Minutes IEEE P802.11  
Wireless LANs

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| IEEE 802.11 TGbh Meeting Minutes, April 11, 2023  Randomized and Changing MAC addresses (RCM) | | | | |
| Date: 2023-04-11 | | | | |
| Author(s): | | | | |
| Name | Affiliation | Address | Phone | email |
| Peter Yee | NSA-CSD | Mountain View, CA |  | peter@akayla.com |
|  |  |  |  |  |

Abstract

This document contains the minutes of the IEEE 802.11bh telecon meeting of April 11, 2023.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting April 11, 2023 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 9:33 a.m. EST.**

Agenda slide deck [11-23/0621r00](https://mentor.ieee.org/802.11/dcn/23/11-23-0621-00-00bh-agenda-tgbh-2023-april-11.pptx)

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)**
  + 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:** [**11-22/0973r21**](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-21-00bh-cc41-comments-against-d0-2.xlsx)
* **Motions record:** [**11-22/0651r15**](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-15-00bh-tgbh-motions-list.pptx)
* **Discuss Contributions (next slide)**
* **Review D0.2 CC comments, prepare for CC comment resolutions motion (next week)**
  + Move to approve the resolutions of CC41 comments, and incorporate the text changes into the P802.11bh draft, as indicated in 11-22/0973r<latest>.
* **WBA liaison response**

Any comments? [None]

Any objections to agenda? [None]

1. **Timeline**

We are targeting a WG letter ballot coming out of the May meeting and all efforts are directed to achieving that.

1. **IRM Proposed Text**

Graham Smith (SRT) presented [11-23/0129r04](https://mentor.ieee.org/802.11/dcn/23/11-23-0129-04-00bh-irm-proposed-text.docx). This was discussed at the previous meeting, but the PASN additions were not described with sufficient clarity. The introductory material for 12.2.11 is now updated to show that PASN is not part of an associated state. Other text in 12.2.12.2 discussing PASN is also clearly separated from the text that covers the Association case.

Q: Can the MAC address be changed later in the 4-way handshake?

A: Do you mean with Secure Action frames? The group seemed to want to move away from that.

C: Yes. It seems very early to know the next MAC address in the sequence. It might be lost.

C: It could be changed or added. I’m open to that. It’s up to the group’s preference.

C: I’d like to not rehash agreed upon issues.

Q: I believe that Okan’s upcoming presentation builds on this presentation, but not the inverse?

A: That’s correct.

Q: As far as resolution of the CIDs is concerned?

A: Yes. IRM or Device ID can be used to solve those CIDs.

C: We have to agree which resolutions for those CIDs will be used, or both could be included.

1. **11bh D0.2 CR for device ID in PASN**

[11-22/1806r02](https://mentor.ieee.org/802.11/dcn/22/11-22-1806-02-00bh-cr-for-pasn.docx) gives an option for using device ID instead of or in addition to IRM with PASN. The device ID is assigned by the AP in PASN Authentication message 2, and it is used by the non-AP STA in Authentication message 3. In both messages, the device ID is encrypted and placed in the Device ID IE. It should be exchanged for each FTM session and for each return to the same ESS. The proposed text shows when the device ID is transmitted when using PASN as an adjunct to the existing text that covers FILS and non-FILS cases.

C: I would just change 12.2.11 to 12.2.11.1 as the subsection being modified to align with Graham’s presentation.

C: In your picture, this seems backwards. The non-AP STA doesn’t tell the AP who he is until he has been given a new identity. The AP doesn’t know who the non-AP STA is until after a new device ID has been assigned. What should happen is that the non-AP STA should tell the AP who he is. Looking at Annex Z, an opaque identifier is produced and sent in one of these handshakes. That should then be usable in Authentication message 1 by the non-AP STA. The AP should be able to unwrap the device ID, recognize the non-AP STA, and then send the new one to the non-AP STA in message 2, and there’s no usage of device ID in message 3. Otherwise, the AP has no linkage between the returning STA and the device ID it issues. It doesn’t help the AP to track non-AP STAs. I think it would be better to reverse the ordering.

