Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Teleconference Minutes, November 7, 2023Randomized and Changing MAC addresses (RCM) |
| Date: 2023-11-07 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Stephen Orr | Cisco | San Jose, CA, US |  | sorr@cisco.com |

Abstract

This document contains the minutes of the IEEE 802.11bh teleconference of November 7, 2023.

Note: Highlighted text are action items.

**Meeting November 7th, 2023, 9:30 a.m. to 11:30 a.m. EDT**

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

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

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

**Secretary: Peter Yee**

**Editor: Carol Ansley (Cox Communications)**

**The teleconference was called to order by the Chair at 9:33 a.m. EDT.**

The agenda slide deck is [11-23/1926r0](https://mentor.ieee.org/802.11/dcn/23/11-23-1926-00-00bh-agenda-tgbh-2023-nov-7.pptx).

**Policies and procedures were presented by Chair Mark Hamilton. (Slides 4 to 15)**

There were no Patent declarations.

Copyright policy slides were presented (Slides 10 and 11)

* **Agenda:**
* **Attendance, noises/recording, meeting protocol**
* **Policies, duty to inform, participation rules**
* **Organization topics:**
	+ Timeline reminder (slide 16)
	+ Motions record: [11-22/0651r28](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-28-00bh-tgbh-motions-list.pptx)
* **Comment Resolution**
	+ Comment resolution document: [11-23/1152r26](https://mentor.ieee.org/802.11/dcn/23/11-23-1152-26-00bh-ieee-802-11bh-lb274-comments.xlsx)
	+ Withdrawn CID47
	+ Comment resolution queue (slide 17)
* **Discussion on response to WBA liaisons (was due Sept):** [**11-21/0703r0**](https://mentor.ieee.org/802.11/dcn/21/11-21-0703-00-0000-2021-april-liaison-from-wba.docx)**,** [**11-21/1141r0**](https://mentor.ieee.org/802.11/dcn/21/11-21-1141-00-00bh-excerpts-of-wba-document-wi-fi-id-scope.pptx)**,** [**11-22/0668r0**](https://mentor.ieee.org/802.11/dcn/22/11-22-0668-00-0000-liaison-statement-from-wba-re-wi-fi-devices-identification-group.pdf)**,** [**11-22/0653r0**](https://mentor.ieee.org/802.11/dcn/22/11-22-0653-00-0000-2022-march-wba-whitepaper-re-device-identification.pdf)
	+ [11-23/0888r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0888-00-00bh-wba-liaison-discussion.pptx) Stephen Orr

The agenda, with comment resolution submission updates acknowledged, was approved with unanimous consent.

* **Timeline Review**

Hopefully, we will be able to wrap up comment resolution in time for a recirculation ballot by November, if not earlier. We still appear to be on track – F2F meeting next week 11/13 in Honolulu

* **Comment Resolution**
* **CID 47 Discussion – mark as rejected.** May bring it back for the next ballot round. Will be ready for motion next week.
* **Revisit CID 103, to consider alignment with CID 107 resolution: IRM topics:** [**11-23/1373r7**](https://mentor.ieee.org/802.11/dcn/23/11-23-1373-07-00bh-cid-resolutions-irm-2.docx) **(Smith)**
	+ - **244 and 72 also amended by 103. The TG proposed to amend the text – see 11-23/1373r7.**
* **Revisit CIDs 84, 85, 87, 212:** [**11-23/1726r2**](https://mentor.ieee.org/802.11/dcn/23/11-23-1726-02-00bh-lb274-cid-resolutions-for-pasn.docx) **(Mutgan)**
	+ - 84 and 212: Encrypting IRM element in PASN Frame 3 and 2. Resolution to add the details.
			1. Discussion on generation of the PTK. Suggest adding the KEK
				1. KEK = (PTK,256, KEK Length Bits)
				2. KEK is used to provide Data Confidentiality for certain fields (IE’s) in PASN frames.
				3. Modification to the TK calculation adding in the KEK Length bits
			2. The KDF HASH is selected based on the pairwise Cipher Suite selected.
			3. 12.2.11.3 – Device ID should be encrypted in PASN frame 2 and IRM encrypted in frame 3. KEK is to be used to do the encryption.

