Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Plenary Meeting Minutes, November 2022Randomized and Changing MAC addresses (RCM) |
| Date: 2022-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Peter YEE | NSA-CSD | Mountain View, California |  | peter@akayla.com |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This document contains the minutes of the IEEE 802.11bh November 2022 Plenary meeting.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting November 14, 2022, 8:00 a.m. to 10:00 a.m. ICT**

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

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

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

**Secretary: Peter Yee (NSA-CSD)**

**Editor: Carol Ansley (Cox)**

**Mark Hamilton, the TG chair, called the ad hoc meeting to order at 8:09 a.m. ICT.**

1. **Policies and procedures were presented by the chair. (Slides 4 to 15)**

The meeting registration requirements, meeting protocol, attendance, patent policy [no claims noted], copyright policy, and code of ethics & conduct were all displayed.

1. **Agenda**

The task group agenda is found in [11-22/1704r01](https://mentor.ieee.org/802.11/dcn/22/11-22-1704-01-00bh-agenda-tgbh-2022-nov-14.pptx) (updated over the course of the meeting to [11-22/17904r02](https://mentor.ieee.org/802.11/dcn/22/11-22-1704-02-00bh-agenda-tgbh-2022-nov-14.pptx)). The primary agenda is:

* **Attendance, noises/recording, meeting protocol reminders**
* **Policies, duty to inform, participation rules**
* **Organization topics (see Backup slides)**
	+ **November Plenary meetings: [Ad-hoc, Monday, 8:00-10:00]; Tuesday, 13:30-15:30; Wednesday, 8:00-10:00; Thursday 8:00-10:00**
	+ **Timeline review: Can we complete comment collection and agree on D1.0 during November session?**
* **Issues Tracking:** [**11-21/0332r37**](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* **Motions record:** [**11-22/0651r8**](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-08-00bh-tgbh-motions-list.pptx)
* **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)
* **Contributions (slide 17)**
* **Consider/Review CIDs that are “not controversial” and are not closed/not being discussed**
* **Consider “controversial” topics – time permitting**
1. **Comment Collection Status**

[11-22/0973r13](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-13-00bh-cc41-comments-against-d0-2.xlsx) contains the latest updates to the comments collected and their resolutions.

1. **Discussion on Device ID renaming**

Antonio de la Oliva (InterDigital) presented [11-22/1665r01](https://mentor.ieee.org/802.11/dcn/22/11-22-1665-01-00bh-deviceid-renaming-discussion.pptx). De la Oliva is suggesting various alternatives to the term Device ID: Persistent Opaque Identifier, Persistent Identifier, or a combination of the two depending on context. He looked at the current draft in order to determine what terms are currently used and their characteristics. Device ID is not currently used to describe any of the MAC address-based schemes as none of these have yet been incorporated into the draft.

Q: Didn’t we agree that the ID blob used is the opaque identifier?

A: Let’s complete the presentation first, which may be informative.

According to the current draft, the AP’s application layer generates an ID and sends it to the AP’s SME. The AP’s SME then makes that ID opaque according to some procedure. The opaque ID is sent to the STA’s SME and stored – the STA is oblivious to the actual ID and only operates on the opaque ID, sending it back to the AP when needed.

Q: When you refer to the non-AP STA as not being able to “de-opaque” the identifier, you mean that de-opaquing is only done by the AP. Can you differentiate between the content of the identifier and the purpose of the identifier?

A: The STA can’t, according to the current draft. The AP can. The opaquing operation is performed by the set of APs that share a common key.

C: The difference between the visibility of the identifier and its purpose needs to be clarified. The non-AP STA needs to know what purpose it is being assigned an identifier for.

C: I think that exists in the current draft.

C: That’s fine. The key point is that there is a mechanism by which the non-AP STA can clearly determine what the purpose of identification is.

C: Agreed.

C: The step of the application layer generating an ID is preceded by an out-of-band step of establishing a long-term identity for the non-AP STA. Annex Z is wrapping that identifier. The idea that the network is assigning an ID to the non-AP STA is probably not the right beginning.

C: Agreed.

C: There is an option of the AP assigning a random thing that can be used to identify the returning station. It’s a token that the STA is given. I fully agree that these things are out of the scope of what we are doing, but there are different use cases that are enabled and supported by the current draft.

C: I agree with that as well. Persistent means to me something that lasts longer than a packet, but it may be relatively short lived.

The conclusion: there are two flavors of Device ID: an opaque identifier that is generated by the AP and used by the STA; and a non-opaque identifier, stored at the AP or infrastructure.

Q: We have still some on-going discussion on STA-generated things, which will have impact here. Are you trying to solve that case too, or do you think there’s something different that’s needed there?

A: It’s not clear to me what would be used for a STA-generated identifier.

Q: So, you’re only trying to cover the existing draft, which does not have STA-generated identifiers.

A: Correct.

Straw poll: Do you support the following nomenclature:

* POI: Persistent Opaque Identifier (use of identifier within IEEE 802.11 scope)
* PI: Persistent Identifier (identifier when exchange between higher layers/application) and AP’s SMEs

Q: When you say the POI is opaque, you mean to third parties?

A: Opaque is to everyone.

Q: What does persistent mean? Just to the STA?

A: It’s for more than one packet.

Q: Do we have a definition of what persistence means within the 802.11 context?

A: No

Q: If we are going to create a POI, does the opposite also make sense? Do we need non-persistent opaque identifiers and identifiers?

A: Let’s answer that after the straw poll.

The vote on the straw poll was: 5/9/5 Y/N/A (Yes/No/Abstain)

C: When a non-AP STA joins the network and gets an identifier for a single association, it could be tracked during that single association. IEEE 802.11az that uses the identifier to coordinate with RCM and provides it to an upper layer.

C: You can certainly do that within a single association, you have a single MAC address and can be tracked by that, so this identifier doesn’t make a difference. I fully support providing guidelines for this identifier. The STA doesn’t necessarily have to trust the AP, but that’s independent from the naming. But for a single session, we’re not changing the status quo.

C: I agree with that, I’m just wondering about the case where the identifier is going to be assigned irrespective of the STA’s consent. We discussed that before, so I won’t waste the group’s time.

C: Maybe it’s worth asking what the people voting “No” in the straw poll see as controversial.

C: I’m of two thoughts. Perhaps we want to add one contribution this morning. Dan’s “Using Opaque Identifiers” ([11-22/1941r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1941-00-00bh-using-opaque-identifiers.pptx)) might help. The other is to hear more from those voting “No”.

Q: Dan, are you willing to give your presentation?

A: Sure.

Q: Is the group willing to modify the agenda thusly?

A: [No objections.]

1. **How to Use the Opaque Blob**

Dan Harkins presented [11-22/1941r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1941-00-00bh-using-opaque-identifiers.pptx/). The opaque identifier is generated by the network for the STA. This is not the real identity of the STA. It’s just a blob that is non-identifying by itself. The blob is a transport mechanism used outside of a 4-way handshake. The 4-way handshake requires a PMK. The PMK is established in an out-of-band bootstrapping method. That establishment mechanism uses the blob. The STA gets a new blob as often as the AP sends it one, presumably during each 4-way handshake. There’s text missing in the IEEE 802.11bh draft to explain the bootstrapping of blobs. Text could also be added to describe other uses in current protocols for which identifiers are important but allow tracking.

Q: What do we do with existing STAs that don’t support SAE authentication? How is the blob handled outside of systems that don’t do SAE? For open system authentication, they just handle things after the PMK.

A: How is the PMK generated?

Q: By the 4-way handshake.

A: No, the PMK is needed before the 4-way handshake. It is input to the 4-way handshake.