C: I agree the ordering is a bit strange here. That’s because of the desire to encrypt the device ID. So, this solution treats the STA as a new STA each time. In message 1, the STA should indicate that it wants to use device ID. The STA should tell the AP in message 1 that it’s okay to use the device ID. The AP then assigns the STA an encrypted device ID. The AP considers a STA like a new STA each time. That’s the assumption that we have to make here. I had proposed device ID in message 1 previously, but that wouldn’t be encrypted. We can have that solution as well. We just have to decide which solution to use. It seems you prefer the opaque device ID solution.

C: The reason for addressing a pre-association use case was (among other things) to allow steering. In this proposal, you have to go most of the way through these steps before you get the information that tells the AP that this is actually a known STA. It doesn’t seem to help with use cases like STA steering.

C: I think the pre-association use cases like steering are broken and I’m not interested in them. Also, I’m not sure we need to assign an identifier in PASN. We could do normal assignment on Association. PASN assignment seems like overkill. It’s also not clear that use of the device ID is optional.

Q: So, you want to keep the first paragraph of the proposed text?

A: Yes, we need to make clear it’s optional. And we need to be able to associate with or without use of the device identifier. That’s something to clarify.

C: We have the MIB variable in the text saying that the non-AP STA wants to use the feature or not.

C: I think clear declaration of the use of optional features is not the way to do it. I want clear text saying that.

Q: You are just modifying some of the paragraph’s in Kurt’s proposal, not deleting anything, right?

A: Yes.

C: Without showing changes between the two documents, it’s really hard to see how the proposal before us fits in with Kurt’s proposal. I prefer to have tracked changes.

C: I think it should be clear to the editor.

Q: Only the red text is changes, right?

A: Yes.

Q: If you don’t consider my comment is clear enough, perhaps we have a different point of view. Why do we have partially copied text that isn’t modified? It’s difficult to tell what this presentation changes.

A: It gets messy when we try to modify some of the text and not replace all of it. Maybe I could make some changes and show the changes.

C: I just want to see the modifications and not the unmodified text.

Q: Looking at the flow diagram in the presentation, the first Auth message 1, he doesn’t have a device ID. Auth message 2 assigns the device ID in an encrypted format. Then taking that device ID to AP2, it won’t be recognized. As long as the device ID in message 1 can’t be unwrapped by anyone, it shouldn’t be a problem. Whether an AP assigns a new one or uses Annex Z to obfuscate one, should be sufficient as long what’s in message 1 can’t be correlated with anything. So, why do we have to use ID2, ID3, and ID4?

A: Yes, that’s my idea. Message 1 conveys the wrapped identity and then don’t do so in message 3. That gives the AP the STA’s identity.

C: There are pre-association use cases where this could be useful. The AP can still send a new ID in message 2. The obfuscation each time helps.

Q: We did have a discussion where the group leaned toward not sending something unencrypted that could later be correlated. I guess we are revisiting that decision. Would that imply that we need to make Annex Z normative in this situation where the device ID is sent in message 1? I’m unclear on that.

Q: I have moved the introductory text with the MAYs to 12.2.11, so nothing is lost. Now to the question at hand, if the STA already has an ID, I think it gets lost in this scheme. If the ID came from a classical exchange, can’t it be in message 1? I know that’s sort of in the clear. The STA doesn’t know that it’s in the clear. Is it changing the ID every single association, and does it have to? I think we may be moving away from the ID scheme, although what was outlined (use in message 1) should work. Do we need to spell out a new scheme separately instead of trying to insert it into the present text?

C: Message 1 isn’t encrypted, so that might set requirements on device ID.

C: Annex Z can be used to convey a long-term identity across all associations. If you don’t want to use a long-term identity, on first connection, the non-AP STA can decrypt the device ID it is assigned. On the next association, it could put the device ID in the clear and send it to the AP. The AP could then recognize the STA and assign it a new device ID. Then in message 3 the STA sends the freshly assigned device ID and no one can correlate. That’s an option to using Annex Z, although I think that’s a superior solution. As far as the non-AP STA is concerned, the device ID is just a blob. It has no particular significance. The AP is responsible for the linkage. As long as the values are only used once, no long-term persistent ID is needed by the STA. It’s not as functional as using Annex Z with a long-term ID.

