Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Plenary Meeting Minutes, March 13-16, 2023Randomized and Changing MAC addresses (RCM) |
| Date: 2023-03-16 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Peter Yee | NSA-CSD | Mountain View, CA, US |  | peter@akayla.com |
| Stephen Orr | Cisco | Wallkill, NY |  | sorr@cisco.com |

Abstract

This document contains the minutes of the IEEE 802.11bh plenary meeting of March 13-16, 2023.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting March 13th, 2023 8:00 a.m. to 10:00 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 8:03 a.m. EST.**

Agenda slide deck [11-23/0180r01](https://mentor.ieee.org/802.11/dcn/23/11-23-0180-01-00bh-agenda-tgbh-2023-mar-plenary.pptx)

1. **Policies and procedures were presented by the Chair Mark Hamilton. (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:**
	+ March Plenary meetings: Monday, 8:00-10:00 (pre-meeting); Tuesday, 13:30-15:30; Wednesday, 8:00-10:00; Thursday 8:00-10:00
* **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:** [**11-22/0973r15**](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-15-00bh-cc41-comments-against-d0-2.xlsx)
* **Motions record:** [**11-22/0651r11**](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-11-00bh-tgbh-motions-list.pptx)
* **Review Status of CC resolutions**
* **Way Forward to D1.0**
* **WBA liaison response**

Any comments? [None]

Any objections to agenda? [None] – approved

1. **Review Status of CC**

**CID#5**

Assigned to Mark Hamilton – question on whether we still need this item

C: I don’t think we have defined a MIB for this. Discussion on defining an MLME to address this.

A: Mark Hamilton will take an action item to work on this.

Q: Would this build on MIB definitions already done?

C: Yes – build on or interact.

**CID#7**

Group needs to decide whether to come up with another solution. Either we will have another solution to address this – or reject this CID if no other solution is agreed to.

**CID#8**

C: This is already covered.

**CID#9**

C: Is this already covered with our response codes?

Q: Comment text seems confusing

C: Proposed text changes…1329r15 – does this cover the use cases?

Q: Have we motioned 1079?

A: No

C: Would like to discuss 1079 – there are two solutions.

C: This is for the STA generated ID.

C: Where is CID#9 being resolved in the text?

Chair – we can put this on the agenda and discuss.

**CID#12**

What are we going to call this Device ID concept? Do we need a better name than Device ID?

C: Suggest we wait until we have the solutions – then we can come up with a name.

Chair – the more stuff we can do in parallel the better. Given the solution we have right now – do we want to change this?

C: If we decide to go back to Device ID – Kurt Lumatis’s submissions will need to be changed.

C: Device ID is as good as any – once we get D1.0 out, we can revisit.

***CID#12 withdrawn***

**CID#15**

C: This case may be addressed in 1329r15

**CID#16**

Q: Is this already covered?

C: This has not been covered in the MIB or MLME SAP – it is missing.

C: This is actually storing the ID somewhere.

C: Device ID is only exchanged in the EAPOL Key Frames (supplicant and authenticator) – we do not need a new MLME SAP.

C: Do we need to extend the current FILS MLMS SAP?

C: Yes, it would be a new parameter.

C: Non-FILS case – can we do with MIB?

No objection to that direction

**CID#17**

C: User Opt-in, how do you set this?

Q: The part of the MIB Kurt has done, is that sufficient?

Q: Yes – covered in 1152.

**CID#19**

C: Solved by coming up with a new mechanism or reject.

C: Submitted resolution – sending Device ID in authentication frames. Based on previous comments it may not be accepted here. Text is there.

Chair – this may not have been listed in the contributions.

C: We did not do a straw poll, but comments were mostly negative.

C: Request for straw poll in 3rd session.

Chair – let’s run on March 14th session.

**CID#24**

C: AES-SIV decrypter failure. Comment will be withdrawn. It was handled with the current Device ID. 802.11 does not talk about failures of the decrypter.

**CID#27**

Chair: Any objection to the draft text Kurt has proposed enough to resolve (1599)?

Chair will craft the motion.

**CID#32**

C: The text was modified – just need to replace if not done.

Chair – need to let Kurt know he is working on clause 9.

**CID#35**

Chair – how does Annex Z relate to our Identifiers?

C: We can pass this device ID encrypted and can use Annex Z to obfuscate it if it’s in the clear over the air.

C: This may deal with the pre-association use cases on how we obfuscate the ID.

Chair – is this waiting based on determining if we are going to address the pre-association use case?

C: This needs to be addressed in the pre-association use case.

C: Annex Z is an example of how you might obfuscate the ID.

C: Just a check if the text is clear in relation to Annex Z.

**CID#36**

This goes into the category of do we address the pre-associaiton use cases.

**CID#40 & 41**

Group has to agree if this the direction we will go.

**CID#45**

Is this covered in the current text?

A: Not sure if 4.5 was addressed in the submission.