Q: This won’t work with WPA2-PSK. It uses the same PMK for everybody, so there’s no way to pass opaque identifiers when there’s no way to differentiate STAs. You’re assuming that devices will do WPA2-PSK and IEEE 802.11bh, but they won’t do WPA3?

A: Yes. I’m trying to understand the passing of the blob in the authentication step. Many APs don’t support SAE.

A: They don’t support IEEE 802.11bh either.

C: The use of the SAE scheme is problematic because the blob will only be changed on successful completion of the 4-way handshake. If that isn’t successful, the blob is reused, enabling some sort of tracking. To your point to additional specification being needed, I agree. Currently, there’s nothing in the draft that mandates changing the blob per association. We can certainly define frequent identifier changes. We might also work with IEEE 802.11bi to see if they have concerns.

Q: I don’t understand why anybody would use Device ID solely in the 4-way handshake. Why?

A: Café use case: the password is on the wall.

Q: The troubleshooting use case is outside of the scope of this presentation, right?

A: Yes. This is when the STA is wandering around the network having troubles connecting. He can’t connect, get a blob, complete a 4-way handshake, or assist the network help desk in assisting him.

Q: When we made the presentation about RCM, before the first association, we can use the same RMA (random MAC address). In your scheme, the same blob identifier is used, which can be tracked by a third party. Our proposal is similar to this one. What’s the right direction to move forward on?

A: You said the same identifier is used over multiple associations. That’s not correct. It’s changed on each successful association.

C: The AP can reject that association request for any reason. Then, the STA will use the same identifier for the next association attempt.

Q: For the diagnostics issue, you said this doesn’t help. Even though the 4-way handshake may not complete, the network will have some information that it can use to troubleshoot.

A: The STA will pass the blob, and if it has an old password that doesn’t match the AP’s current password, then the AP will have some idea of who is trying to authenticate and why the authentication is failing. But that’s not always the case.

Q: We are assuming that the device is sending some identifier when bootstrapping. We need to document how that can happen and needs to happen. What happens when a device loses state? Does it need to retain the initial ID?

A: The device has to retain a whole bunch of stuff: identifier, blob, SSID, password. If any of that is lost, the STA is screwed.

Q: The AP has to maintain that sort of thing.

A: Yes, including a key to generate and decrypt blobs.

C: It would be good to document those requirements.

Q: When you say that you need an out-of-band scheme for bootstrapping, the STA needs to indicate it wants a blob, right?

A: Yes.

Q: Slide 10 has all of the problems that I tried to solve in my presentation. This is the long-term/persistent identifier I was talking about. We need to solve this. We are referring to Device ID sometimes. I vote for blobification and deblobification as terms.

C: This is really describing what’s in the current draft and that some explanatory material is needed to enhance the current draft.

C: Yes. I think it would help if we identified some candidate protocols like SAE that use an identifier and request a blob. I could also provide text to describe slides 6 and 7.

Q: Would these be examples in the Annex?

A: Not in the Annex. I think it would need to be normative text. The blob in your profile is what you need to pass as your SAE identifier.

Q: On slide 8, do you see the bootstrapping text as normative?

A: Yes. And the first use of blobs in the current protocols would be too.

C: It would be good for you to bring some text.

Q: That sounds like good text to put in section 11. Just a suggestion. Or do you prefer in Annex Z?

A: I think it goes in 12.4. Other protocols should have text added to the section describing that protocol.

Q: On slide 7, for the SAE authentication request, an ID is carried. And it’s the same in message 2 of the 4-way handshake. It seems unnecessary to carry it in both places.

A: Point taken, but I don’t think the duplicate identifier is being passed. I don’t want to change the 4-way handshake. Technically, it’s duplicative, but I don’t think it’s necessary to remove the duplication.

C: On slide 8, we might need to describe the requirements for the new text rather than splitting things between informative and normative.

C: I agree, we could have normative text on the requirements. And if you want your own scheme that doesn’t match Annex Z, meet these normative requirements.

C: I think IEEE 802.11bi will have a requirement to protect the password identifier, but as we will publish before them, we might have to modify our text appropriately. The split between the two groups can be problematic. Our text needs to be clear that something like that needs to be considered.

C: Agreed. I see this as something that crosses between the two groups.

C: I remain concerned about the unsuccessful 4-way handshake where a new blob is therefore not supplied. Thus, the SAE-Commit identifier is re-used and is trackable.

Q: Isn’t this a problem without IEEE 802.11bh? We aren’t making it worse, right?

A: Yes, I agree if you mean SAE using different password identifiers.

Q: Is that something in the context of 11bh or 11bi to solve?

A: That’s what I was trying to clarify. I claim that if it’s an existing problem today (pre-11bh), then it’s within 11bi’s scope to solve. Dan’s suggestion doesn’t make it worse and 11bi could make it better.

C: For the full set of use cases for 11bh, I don’t agree – this could make things much worse. I think the question about protecting password identifiers goes beyond what 11bh is doing. That’s for 11bi. IEEE 802.11md started something along those lines. I don’t care which group does it, just make it go through as soon as possible. We can work on the dependencies between the task groups in any case. Just do it where it is easiest. It’s probably in 11bi’s scope. As long as we’re clear that it’s getting covered.

C: I’ll note that IEEE 802.11me would be the fastest course.

C: They threw it to IEEE 802.11bi. I agree that it needs to be done ASAP, but where it gets done is not a technical question. I would hope the people who make these non-technical decisions will figure it out.

Q: I’ll discuss this with Mike Montemurro and Carol Ansley. Do you think you can have text this week?

A: Yeah, probably something for Thursday.

1. **CID resolutions for 12.2.11**

Kurt Lumbatis (ARRIS/CommScope) shared [11-22/1329r07](https://mentor.ieee.org/802.11/dcn/22/11-22-1329-07-00bh-cid-resolutoins-for-12-2-11.docx), which is an update of material presented originally in September. It attempts to resolve comments on section 12.2.11. It currently uses the term “Identifier” until a common term is agreed upon.

C: Minor technical point: A Reassociation Request frame is not sent to an ESS, it’s sent to any AP in the ESS.

C: Thank you.

Q: Do the FILS cases in your text should also allow Reassociation Response frames as well as Association Response frames?

A: Right.

Q: Do we need the requirement that a non-AP STA shall return the most recently received Identifier for the ESS when associating? What if it doesn’t want to? This should be an independent requirement.

A: [Rewords the statement.] Is that acceptable?

C: Yes.

C: Since these are standalone statements, change “the ESS” to “that ESS”, since the non-AP STA may be dealing with multiple ESSes and the existing statement could be confusing.

Q: This text isn’t very good for a standard: it says the AP can do anything it wants. We shouldn’t say it can do anything. How does help that an implementer write code?

Q: We don’t have text for the non-initial case where the non-AP STA wants an identifier. What does it do at that point? How do we deal with denial-of-service attacks?

A: Perhaps, we want more sentences and words, like “when an identifier is needed…” Start with “Generally, when a new identifier is needed, these things happen.” “Generally, when a STA returns a network, these things happen.”

C: I’ll break out the last paragraph out and make it clearer so that we can have normative text.

C: Note that this presentation covers several CIDs for which resolutions have already been agreed. Kurt is building on those. Make sure that his updates agree with the previous resolutions.

C: I’ll update the text overnight for presentation tomorrow.

**Recessed at 10:00 a.m. ICT**

**Meeting November 15, 2022, 1:30 p.m. to 3:30 p.m. ICT**

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

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

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

**Secretary: Peter Yee (NSA-CSD)**

**Editor: Carol Ansley (Cox)**

**Mark Hamilton, the TG chair, called the meeting to order at 1:32 p.m. ICT.**

1. **Policies and procedures were presented by the chair. (Slides 4 to 15)**

The meeting registration requirements, meeting protocol, attendance, patent policy [no claims noted], copyright policy, and code of ethics & conduct were all displayed.