Q: So, you think it’s okay to send the device ID back in message 1 unencrypted because it is only ever on the air in that form once.

A: Yes. It would be workable. The identity is used once by the non-AP STA.

Q: I think we’ve been back and forth on this question before. Can we get some consensus? Would we like the non-AP STA to send a previously assigned ID in message 1 rather than waiting until message 3?

A: I hear the point of using message 1. The devID1 in the diagram could be an opaque identifier and is a long-term identifier that is used with Annex Z optionally. Annex Z isn’t currently mandatory, hence the presented scheme. Thinking about assigning the opaque value in the previous association, then if the STA uses the opaque ID and has to send the association message 1 again without having gotten to message 2 might be a problem. If we use encryption in message 3, that’s different. From a practical point of view, both work.

C: I think any of this discussion is dependent on use of Annex Z. Let me know if you disagree. I’d like to stop talking about opaque IDs and Annex Z unless that’s connected to this discussion. The danger of putting things in Auth message 1, is that not completing the sequence leaves the STA with only having the device ID that it can’t reuse.

Q: We have no idea who the AP is when we send the first message, so sending the device ID to the AP could open us up to active attacks. Have we analyzed whether it’s safe to put the device ID in message 1?

C: That’s another interesting point to consider.

Q: Do we get real authentication of the AP by the time we get to message 2 before sending message 3?

A: I don’t have a good answer to that. PASN and its use case, the PMKID would be the ID for PASN. I asked that during the last face-to-face meeting. But we seemed to commit to using PASN with device ID instead of using the PMKID.

C: I don’t remember the details for PMKID usage, but the PMKID doesn’t change unless you delete it or reboot your device. From a practical point of view, the AP saves the PMKID in the expectation that it won’t change for some time. Here, we can change the device ID every time.

C: I think that was an answer to a different question.

C: I agree. My thinking was that using PSK with device ID in message 1. The attacker AP spoofs a known AP. It gets message 1 and has the same PSK. Then it makes a PASN association with the real AP using the recorded message 1 and claims to be the STA. I’d like to understand how we protect against such an attack.

C: With that replay attack, if we do change the device ID with each association, then a replay attack won’t work because no one will recognize it. And the AP will know that the STA has accepted a new ID, which would make it more robust.

Q: We seem to be dredging up old discussions. Does the presenter have enough information to discuss the options, pros/cons that have been raised?

A: Perhaps we can run a straw poll to see the preference between message 1 and message 3.

C: We could, but I want to be sure the group understands the tradeoffs clearly. Otherwise, we will just end up revisiting the point in the future.

C: I need more clarity before I can give a meaningful straw poll response.

Q: I agree that those answers are needed, but I want to know if the one-time use of the device ID is the main concern here.

A: Yes, that and how easy it is to fake being the real AP and stealing the device ID of the STA. Active attacks are pretty easy in this model.

Q: There’s no real security context that’s being revealed by intercepting the device ID. There’s no compromise such that the fake AP can use that information to spoof the real AP once something secure starts happening. I think we are overemphasizing the security issues of this device ID when there aren’t really any.

Q: If the attacker replays message 1 to the real AP, doesn’t it steal the identity of the STA?

A: Only for device steering. It’s not a shared identity.

C: I’d still like more details.

C: We are trying to define a uniform solution to meet all sorts of use cases. PASN has lots of modes.

C: I have to check IEEE 802.11az. If the PMKID is sent in message 1, it will be used subsequently as well. If not there, it’s sent in message 3. I think maybe PMKID is not a good thing to use here, but I will check and provide a formal explanation. Separately, the use case looks like pre-association identification, but it doesn’t solve everything. It solves FTM use cases. IEEE 802.11az made it possible to encrypt these frames. The only we are addressing here is how to identify the STA. If it there’s an active attacker, let’s look at the worst case. FTM isn’t compromised.

