, Jodi | IEEE SA |
| TGbh | 11/8 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 11/8 | Henry, Jerome | Cisco Systems, Inc. |
| TGbh | 11/8 | Huang, Po-Kai | Intel Corporation |
| TGbh | 11/8 | Levy, Joseph | InterDigital, Inc. |
| TGbh | 11/8 | McCann, Stephen | Huawei Technologies Co., Ltd |
| TGbh | 11/8 | Mutgan, Okan | Nokia |
| TGbh | 11/8 | Orr, Stephen | Cisco Systems, Inc. |
| TGbh | 11/8 | Rosdahl, Jon | Qualcomm Technologies, Inc. |
| TGbh | 11/8 | Sam, Harvey | Broadcom Corporation |
| TGbh | 11/8 | Sevin, Julien | Canon Research Centre France |
| TGbh | 11/8 | Thakore, Darshak | Cable Television Laboratories Inc. (CableLabs) |
| TGbh | 11/8 | Yang, Jay | Nokia |