1. **Agenda**

The task group agenda is found in [11-22/1703r02](https://mentor.ieee.org/802.11/dcn/22/11-22-1703-01-00bh-agenda-tgbh-2022-nov-plenary.pptx) (approved by unanimous consent and updated over the course of the week to [11-22/1703r07](https://mentor.ieee.org/802.11/dcn/22/11-22-1703-07-00bh-agenda-tgbh-2022-nov-plenary.pptx)). The primary agenda is:

* **Attendance, noises/recording, meeting protocol**
* **Policies, duty to inform, participation rules**
* **Organization topics:**
	+ **November Plenary meetings: [Ad-hoc, Monday, 8:00-10:00]; Tuesday, 13:30-15:30; Wednesday, 8:00-10:00; Thursday 8:00-10:00**
	+ **Approve September interim and Sept/Oct/Nov teleconference minutes**
	+ **Timeline update review**
* **Issues Tracking:** [**11-21/0332r37**](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* **Motions record:** [**11-22/0651r08**](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-08-00bh-tgbh-motions-list.pptx)
* **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)
* **Motion #13 - dot11DeviceIDActivated MIB attribute**
* **Contributions (slide 21)**
* **Way forward to D1.0 (slide 22)**
1. **Approve Minutes**
	1. September interim session: [11-22/1737r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1737-00-00bh-minutes-tgbh-interim-meeting-september-2022.docx)
	2. Teleconference minutes:
		1. Sept 27: [11-22/1693r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1693-00-00bh-802-11bh-telecon-minutes-september-27-2022.docx)
		2. Oct 11: [11-22/1755r02](https://mentor.ieee.org/802.11/dcn/22/11-22-1755-02-00bh-802-11bh-telecon-minutes-october-11-2022.docx)
		3. Oct 25: [11-22/1810r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1810-00-00bh-802-11bh-telecon-minutes-october-25-2022.docx)
		4. Nov 8: <tbd>

Result: Unanimous Consent

1. **Timeline**

An initial WG letter ballot on a Draft 1.0 is the goal for November, but this seems unlikely. The timeline continues to show an end date of December 2023, but if the task group does not hit the ballot this month, things will slip into 2024.

1. **Motion #13 (dot11DeviceIDActivated MIB attribute)**

[See [11-22/0651r08](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-08-00bh-tgbh-motions-list.pptx), slide 22]. Move to approve the text changes in [11-22/1599r3](https://mentor.ieee.org/802.11/dcn/22/11-22-1599-03-00bh-revisions-to-rsn-extension-element.docx) and incorporate the changes into the latest TGbh draft. Moved by Kurt Lumbatis (ARRIS/CommScope). Seconded by Jay Yang (Nokia). Vote: 14/2/10 (Y/N/A), with voting status to be checked/confirmed after the meeting. The motion apparently passed.

1. **CID resolutions for 12.2.11**

Kurt Lumbatis presented his updated [11-22/1329r09](https://mentor.ieee.org/802.11/dcn/22/11-22-1329-09-00bh-cid-resolutoins-for-12-2-11.docx). The last paragraph in [11-22/1329r08](https://mentor.ieee.org/802.11/dcn/22/11-22-1329-08-00bh-cid-resolutoins-for-12-2-11.docx) has been broken into bullet points.

C- The verb ‘may’ should be replaced with ‘shall’ to be normative.

Q- It was unclear to me whether the bullet points were supposed to cover all possible actions on the part of the AP. Is there anything else it can do?

C- We need normative text here that says the AP must respond in some reasonable fashion.

C- Agreed, there’s nothing in the text above about what happens when the Identifier is recognized.

C- It has been pointed out that ‘may’ is normative language too. But this text isn’t very helpful to an implementer – it basically says, “Here are also possible things that that can be done.” There’s no guidance.

Q- Do you have a recommendation here?

A- We’ve never defined bootstrapping for setting up your identities. If the STA thinks it has a valid identity and the AP does not, then you should go back to your bootstrapping process. If you are using WFA Hotspot, then go back to that. If it’s high security and you assert an invalid identity, maybe the guards come out and arrest you.

Q- Within the scope of IEEE 802.11bh, what do you think the AP should do?

A- It should reject an unrecognized identifier. Tell the upper layer that there was a failure. Saying that the AP can do anything it wants isn’t helpful.

C- I agree this should be helpful to implementers; it should be helpful to be both AP implementers and non-AP STA implementers. I would assume that in this case, the 4-way handshake would continue. But I don’t think the AP should be required to do so as we have never required that before when there was a leading recognition failure. I think it’s useful to note what the AP could do when the identifier is not recognized, but it shouldn’t be normative. For bootstrapping, the non-AP STA has no way of knowing whether its bootstrapping credentials remain valid. In my view, this full paragraph more valuable as a note without mandating AP or non-AP STA behavior.

C- This text should be an “If” statement, not a “When” statement. It’s exception handling. You have to know what the AP will do, which I think should be assignment of a new identifier. You don’t have to say why. That newly assigned identifier could be the one just received. But the AP saying nothing (ignore the identifier option) makes no sense.

C- For me, this paragraph is like a feedback mechanism. It looks like AP text action, but it is more beneficial to the non-AP STA. This is one thing we missed in the draft. Normally, with this kind of identifier, acknowledged/not acknowledged needs a status code. I think this paragraph tries to do that. We don’t have a status code in the 4-way handshake. But it seems odd to assign a new identifier. Giving feedback to the non-AP STA is useful. We could put a note for some of the points.

C- This highlights a fundamental disagreement in this group. This situation happens when the key used for generating these things gets changed and the non-AP STA is using an old key and therefore its responses can’t be parsed correctly. Annex Z requires an identity in order for the function to act. Some people think the identifier is something the network just dreams up and it has no bearing on any state or anything else. There’s an underlying identity that the client has. If the STA tries to associate and the AP just hands it a random identity string, I don’t see how that’s useful to anybody.

Q- I think the text is useful, but after listening to others, there are changes needed. Did we agree that dot11Active was on a per BSS or per AP basis? Depending on that choice, this text might need to be rewritten.

A- It’s activated per SSID.

C- Then it should work.

C- We’ve had discussion in the past whether we wanted a network-generated ID or the STA had to provide material to the AP to generate an ID. This was written as a random blob generated by the network and assigned to the non-AP STA. I tried to write this text in view of a network-generated ID. There have been submissions about a STA submitting an ID or material used by the network to generate an ID, but I don’t believe we had consensus for this. This is preliminary text to see if we can reach consensus.

C- Let me get back to the idea of the network pulling identities out of the air and assigning them to the STA. If the network is free to choose identities, how is this useful for troubleshooting? The user can’t tell what the identifier is, which needs to be conveyed to the help desk for troubleshooting. And each network could choose its own identifier contents, which could be confusing. There are lots of things in this spec that are not defined, but what we have defined should address our identified use cases.

C- The protocol we have in the draft allows for completely random values and it allows the design given in Annex Z for protecting a longer-term identifier. Both work. As far as the draft is concerned, it is silent about the mechanism for the opaque identifier generation. We do have use cases that work fine with a random value. The network can recognize a returning STA with a random identifier. I don’t know if that’s a useful use case, but it’s there. I don’t agree that a random ID is useless. I’m claiming there are multiple ways the identifier can be used, but I think we should do more than an informative annex. We need normative text for a scheme and the remainder gets its own (non-normative) annex. I think that’s fine and by design for the protocol. I don’t think we should require Annex Z with its out-of-band provisioning mechanism. That would be limiting.