Q: This may affect PASN as it is currently defined unless you are suggesting to add a new clause that will add PASN when using Device ID and IRM. We may need to do something different here. Add a new subsection or clause for when using PASN and Device ID. Do we copy this an retitle it for PASN with IDs – don’t see how we make the change without fundamentally changing how others are using the spec.

A: The problem is not the KEK – its changing “the non-AP STA in the first PASN frame”

C: Similar concern on where the Cipher suite is coming from. This may break PASN for non-ID use. Adding the KEK now changes the length of the PTK. Suggestion from last week was to use an existing key. Is there an follow up on using an existing key?

A: Agree that if we change this 11az may change. Maybe we do not modify it here – to be compatible with 11az.

C: By changing the way things are built – you are building different keys. If we need to build new keys because the non-AP STA is selecting the cipher suite.

A: PASN-Protection Key was derived by the KDK in initial submission.

C: If the KDK is being built on a different cipher suite can we reuse the key.

Q: Why is the non-AP STA selecting the cipher suite?

A: We want to encrypt the second and third frame – meaning that the AP should encrypt the IE there. The idea was that the non-AP STA should the cipher suite.

C: Discussion on how the AKM and cipher suites are negotiated between PASN AP and non-AP STA.

C: Need to move the discussion to the reflector – get some additional security and PASN expertise.

C: KEK is used to encrypt keys

C: The use of PASN in the same ESS therefore the Device ID is know and we are sharing the KEK between all the APs within the ESS, then we could use the KEK freely. If PASN is to be used outside the ESS then we have a different situation with the keying situation and how the keys are derived.

C: Non-PASN cases the DeviceID and IRM should be distributed to the APs in an ESS.

C: While the KEK (or whatever key we are using) is known to the APs within the ESS – how is that shared with the non-AP STA coming back if the KEK is not a static key? If that happens the key has to be shared and the non-AP STA has no way of getting that information until it is identified.

* **FT case (CIDs 131, 136, 274):** [**11-23/1852r1**](https://mentor.ieee.org/802.11/dcn/23/11-23-1852-01-00bh-cr-for-ft-case.pptx) **(Li)**
	+ Allow a STA to use a different MAC address for each Fast BSS transition.
		- Recap of FT key hierarchy
		- MAC address of non-AP STA is used as an input to generate the keys
		- Option 1: Generate a batch of new PMK-R1s (slide 8)
		- Option 2: Reuse the PMK-R1s (slide 9)
		- Signaling - FT add new element (IRM and Device ID)
			* Signaling for Device ID (Slide 11)
			* Signaling for IRM (Slide 12)
		- Straw Poll request on option 1 or 2

C: Is slide 11 option 2

A: Yes

C: With FT do we assume before this happens that a 4WHS had already occurred.

Q: In the first authentication request M1 – why is there a Device ID in there at all? The STA has previously been given an ID - the STA just needs to tell the AP “this is my Device ID” why declare it in the clear?

C: Device ID has grown from a simple ID for the STA, it is being changed every time because it is being sent in the clear. It is now a different thing all together from what was originally defined. IRM seems a lot cleaner.

A: Option 1 does not support Device ID

Chair: Does anyone want to speak for Option 1

C: Option 2 supports a version of Device ID…it changes the Device ID vs being semi-permanent.