C: I’m trying to figure out how we move forward from this discussion. Some of the discussion feels like we are going in circles. A presentation to pull the issues together would be helpful. Perhaps Okan and Mark could generate something offline.

C: That sounds good.

1. **Discussion on CID 35**

Continuing last week’s discussion in [11-23/0623r00](https://mentor.ieee.org/802.11/dcn/23/11-23-0623-00-00bh-discussion-on-cid-35.pptx), we had a request for an explanation of the Annex Z connection. It’s a pretty general request. We discussed this at the last face-to-face plenary meeting as well as April 4’s call. Mark Hamilton presented a new paragraph for 12.2.11 or thereabouts that gives the requested explanation. There were some comments and concerns with the proposed text during last week’s call, particularly around the term “opaque identifier” or even “identifier”. We mostly focus on Device ID (or device ID, lowercase). Hamilton now suggests clarifying that Annex Z is for constructing something that is sent over the air, which doesn’t impact the identifier concept itself. He also suggests that this is only for Device ID and not for IRM, that is only for network-generated IDs.

Q: I’m fine with the proposed text. I don’t understand the final bit that says the AP is hiding the ID from the non-AP STA?

A: Yes, the non-AP STA doesn’t have to know the real ID.

C: I had conceived of a long-term identity being transformed each time by Annex Z, but I hadn’t really contemplated hiding the long-term identity from the non-AP STA or that that was a requirement of the group.

C: I see your point and I could delete that part. I think there was something in Annex Z that implied that the identity is kept opaque to the non-AP STA. I don’t see why that would be necessary.

Q: Does Annex Z become normative text?

A: No, I don’t think so. Can you explain your logic?

A: This proposed text would seem to make Annex Z normative.

C: No, I say that something equivalent is allowed as well.

C: I’d like to see that Annex Z is optional.

C: I’m not sure that the subtle difference makes Annex Z normative.

Q: Another question: Why is the second part “or any procedure that affords comparable security and privacy” there?

A: That goes back to the optionality. Annex Z is an example, but any similar method is acceptable. Device ID is already encrypted, so there’s no need for Annex Z.

C: My proposal probably needs more words to explain what we are trying to do, but let’s address the queue first.

C: The first Device ID should be lowercase because that’s the content.

C: I saw that, but I can read it both ways (device ID or Device ID).

C: We agreed that lowercase device ID is the conceptual thing and uppercase Device ID is what’s transmitted.

C: Device ID is always secure the way it is exchanged. The opening bit about “exchanging the Device ID over the air” is confusing. That’s how it is always exchanged. If, for any reason that the Device ID is sent in the clear, Annex Z can be used to secure it. We need to say the when of Annex Z.

C: In general, this Annex Z is defining an AP mechanism for defining a Device ID and getting it from the STA and knowing it’s the version that the AP assigned. This is an AP mechanism. The STA can only receive an identifier and send it back unchanged. The STA only stores that identifier. The AP can determine the validity of the identifier. I would hope to see some non-AP STA considerations for use of the device ID as only being stored by the STA. Privacy considerations should indicate this is an AP internal parameter and that it applies to over-the-air transmission. It should be clear what’s being protected.

C: The text in the presentation is in the context of the preceding text in the section.

C: If you look at Annex Z, it lists its security properties. If you have an alternative proposal, you need to have comparable properties, otherwise you are leaking information about the STA. Hence the sentence that says “comparable security”. Saying that everything is protected under the 4-way handshake doesn’t cover the properties. Passing things only under the 4-way handshake means that we aren’t solving all of the use cases. Device ID is not always passed securely. Annex Z and the 4-way handshake are not the totality of IEEE 802.11bh. Provided that comparable security to Annex Z is utilized, any other mechanism is fine. Removing the requirement for comparable security makes me wonder what procedure is desired that is less secure.

Q: Where do you think this comparability would be? In IEEE 802.11bh, IEEE 802.11bi, or somewhere else?