Q- A question about the second bullet. What’s the acknowledgement mentioned there?

A- We had discussion in Montréal that there was a need for the AP to indicate it had recognized the non-AP STA. One recognition was, “I know you, keep using your ID.” The other one was, “I recognize you, here’s a new ID.” I could change “in acknowledgement” to “as acknowledgement” or “as feedback that it has been accepted.”

C- We need to make sure we understand the intent before wordsmithing “accepted”.

Q- What does “does not wish to recognize” in the third bullet mean?

A- You gave an ID to the network in the wrong format, so it can’t figure it out.

C- But that’s a different meaning. “I want to recognize you, but I can’t.”

C- The first use case I don’t know who you are, but I’ll give you an ID I recognize. The second one is, “Okay, keeping using that ID, I agree to recognize.” The third bullet item is “I don’t know you and I’m not willing to deal with you.”

C- We probably need a straw poll to determine what concept we are trying to accomplish here, rather than wordsmithing things.

C- This is brand new text. I would simply make it that the AP assigns a new ID if it receives an unrecognized ID. Nothing more. Don’t give back one that the AP can’t handle or recognize. The “ignore” option should not be allowed.

C- I would expand on that. The third bullet adds nothing but confusion. Remove it. Rejection should be explicit. So should identity assignment.

C- I like requiring the AP to do something, but it seems to be against the use case that was described. I think it’s valid that an identity has to come from an out-of-band step provisioning mechanism. In that case, it’s unrealistic to assume the AP can generate a new identity on its own. I think we have use cases with conflicting requirements. Yes, the AP could be mandated to assign a new ID, but it doesn’t work when there’s an identity mechanism that is out-of-band of the STA/AP interaction. Whether that is done should be conditional if the network doesn’t use Annex Z.

C- Or the AP could return a failure and tell the STA to start over.

Q- Are those two options the only options that make sense?

C- In the standard case, where the ID was allocated earlier, then if the AP wants to, it assigns a new identifier. Same as if there is no identifier. Then there’s no ambiguity. In both cases, the AP doesn’t know who it is. I understand the AP doesn’t create the identifier. It assigns it however it is generated.

C- The language we have in the current baseline and this document do not address the [Annex Z] use case. And we aren’t looking here at a “no ID given” use case. We do need to make sure we have an understanding of the use cases before we can have the discussion.

C- In the second bullet, if the AP wants to return recognition status, it should be explicit, not implicit. If you look at the baseline, there are a lot of similar approaches, like for PMKID.

Straw poll: If an AP receives an Identifier that is not recognized it can:

* Assign a new identifier (and return it)
* Use the received identifier (with some feedback this is what happened)
* Continue the 4-way handshake and association with no identifier
* Fail the 4-way handshake/association

C- I think we need a paragraph that indicates that an identifier is either AP/network generated locally, or it is derived by an out-of-scope process.

C- This presentation is an attempt to answer comments received during the comment collection.

C- Yes, that’s understood. The question is how to get the group to a consensus, independent of the comments. Then we can address the comments.

C- I don’t think the text of the straw poll covers the authentication of the STA well enough. When the AP assigns the STA an identifier, it does not know if 4-way handshake authentication will succeed. So, you probably want to address the case where the AP assigns an identifier, but the 4-way handshake fails. In that case, the identifier should be discarded. If an authentication succeeds, then the AP-assigned identifier should be used going forward.

C- I’m not sure we need to cover that here.

C- The first bullet point should say that the identifier is used assuming that the 4-way handshake succeeds.

The straw poll has been split to have an additional portion separate from the text above:

An identifier is generated by:

* AP/network locally generates it
* It is derived by an out-of-scope process

C- Annex Z is covered in our baseline. The ID being generated externally, can still use a different, protected, network-generated ID for authentication purposes here. We need to be careful about what mean by an identifier. Annex Z has a specific meaning for the term. That one is not generated by the network. A blobified version of that is generated by the network. The straw poll is confusing because we have two different identifiers under discussion. One is an input to generating an opaque identifier. I don’t know if explaining makes things clearer.

C- My problem is that we don’t have to use the algorithm.

C- It still works – the blobify function could return the same value.

C- You could delete Annex Z as we don’t have to do it.

C- Correct, but it’s a useful example.

C- We have multiple identifiers in the baseline. I don’t know what we are referring to here.

C- I think there’s the Annex one and the AP-generated one.

C- You can use them together. It’s not an ‘or’. You could do both.

C- I am tempted to say that we can’t run this straw poll until we understand things better, perhaps with a paragraph or two to make things clearer. The point is that the AP sends a new identifier in message 3. At that point the AP has completed successfully the part of the association that requires the AP to recognize the STA. Message 4 isn’t germane to that.

C- What I was saying was that there’s no guarantee the 4-way handshake completes.

C- That doesn’t matter. The STA could go out of radio range between messages. It doesn’t matter.

C- I believe we should move to a different topic and get a volunteer with the paragraphs mentioned above.

C- If we do the next straw poll, we can fix the text and return to the first straw poll later. It’s a higher-level discussion.

The straw poll that was finally run reads:

If an AP receives an Identifier that is not recognized it can (choose zero or more):

1. Assign a new identifier (and return it)
2. Use the received identifier (with some feedback that this is what happened)
3. Continue the 4-way handshake and association with no identifier
4. Fail the 4-way handshake/association
5. This condition does not need to be specified.

C- I think we can’t do 5 because implementers need to know how to address this when it happens. Don’t we have to address this case?

C- I think that’s depending on the use case/scenario. With a closed network and I know the identifiers, if I see an unknown one arrive, I would like to handle that. If the network is open, then the AP could assign a new one or use the one proffered.

C- I’m confused. I think a lot depends on what’s coming in as the previous commenter just said. If I don’t know who the incoming STA is, what does assigning an identifier to it mean? What is the state going on here when these actions are occurring. If I come in with an identifier and make it through the 4-way handshake, it can assign me one. If I can’t make it through the 4-way handshake, what’s the point of assigning one?

C- No, if you come in without an identifier or with an unknown identified, you’re asking to be recognized when you come back, regardless of who you are. In the weird the case you use an unknown identifier, as long as the STA can pass the 4-way handshake, then it should be allowed as an identifier. That keeps things nice and simple.

C- I think my answer to the straw poll changes if I have been associated previously and given an ID, or if I haven’t been.

C- The language of the straw poll is “if an AP receives an identifier”. The AP has already received the identifier, the PMK is there, and authentication has occurred. Run the straw poll. I don’t think there’s further value in discussing it more. Let’s see the results.

The result of the straw poll is: **1**: 11; **2**: 6; **3**: 3; **4**: 9; **5**: 4, with 9 participants not answering at all.

Q- Did we talk about the scenario where a returning, previously identified STA is coming back in pretty quick succession with an unknown identifier. So, the identifier hasn’t aged out on the AP. It’s using the same MAC address.

A- We haven’t talked about, but I’m not convinced we are trying to deal with that scenario. I’m not sure it adds anything.

C- Maybe it’s worth mulling over.

C- Per our current spec, such a station would be non-compliant, so I’m not sure it’s worth considering further.

C- It’s been asked why people chose option 4. There are many reasons why that could be done. Annex Z has a case where if the identifier isn’t recognized, it is not authorized to use this network. Mostly, I think option 1 makes sense, but option 4 depends on the use case.

Q- How does the STA understand why it was turned away in option 4?

A- I didn’t put that into the straw poll to save on lots of details. There could be an indication of an exact reason.

C- We should do that for option #4, because there are so many failure reasons.

C- Up to the point of denial-of-service attacks showing up, however.