Chair – anyone in support of Option 1 – do we have Consensus on Option 2

C: concerned about the newness of this…do we want to do this before we choose an option

Chair: Don’t support FT

C: Or modify FT

Will discuss further next week

* **CIDs 289, 294:** [**11-23/1866r0**](https://mentor.ieee.org/802.11/dcn/23/11-23-1866-00-00bh-cid-resolutions-for-cids-289-294.docx) **(Smith)**
	+ Device ID Status field
	+ 289 – proposed
		- Indicates the device ID has been recognized by the AP
		- Indicates the device ID has not been recognized by the AP
	+ 294 proposed
		- Indicates the IRM has been recognized by the AP
		- Indicates the IRM has not been recognized by the AP
	+ **Resolution - Accepted**
* **(Revisit?) CID 67:** [**11-23/1245r24**](https://mentor.ieee.org/802.11/dcn/23/11-23-1245-24-00bh-cid-resolutions-irm-1.docx) **(Smith)**
	+ Change when to “If”
	+ **CID 67 – Revised**
* **Numerous misc CIDs:** [**11-23/1855r0**](https://mentor.ieee.org/802.11/dcn/23/11-23-1855-00-00bh-lb274-misc-cid-resolutions.docx) **(Hamilton): 54, 55, 74, 117, 122, 165, 167, 190, 223, 267, 268, 273, 286, 292, 293**
	+ CID 122
		- Change “when it associates” to “when it (re)associates”.
		- Non-AP STA cannot change its MAC while connected to an ESS
		- Unless we change 12.2.10 – the MAC address cannot change at (re)association

Q: Want to differentiate something. Are we talking about changing the MAC address used in an ESS during an (re)association or the IRM during a (re)association. If it’s the IRM I am ok with that.

C: IRM would allow you to change that MAC address on (re)association. But we didn’t specify correctly and straightforward to do that. The question is “why not” – its got better privacy. Either reject now or go work up some text to stick into 12.2.10

Chair – we do need to clear up 12.2.10, but we also need some text in our expected behavior section to clear this up

C: We are going to have a scope issue and go beyond what 11bh set out to do. Could be a PAR modification.

C: If we do a change here – we are going to change the same section in 11bi and have a race condition. I would avoid having both TGs doing work in the same section.

A:11bi comes after 11bh – therefore 11bi builds on what is proposed in 11bh.

Q: How does this work out in the field now? When a device (re)associates going from one AP to another – does it currently change its MAC address or not? Are we trying to fix something that doesn’t need to be fixed? Could leave it alone and let it go. Is this being broken by RCM?

Chair: The PAR wasn’t clear on what exactly it means. Fixing things that RCM has broken. Does RCM as it is currently used – break reassocation

C: We should take IRM out of the reassociation

Chair – what is the consensus of the group?

C: If an RCM is used – its RCM should be used throughout the ESS (spec is clear). Do all devices do that today – maybe not. But the spec is clear on when a device should maintain its MAC address for reassociation.

**Chair – the group has consensus that we will not deal with RCM at reassociation time and will leave it to 11bi.**

Chair - Does anyone want to be involved in and offline discussion to remove reassociation language?

**Meeting adjourned at 11:30 a.m. EDT**

**Attendance**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 11/7 | Ansley, Carol | Cox Communications Inc. |
| TGbh | 11/7 | Chen, Junbin | TP-Link Corporation Limited |
| TGbh | 11/7 | DeLaOlivaDelgado, Antonio | InterDigital, Inc. |
| TGbh | 11/7 | Hamilton, Mark | CommScope, Inc. |
| TGbh | 11/7 | Henry, Jerome | Cisco Systems, Inc. |
| TGbh | 11/7 | Levy, Joseph | InterDigital, Inc. |
| TGbh | 11/7 | Mutgan, Okan | Nokia |
| TGbh | 11/7 | Orr, Stephen | Cisco Systems, Inc. |
| TGbh | 11/7 | Patwardhan, Gaurav | Hewlett Packard Enterprise |
| TGbh | 11/7 | Rosdahl, Jon | Qualcomm Technologies, Inc. |
| TGbh | 11/7 | Sam, Harvey | Broadcom Corporation |
| TGbh | 11/7 | Sevin, Julien | Canon Research Centre France |
| TGbh | 11/7 | Smith, Graham | SRT Wireless |

 |  |  |  |