A: In IEEE 802.11bh. And if you don’t want to use Annex Z because it’s too complex, then that mechanism should be at least as secure. I think PASN is an example of the device ID can be used. Placing it in message 1 means that it has to be protected itself rather than as part of the message exchange. Otherwise, the AP is keeping track of too many IDs. PASN is a use of a device ID that helps with pre-association where there isn’t an encrypted exchange. The STA connects. Who is he? Whatever the opaque blobs says he is.

C: I want to delete the “that affords comparable security and privacy” bit. Otherwise, if we don’t have a mechanism that’s as security, we are forced to do Annex Z. That removes AP vendor flexibility.

C: We have a fundamental problem here.

C: Annex Z lists valuable security capabilities. We can move those properties into normative text in Clause 12. Annex Z will meet them. Any other mechanism can too.

C: If the AP vendor can’t find another solution, they have to do Annex Z.

C: No. If you don’t want to do Annex Z, just meet the properties required.

C: The current spec says that device ID is included and secure.

C: Then if it’s already secure, what’s the problem with saying “comparable security”. That part of the sentence is a no-op if it’s already secure. Why remove that text?

Q: Why do we have to provide a solution that is comparable to Annex Z?

A: To prevent tracking.

C: But it’s already encrypted, so it can’t be tracked.

C: Then you can only work in the context of the 4-way handshake.

C: With PASN, it’s fine. But if the Device ID is not used in the first PASN message, we don’t need a comparable mechanism because the Device ID is encrypted (as in message 3).

Q: What about if someone uses the Device ID in a different situation?

A: Then I would want a dedicated contribution to cover that situation.

C: My point is that if the Device ID is only passed in encrypted form over the air, then that’s comparable security to Annex Z. That’s an alternative means and comparable.

C: The wording is confusing, because it sounds like something else needs to be done, when nothing needs to be done because it is already encrypted.

C: If you are passing it in encrypted form, nothing else needs to be done. That’s a comparable procedure.

C: Adding “(including nothing, if appropriate)” could cover that.

Q: What does that mean?

A: If it’s already encrypted, it already has security and privacy, so a no-op procedure is all right in that case. This will need more discussion and debate.

C: Perhaps we can work on this offline.

**Meeting adjoined at 11:31 a.m. EST.**

**Attendance**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 04/11 | Ansley, Carol | Cox |
| TGbh | 04/11 | De la Oliva, Antonio | InterDigital |
| TGbh | 04/11 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 04/11 | Harkins, Dan | HPE |
| TGbh | 04/11 | Hedayat, Reza | Apple |
| TGbh | 04/11 | Henry, Jerome | Cisco |
| TGbh | 04/11 | Huang, Po-Kai | Intel |
| TGbh | 04/11 | Kneckt, Jarkko | Apple |
| TGbh | 04/11 | Levy, Joseph | InterDigital |
| TGbh | 04/11 | Lumbatis, Kurt | ARRIS/CommScope |
| TGbh | 04/11 | Luo, Ye | Nokia |
| TGbh | 04/11 | McCann, Stephen | Huawei |
| TGbh | 04/11 | Montemurro, Mike | Huawei |
| TGbh | 04/11 | Mutgan, Okan | Nokia |
| TGbh | 04/11 | Orr, Stephen | Cisco |
| TGbh | 04/11 | Riegel, Max | Nokia |
| TGbh | 04/11 | Rison, Mark | Samsung |
| TGbh | 04/11 | Rosdahl, Jon | Qualcomm |
| TGbh | 04/11 | Sam, Harvey | Broadcom Corporation |
| TGbh | 04/11 | Sevin, Julien | Canon |
| TGbh | 04/11 | Smith, Graham | SRT Wireless |
| TGbh | 04/11 | Smith, Luther | CableLabs |
| TGbh | 04/11 | Stanley, Dorothy | Hewlett Packard Enterprise |
| TGbh | 04/11 | Thakore, Darshak | CableLabs |
| TGbh | 04/11 | Yang, Jay | Nokia |
| TGbh | 04/11 | Yee, Peter | NSA-CSD |