C- We can remove the last paragraph by modifying the previous paragraph.

C- That’s true if we agree with #1 in the straw poll, but I’m not convinced that everyone agrees with that option.

C- Option #4 seems like a strange thing to do. We don’t authenticate the AP. We might copy the device ID if it is shared in other places. If you want to authenticate the STA, using the existing mechanisms and use the device ID. Somehow, this option #4 seems quite limiting. It always requires the device ID to be used and I’m not in favor of that.

C- The non-STA doesn’t have to provide an identifier, but the point of this paragraph was that if it did decide to provide one, this is what happens.

Q- Why would you proceed as far as failing the 4-way handshake?

A- That’s back to the suggestion of assigning an identifier if the STA wasn’t recognized as a simplification.

Q- Can we rule out some options?

A- Maybe #3?

C- I think we have a problem of people not understanding the use cases and therefore pulling the options that support them.

C- Read Dan Harkin’s presentation from yesterday that covers that use case very clearly.

Q- Why does #3 eliminate it?

A- I misunderstood. However, I don’t want to eliminate #3 either.

C- I’m just suggesting baby steps by removing options.

C- I don’t support that point. The AP should be able to do whatever it wants. I don’t think this straw poll was all that useful.

C- Well, #5 can be removed.

C- Sure, that’s agreeable.

C- If there are exceptional cases that mean option 4 happens, write it up as a separate paragraph. Just have a nice set of rules. Trying to make all options under a single use case is wrong. Keep it simple.

Q- I really don’t understand the answers we got on this straw poll. We’re talking about a STA that’s been associated at one point and was assigned an identifier. Now it is coming back to the network. It pings the AP with its identifier, which is tied to its past association. With this case, is that the precursor to the straw poll?

A- There’s also identifiers that are assigned out of band and there’s never been an association.

C- Fine, the STA thinks it has an identifier that it believes the AP knows and has a correspondence to a security context. Then the STA pings the AP, but the AP doesn’t know it. I’m assuming that the STA is using the identifier to get a security context back.

C- That’s a leap we haven’t made: that these identifiers are used to identify security associations.

C- Either way, if the AP hits this identifier, there’s some context associated with it. But since the AP doesn’t recognize, what possible use would there be to assigning an ID to something you can’t identify. Without an association, what’s the point of assigning the ID?

**The meeting was recessed 3:30 p.m. ICT.**

**Meeting November 16, 2022, 8:00 a.m. to 10:00 a.m. ICT**

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

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

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

**Secretary: Peter Yee (NSA-CSD)**

**Editor: Carol Ansley (Cox)**

**Mark Hamilton, the TG chair, called the meeting to order at 8:02 a.m. ICT.**

1. **Policies and procedures were presented by the chair. (Slides 4 to 15)**

The meeting registration requirements, meeting protocol, attendance, patent policy [no claims noted], copyright policy, and code of ethics & conduct were all displayed.

1. **Agenda**

The task group agenda is found in [11-22/1703r02](https://mentor.ieee.org/802.11/dcn/22/11-22-1703-01-00bh-agenda-tgbh-2022-nov-plenary.pptx) (approved by unanimous consent and updated over the course of the week to [11-22/1703r07](https://mentor.ieee.org/802.11/dcn/22/11-22-1703-07-00bh-agenda-tgbh-2022-nov-plenary.pptx)). The primary agenda is:

* **Attendance, noises/recording, meeting protocol**
* **Policies, duty to inform, participation rules**
* **Organization topics:**
	+ **November Plenary meetings: [Ad-hoc, Monday, 8:00-10:00]; Tuesday, 13:30-15:30; Wednesday, 8:00-10:00; Thursday 8:00-10:00**
	+ **Approve September interim and Sept/Oct/Nov teleconference minutes**
	+ **Timeline update review**
* **Issues Tracking:** [**11-21/0332r37**](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* **Motions record:** [**11-22/0651r08**](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-08-00bh-tgbh-motions-list.pptx)
* **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)
* **Contributions (slide 21)**
* **Way forward to D1.0 (slide 22)**
1. **Discussion on MAAD and all that goes with it**

Graham Smith (SR Technologies) presented again [11-22/1650r05](https://mentor.ieee.org/802.11/dcn/22/11-22-1650-05-00bh-discussion-on-maad-and-all-that-goes-with-it.pptx), a document that he had previously presented in an abbreviated manner during a teleconference. Smith is advocating for a “pre-scheme”, that deals with pre-association use cases, and in this case for the MAAD (MAC Address Designation) proposal. The AP assigns two new MAAD MAC addresses at every RSN association, one used for association, the other for probing. The latter is used optionally. The former is optional if the STA does not wish to be identified, but if used, it must also be used during reassociation as well. Addresses are assigned as part of the 4-way handshake, except when using FILS, in which case the addresses are received in the Association Response frame. MAAD can co-exist with Device ID. A fourth idea for overcoming spoof AP tracking of a STA is given that involves an ID assigned by the AP to the STA. During a Probe Response, the AP sends the ID if it recognizes the MAC Address #2 used in the Probe Request by the STA. It sends a random ID value if it does not recognize the STA, so that it is not obvious to an attacker what is a real ID. New addresses and IDs are assigned upon association. Having made his argument, Smith points to [11-22/1584r02](https://mentor.ieee.org/802.11/dcn/22/11-22-1584-02-00bh-more-than-one-scheme.pptx), which asks if we can’t have both types of schemes in IEEE 802.11bh.

C- We don’t seem to have a full understanding of the security requirements we are solving. As soon as an assigned address is used in Address #2 in a Probe Request, it seems to be less private than a fully random MAC address scheme. You continue to use the same Address #2 until a successful Association, which then assigns a new pair of addresses for that network. We haven’t covered whether the MAC address field is the right place for these pre-scheme identifiers. The MAC address gives certain constraints. Since we don’t have consensus on the security requirements, it’s hard to say where the right place is. IRMA and RRCM probably don’t scale well in enterprise and public use scenarios in terms of the work the AP needs to perform but could be acceptable for home networks.

C- None of these schemes ever talk about the overhead on the AP. In Appendix Z, there is discussion of AP overhead for the Device ID scheme. I’d like to see the same given for MAAD. As for the “local bit” (locally administered bit), it’s the network administrator that administers those addresses. Thus, I’m more in favor of MAAD than IRMA or other STA-generated schemes. MAAD could allow the network administrator to allocate addresses in an IEEE 802c-compliant manner and in a way that has meaning to the administrator.

C- MAAD was designed to eliminate the load brought about by IRMA. It only requires lookups.

1. **TG bh More than one scheme**

Smith then showed [11-22/1584r02](https://mentor.ieee.org/802.11/dcn/22/11-22-1584-02-00bh-more-than-one-scheme.pptx). Multiple schemes (Device ID, MAAD, IRM, RRCM, IRMA) can all be supported simultaneously. Device ID and any of the others would pretty much cover all the use cases. The network decides which schemes are acceptable. IRMA and RRCM bring about a certain load on the AP that the others don’t. It probably makes sense to have the fewest number of schemes necessary to cover the use cases. Smith provides various combinations of scheme options that could be run through straw polls or motions.

C- We need to do something. I don’t want MAC addresses used for a pre-scheme. I would consider a pre-scheme if the identification is moved to some other field. I’m coming around to cover some of the pre-association use cases, but not with the exact pre-schemes given.

C- I would need to see a presentation of what this change to one of the pre-schemes is. I can’t visualize exactly what you mean. There’s also the question of how much extra work is required to do this modified pre-scheme.

C- It has been a while since we had a motion to add new things. Maybe a straw poll to see if a generally acceptable scheme using some identifier before completing Association is something we should work on.

C- How about another option, Device ID and RRCM? I don’t think we need option E (Device ID only) as it is already in the draft. But I would like to cover pre-association use cases to meet industry requirements.

Q- When it comes to the Device ID, doesn’t that cover all the use cases we need to cover? What’s left out if we do Device ID?

A- Device ID doesn’t cover the use cases on slide 19 in [11-22/1650r05](https://mentor.ieee.org/802.11/dcn/22/11-22-1650-05-00bh-discussion-on-maad-and-all-that-goes-with-it.pptx). These are 4.1, 4.2, 4.9, and 4.10.

C- The moment a STA identifies itself to an AP it has not previously authenticated to…

C- 4.2 (home control) can be covered by pre-entering the initial MAC addresses.

C- I don’t see the necessity for doing the pre-association use cases. I don’t see why the STA would want to take on the risk of doing one of the pre-schemes.

Q- What’s the risk?

A- You are identifying yourself to a network that you haven’t authenticated to before.

C- I’ve already covered the spoof AP case, so outside of that, the STA would not be authenticating to a network it had not authenticated to before. And in the spoof AP case, there are mitigations in [11-22/1650r05](https://mentor.ieee.org/802.11/dcn/22/11-22-1650-05-00bh-discussion-on-maad-and-all-that-goes-with-it.pptx).

C- For the straw polls, if we include multiple schemes, there are two approaches: using the schemes separately as a choice or using them in combination. I don’t see a problem using them in combination. Another point. We have comments requesting addressing pre-association use cases, so unless we accept a pre-scheme, we won’t resolve those.

C- Remember that this straw poll is for what goes into the draft, not what the AP ends up advertising it supports. We could motion the schemes individually.

Q- For you, MAAD is your preferred scheme. If you want to use Device ID and MAAD, would you use them together or separately?

A- It comes down to the application that is doing the authentication. The pre-schemes say, “I know you”, while Device ID could do the same, or it could be a meaningful identifier (to the application). It makes sense to use both types of schemes. You advertise support in Capabilities.

C- Support is one thing; use is another.

C- They are separate KDEs. It’s up to the application.

C- [Rhetorically] How about we run a straw poll to see if we have support for a pre-association device identification scheme of any flavor?

Straw poll: Do you support TGbh working on adding a new mechanism to support identification prior to association.

C- Let’s not say “new”, let’s say “additional”. New implies that is something other than what we have seen proposed.

C- In regard to “prior to association”, it might happen in the Association Request frame. Is that prior? It might happen before completion of the Association.

Q- How about prior to State 3 in the state machine.

A- How about we just add “(or at Association Request)” to the straw poll? That way we don’t dive into the state machine.

C- That works.

Q- Should that be additional mechanisms and not just one mechanism?

C- One lesson I’ve learned is that choice is not good. The more choices you have, the worse off your protocol ends up being. I think we should take it to heart and I would argue against multiple mechanisms that are doing the same thing.

C- I think we are okay as we are. That doesn’t stop you from having multiple mechanisms. You add at least one.

The results of the straw poll were: 17/4/3 (Y/N/A).

C- We’ve had some change of heart. That’s good. There appears to be agreement to do some further work.

Straw poll: Do you prefer “pre-association identification” to be communicated via an IE (or similar frame body protocol), or MAC address? Options are “IE/frame body”, “MAC Address”, “either/both/don’t care”, and “need more information”.

C- That works for me, and I can put together a presentation if there’s support for the first option.

C- I’d like to see that presentation before doing the straw poll.

C- Yes, I can do a presentation first.

C- MAAD has been around for a while with many presentations. Putting something in the IE, I need to think about that more and mull it over. A presentation would be helpful. I would select MAC Address because I understand it. I understand why people might not want to use a MAC Address as an identifier. We’ve had many straw polls with differing outcomes. Should we take the previous one and convert it into a motion?

Q- Would that be binding in some way? Until we vote to put text in a document, it’s no more binding than a straw poll.

A- Yes, I agree.

C- On slide 24 (in the agenda, with the second straw poll). I’m really struggling with this. I think we need to do more about spoof APs and should not use MAC addresses as the pre-association identifier. We need to do more to ensure the AP can prove its identification prior to the association and that should be reflected in the straw poll.

C- Jouni Malinen (Qualcomm) will generate a presentation to help understand the second straw poll. Graham Smith already covered the spoof AP. If there are perceived gaps in that, we need a presentation or something more concrete about where the concern is.

C- I’m uncomfortable with the spoof AP concepts. This seems to be outside of the task group’s scope, which is to solve RCM problems.

C- I agree, I had the same thoughts about Graham’s presentation. He doesn’t believe they make the problem worse nor do they solve the problems we have today. Spoof AP seems more like an IEEE 802.11bi problem.

C- I believe Graham has an IEEE 802.11bi presentation on spoof AP as well.

C- The spoof AP scheme is there in case we don’t wait until IEEE 802.11bi is ready, which could take 4 more years than IEEE 802.11bh to be published.

C- I’m sympathetic to that, but we do have scopes written in our PARs.

C- I think I agree that TGbh work on spoof AP defenses is out of scope. I don’t mind using the spoof AP defenses as a justification for one of the schemes. I’m planning on a scheme that uses the ID in encrypted form so that it doesn’t matter, unless you use a unique SSID.

C- I think the problem is not that we are trying to create a scheme that allows the STA to identify that it is talking to the correct AP. I think if we have a scheme in which the STA presents an ID to an AP pre-association, it must know that it is the correct AP to connect to. I think that is within our PAR and scope.

C- I need to think about that more, but our PAR says we are to solve problems that are created by randomizing MAC addresses. Those addresses have no bearing on spoofed APs.

C- The part I’m struggling with is that we have a clear problem to solve RCM issues. But these were some issues that existed pre-RCM. Pre-association, RCM bought anonymity. If we are going to have a mechanism that takes away that anonymity, then the network needs to identify itself to the STA. Until it does so, the network is essentially anonymous to the STA. I don’t want to create a new problem. Pre-association identification to a spoofed network is a problem.

C- The argument being made is that we are not creating a new problem. It sounds like you disagree.

C- Graham did present a solution for how to identify that the AP is a genuine AP.

C- I do agree that we need to be careful, but in this specific case, I think we are being careful.

**The meeting was recessed 9:59 a.m. ICT.**

**Meeting November 17, 2022, 8:00 a.m. to 10:00 a.m. ICT**

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

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

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

**Secretary: Peter Yee (NSA-CSD)**

**Editor: Carol Ansley (Cox)**

**Mark Hamilton, the TG chair, called the meeting to order at 8:03 a.m. ICT.**

1. **Policies and procedures were presented by the chair. (Slides 4 to 15)**

The meeting registration requirements, meeting protocol, attendance, patent policy [no claims noted], copyright policy, and code of ethics & conduct were all displayed.

1. **Agenda**

The task group agenda is found in [11-22/1703r05](https://mentor.ieee.org/802.11/dcn/22/11-22-1703-05-00bh-agenda-tgbh-2022-nov-plenary.pptx) (approved by unanimous consent and updated over the course of the week to [11-22/1703r07](https://mentor.ieee.org/802.11/dcn/22/11-22-1703-07-00bh-agenda-tgbh-2022-nov-plenary.pptx)). The primary agenda is:

* **Attendance, noises/recording, meeting protocol**
* **Policies, duty to inform, participation rules**
* **Organization topics:**
	+ Next meetings plan
	+ Timeline update review
* **Issues Tracking:** [**11-21/0332r37**](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* **Motions record:** [**11-22/0651r9**](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-09-00bh-tgbh-motions-list.pptx)
* **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)
* **Contributions (slide 21)**
* **Way forward to D1.0 (slide 24)**
	+ Motion on initial WG LB
	+ Alternative approach(es)? Agree on specific requirements?
* **Respond to Liaison from WBA:** [**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)
* **Next steps (slides 25, 26)**
1. **ID encoding in “pre-schemes”**

Jouni Malinen (Qualcomm) presented [11-22/2031r01](https://mentor.ieee.org/802.11/dcn/22/11-22-2013-01-00bh-id-encoding-in-pre-schemes.pptx). This is an alternative to using MAC addresses (primarily Address 2/TA) as identifiers (as is done in MAAD, IRMA, RRCM, etc.). MAC address encoding has no length impact, but it also limits the identifier to 46 bits. Its use is difficult for 3rd parties to determine because PDUs appear the same as any other PDUs that aren’t using MAC addresses as identifiers. Instead, Malinen proposes the use of a new information element to carry the identifier. This is easily detected by 3rd parties, but it also makes processing easier on the AP as it can trivially determine if such an identifier is present. The IE can carry a longer identifier than 46 bits, but if needed, the AP can map this to a MAC address. Using a larger identifier IE allows the use of public key encryption of the ID. That public key would be received from the AP by the non-AP STA during the 4-way handshake. The AP then simply decrypts the IE using the private key to obtain the unprotected identifier. One suggestion is to use HPKE (RFC 9180) base mode with a single-shot API. Additional, optional protection can be layered on top of the public key mechanism as a defense against frame cloning and replay. Address 2 could be included as AAD (possibly along with additional header parts) as input to HPKE. A keyed (per non-AP STA) hash with various pieces of information and time stamps is one option. Malinen’s scheme does have a higher processing requirement on the non-AP STA in order to perform the HPKE Seal operation. This is in comparison to just filling in an identifier in a MAC address field. Also, each non-AP STA needs storage for the public key of each ESS with which it wishes to be identified. The AP requirements are processing of the HPKE Open for each frame containing the proposed IE. This might open up the AP to a DoS attack due to the cost of performing the public key decryption on these frames. The storage requirements are for a single private key for the AP instead of a list of MAC addresses. The overlap with IEEE 802.11bi’s needs should be examined along with consideration of what parts of the MAC header should be protected for IEEE 802.11bh’s needs.

C- Since a public key is passed to the STA during the 4-way handshake and RFC 9180 uses uncompressed public keys, there’s an Internet-Draft in the IRTF CFRG that might be of use there. [IETF liaison requested to push on CFRG to move this along.]

Q- Do you think proof-of-possession of the private key is needed for the public key that’s sent?

A- I haven’t identified any use case that needs that.

Q- How could it be that the MAC address could have a collision problem in 46-bits when the AP is assigning the MAC address to be used as an identifier?

A- Locally administered MAC addresses are used for multiple purposes. So, it’s not just the AP in question that is generating locally administered values, so there could be collisions.

Q- Is the same public key used for all STAs associated to the AP.

A- Yes.

Q- Then a 3rd party that is registered to that AP could track other STAs that are registered?

A- No. The public key is used for encryption, but the encrypted value can’t be decrypted by other STAs.

Q- To know what key to use, the AP must parse all the known addresses?

A- For HPKE, there’s no need to. The decryption suffices.

C- I have a proposal for 11bi that encrypts some IEs for privacy reasons. 11bh and 11bi have some overlap. As we do our work here, we should consider making sure our format is suitable for 11bi’s uses.

C- I agree we must do that research. I don’t know if we have to support them because I don’t have data yet. We need to figure it out first.

C- Sort of like Spoof APs. Something to keep in mind, not something we have to answer now.

Q- This is one-way encryption, with the public key going from the AP to non-AP STA?

A- Yes.

Q- Since the non-AP STA is encrypting, it is setting the ID and delivering it to the AP encrypted.

A- Yes. The ID could be from the AP, it could be generated by a rule, or something completely different.

Q- The non-AP STA associates the first time and gets the public key from the ESS. When it returns, it encrypts an ID in an IE in a management frame.

A- It could be used for a Probe Request. It does not have to be an association.

Q- This ID will not change? If you send the IE in two management frames, they will be the same?

A- HPKE will change the output each time it is used, so the encrypted version will not be the same. Also, when completing a 4-way handshake, a new ID value can be supplied to the non-AP STA.

Q- What’s the big advantage? Sticking an ID and encrypting as opposed to changing the existing MAC address doesn’t seem to have a big advantage to me. I don’t know where the ID starts from. This changes the scheme so that the ID means something rather than just be associated with the non-AP STA. I’m struggling to see the big advantage compared to a MAC address that changes every time. This doesn’t solve the Spoof AP problem either. I will send questions in writing. This scheme is probably trying to solve another problem, not the same one as MAAD.

A- There are different views what the requirements are for protection. Where the ID comes from? It could be the same as used in MAAD. You claim that the design using MAC addresses cannot be tracked. I don’t agree. One key difference: if you use HPKE, what’s in each frame will change each time. It is inconvenient to force a device to use the same MAC address. Vendors don’t like this. We should deliver something that implementers are willing to do. But we do need to define our security requirements before we can say we have the right solution. I agree that a single MAC address given in a 4-way handshake can be used for client steering, but as soon as it is used for access control decisions, I’m not so happy.

C- Let’s consider this presentation further via email.

1. **Resolution for CID 19 and CID 20**

Okan Mutgan (Nokia) gave resolutions found in [11-22/1732r01](https://mentor.ieee.org/802.11/dcn/22/11-22-1732-01-00bh-resolution-for-cid19-and-cid20.pptx). Both focus on PASN and FTM from IEEE 802.11az. The CIDs also mention WUR (IEEE 802.11ba, but this isn’t completely clear). CID 19 and CID 20 request consideration for PASN and FTM when using Device ID. For CID 19, Mutgan suggests using the existing Device ID in the authentication frame exchange in PASN. However, the authentication frame body is not encrypted, so an encrypted IE might be a way around that given that PASN provides a PTK. A couple of encrypted schemes are given for protecting the Device ID value, although there’s a cleartext transmission of the Device ID initially.

Q- This uses PASN for messages 1, 2, and 3. This does Diffie-Hellmann that’s subject to a man-in-the-middle attack. There’s probably no authentication. If there’s any value in those IDs, then encrypting them won’t matter.

A- Yes. The FTM frames are protected.

C- Encrypted but perhaps not really protected.

C- I think this is worse than before. I don’t see any real protection for the ID without authentication.

C- I agree, without authentication here, there’s little point to adding an ID here. A bound credential is required for that. I think Malinen’s proposal with HPKE would be a better solution.

Q- Maybe that would be an approach. But you say there’s no authentication here because there are 3 messages here?

A- No. It’s because a man-in-the-middle can insert itself into the exchange and neither side will be the wiser. Diffie-Hellman is different from an authenticated key exchange.

Q- Then the whole PASN is not authenticated, right?

A- Yes but adding a Device ID to that is not doing much.

C- We need to consult a PASN expert.

Q- On slide 16, this is ranging, why do different APs need to know that it is the same STA that is ranging?

A- We need an 11az or 11aq expert here to provide some input.

Q- Is there an assumption that the multiple APs are exchanging Device ID securely on the backhaul?

A- That’s something that 11az people would know.

C- These APs are all part of the same ESS and are assumed to have a secure backhaul.

Q- Isn’t this design outside of the scope of 11bh?

A- This is an attempt to respond to the comments. For each session Device ID, we have to do something like Slide 16, otherwise things don’t work. One session sends the first Device ID, and then each session in turn assigns a different Device ID.

C- Maybe we should take a step back, talk to 11az and 11aq experts to determine if this is in our scope and whether we need to fix it.

C- This seems like a non-issue. If a STA is in an area doing FTM, a unique (random) MAC address is used for the duration of the ranging operation. Each session can use a different MAC address. If the AP needs to know who this is, don’t do it through FTM. Do a connection or something else to identify to the STA. Why mess with Device ID in FTM?

1. **Enhancement of RRCM**

Mutgan next presented [11-22/1802r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1802-00-00bh-enhancement-of-rrcm.pptx), which is an enhancement to [11-22/0818r04](https://mentor.ieee.org/802.11/dcn/22/11-22-0818-04-00bh-use-case-further-discussion-and-rule-based-random-mac-identification-proposal.pptx). He gave a recap of RRCM and IEEE 802.11w (management frame protection). His proposed enhancement to RRCM is to have the AP and non-AP STA generate and store a secret key during the initial association to protect pre-association management frames (such as ANQP, authentication, association) in the future. Then, when a STA returns, it can use this key to protect management frames (which ones is TBD).

C- Process-wise, I’m concerned. This talks about encrypting Association frames, which is an 11bi topic and is being worked on. This is not within our scope.

C- We are trying to solve the problems that RCM created without creating new privacy concerns. The challenge we run into is that some of our proposals have created new privacy concerns. To solve those privacy issues, we run into 11bi’s scope sometimes. I don’t have a good answer how to handle the delineation.

C- This is a supplement to the existing proposal.

C- I want to make sure we define something that will be implemented. As a vendor who implements these sorts of things, I do not want to implement two different ways of encrypting Association frames. If 11bi creates a different scheme, probably only one of them will get implemented. We should limit our scope to not overlap with 11bi. We may have to ask them to cover certain things if we keep our scope limited.

C- This enhancement came up because of comments from Malinen and Kneckt. Now we are told that somethings should be done in 11bi. I don’t think we can put everything in 11bi. 11bi is not for identification.

C- I think we are going too far ahead. The privacy issue is related to long-lived identifiers. Here, we are talking about a device over a period of time that isn’t clear. So far, I think Malinen’s proposal makes a lot of sense. Potentially we could have a session with 11bi, but right now I don’t think we need to address a privacy threat.

C- From Jouni’s presentation, it might work well, but here (slide 6) the protection of unicast frames is the whole body, while group addressed protects a lesser amount. This looks a bit like Malinen’s proposal. Maybe the MMIE [expansion unclear] is used for the whole frame body. Something to keep in mind.

C- There are ways to combine any of the pre-association ideas with Malinen’s proposal.

Q- I didn’t hear any technical issues on Mutgan’s proposal. Does anyone have an opinion on whether it is in scope for 11bh or 11bi?

A- There were no technical objections to the proposal, but I can’t say that meant there was agreement either.

1. **Where do we go from here?**

C- Do we need to have a different sort of approach for the group? We jumped from the issues tracking document and which use cases are in scope without fully wrapping that up, although we got some sort of a direction. Now we are looking at specific technical proposals. Then we go back and ask if each one addresses use cases we agreed to and whether they are in scope. We seem to be going in circles. We dive into technical solutions, then disagree whether they are in scope. Perhaps we should go back to agreeing on the requirements that this group considers and write them down in a requirements document. That’s the typical IEEE process. I’m not sure that’s a step back since we are going in circles right now.

C- I don’t want to repeat the requirements discussion again. But we do need a common understanding on the pre-association cases. We need to understand which ones we want to address. Client steering, probe frames, ANQP, and maybe some sort of access control? I agree that we should keep things as simple as possible. Access control concerns me. Something like Device ID and MAAD might work. As long as there is a statement that says these mechanisms are not acceptable for access control. I’d like to reduce the scope, but I’m not sure how we can do that. Our discussions have not resolved in that direction.

C- We want to deal with pre-association and post-association. We have major concerns from WBA, so I hope 11bh can address these issues.

C- I think we have gotten in trouble when we lump all the pre-association use cases together in one bucket. According to the straw poll yesterday, we seem to feel some pre-association use cases are worth considering and some are not. We need to be more specific. I also want to comment on the “yes, I recognize the device, and the AP might turn on an SSID that is normally off” use case. (This is similar to a use case that Yang or Mutgan raised.) It’s a pre-association step before the association can take place.

C- It might be useful to have a joint session (teleconference or maybe during the January interim meeting) with 11bi and compare notes. You talked about taking a step back and agreeing on a set of requirements. That might be an easy way to compare with what’s going on in 11bi. We can talk about what’s being covered and what isn’t. Then good progress might be possible.

C- I’m sympathetic to that idea, but we need to do some prep work so that we can express what needs to be in 11bh to make sure the discussion is useful. 11bh needs to make sure it agrees on the use cases that we cover.

C- I think we are in danger of taking too long anyhow. 11bh was supposed to be quick and dirty, that was easy to implement. It didn’t have to be the bee’s knees. It had to be as good as RCM. We don’t have to solve AP spoofing or other things that came up. Device ID is simple, and yet we spent two hours discussing what happens when you give the wrong ID. Is that a use case? We are getting new ideas and schemes put in now? If you bring up a scheme, you go blue in the face saying that it fits the use cases and doesn’t create new privacy problems. All of a sudden, we are looking at things in 11bi’s eyes. We are protecting fields here and there. 11bh is not supposed to be dealing with all of this. If we get closer to 11bi, we might just say that 11bh has failed. You might be right that we need to agree on the use cases, but how long will that take? Are we going to dream up new use cases now? I’d put a 3-month hard limit on things. If not done by then, disband. We will have failed. If it’s going to take another chunk of time, it’s going to be useless.

C- We have a chance hopefully addressing the scope of this group if we can agree on the subset of proposed use cases. Mixing in 11bi and dividing the labor will not make us successful. To do something positive within in our scope and timeframe goals, we should define 3-4 specific use cases that we deal with. We received a long list of the problems. We boiled through that list several times. Given the problems that we have trying to address are so many and the privacy issues the solutions raise, I think we are wiser. We know that new privacy work needs to be done. If we agree on the subset of use cases that we deal with without treading too heavily into the 11bi new mechanisms area, then we might be able to do it. I think we said parental controls are outside of our scope. We can go through our use cases on teleconferences and then in January agree on subset to move forward on. Then we can apply our solutions collection, which is not insubstantial, to those problems. I think we can make progress that way. Some of the things done here are interesting and good work, but some of it really should be transferred over to 11bi. I hope we don’t have to shut down.

C- When this group started, I observed that many of the use cases would make many products not work anymore because of RCM. The valid use cases always had the problem that the network needed additional guidance, not the STA. Jouni said something about what the STA vendors would implement. There’s no real reason for a STA vendor to implement 11bh, so it won’t get implemented. Nothing we have here is compelling. So, it doesn’t matter if the APs implement it, it won’t matter if there are no 11bh STAs. I think we need to have a compelling reason for this to be implemented universally, or we should disband.

1. **Next meeting planning**

January: maybe more than 4 slots, as long as we don’t go in circles. But 4 as the default.

C- We need some teleconferences prior to the January meeting. Maybe during those teleconferences, we can decide that more slots are needed.

Suggested teleconferences: 29 November; 13, 20 December; 10 January for 2 hours at 9:30 a.m. EST.

Q- Can we try 7 p.m. EST on Thursdays?

A- That’s very late for Europe.

C- I’ll try alternating them to see how it goes. Maybe later for the morning calls to catch the PST folks.

C- I’d suggest adding 7 p.m. calls, not dropping any 9:30 a.m. calls.

**The meeting was adjourned at 10:03 a.m. ICT.**