Q: Do we still need a change in 4.5.4.10

A: Don’t think we have concluded on this as a group.

**CID#62**

Chair to address.

**CID#63**

Does 1329/1599 address this?

A: Yes.

**CID#64**

Q: Do we need another solution related to 1079?

Chair: Hopefully we can get most of this done Tuesday/Wednesday of the March Plenary.

1. **Way forward to D1.0**

Chair – we need to come to consensus on whether proceed to D1.0 with the solution in D0.2 or continue working on solutions.

C: There may be a third option – chose the option to proceed to D1.0 this week. However, for those supporting RRCM – you can have a letter ballot then add a comment to add RRCM. During the letter ballot resolution, you could then add RRCM at a later stage. This group needs to move forward. If we want to add something at a later stage, we are capable of doing that.

Chair: From a process point of view, I agree. This is kind of what we did with the comment collection on D0.2 –request to add something for pre-association.

C: There has been good discussion on pre-association use cases and solutions. Let’s proceed to the D1.0 and get a letter ballot underway. We are not excluding further work in this area.

Chair – If we go out for an actual letter ballot we will get feedback from the broader group

C: Agree that we need to get D1.0 out. Sure, things can be added after the letter ballot, but we need 75% to get it added. There is a requirement for the Chair to determine if D1.0 meets the scope.

C: Ran some straw polls for RRCM and it didn’t satisfy…maybe we can look at something else.

Chair – we need a champion of another solution to come forward and drive consensus. Any thoughts on which solution may be desirable to bring forward and discuss. We can start now or address this at the next meeting.

C: Its disappointing if this TG does not provide a solution that covers its PAR. Many feel that the present solution does not meet it. I’ve championed MAAD then went to IRM. I’ve done presentations and discussed them on the reflector but did not get support in straw polls. However, RRCM was picked in down selection, but did not receive support in straw polls. Because it doesn’t meet the PAR this gives us the problem. After two years of deliberations – to go back to the WBA and WFA with only a solution that doesn’t meet all the use cases is a problem.

C: Member agreed to present on an IE-based solution during Wednesday Plenary session (3/15).

Chair – we will have two proposals to consider.

Chair – question on whether we are meeting the PAR. Do we need to have a discussion on if we are meeting it? Should we start this discussion first? Unless we have 75% agreement that we want to proceed forward with anything, we will not go anywhere.

C: What we currently have is close enough to meet the PAR. Or if need to, we can modify it. The question is what we want to cover with our solution. Beyond that the PAR can be modified if needed.

Chair: The other approach – we could focus on the scope we want to have? Do we want to 75% support for the proposed solutions, or do we need to dive into the technical details?

No response was provided to the Chair’s comment.

C: Can we take a straw poll to make sure that Device ID is exactly what we want?

C: Nobody can suggest any other name.

Chair – is there anyone that objects to adopting the device ID name for this round of the draft.

Note: The only things that get capitalized are Field or Frame names – a concept does not have capital letters.

**Meeting adjoined at 9:45 a.m. EST.**

**Meeting March 14th, 2023, 1:30 p.m. to 3:30 p.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 meeting was called to order by the Chair at 1:31 p.m. EST.**

Agenda slide deck [11-23/0180r02](https://mentor.ieee.org/802.11/dcn/23/11-23-0180-02-00bh-agenda-tgbh-2023-mar-plenary.pptx)

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

There were no Patent declarations.

Copyright policy slides were presented (Slides 11 and 12)

1. **Agenda:**
* **Attendance, noises/recording, meeting protocol**
* **Policies, duty to inform, participation rules**
* **Organization topics:**
	+ March Plenary meetings: Monday, 8:00-10:00 (pre-meeting); Tuesday, 13:30-15:30; Wednesday, 8:00-10:00; Thursday 8:00-10:00
	+ Approve January interim and January/February teleconference minutes
* **Issues Tracking:** [**11-21/0332r37**](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* **Motions record:** [**11-22/0651r11**](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-11-00bh-tgbh-motions-list.pptx)
* **Review updates to** [**11-23/0083r6**](https://mentor.ieee.org/802.11/dcn/23/11-23-0083-06-00bh-identifier-status-codes.docx) **and** [**11-22/1329r16**](https://mentor.ieee.org/802.11/dcn/22/11-22-1329-16-00bh-cid-resolutoins-for-12-2-11.docx)
* **Results of Comment Collection on D0.2:** [**11-22/0973r16**](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-16-00bh-cc41-comments-against-d0-2.xlsx)
	+ Ready for motion on the ones that are prepared (marked in green)?
	+ Updates on assigned items
* **Way forward to D1.0 (slide 22)**
	+ **Presentation on IRM (Graham Smith)**
	+ **Presentation of 11-22/1079?**
	+ **Presentation/discussion on CIDs 19 & 20? (Okan? Jonathan?)**

Any comments? [Several additions made to the list of presentations]

Any objections to agenda? [None] – Approved with unanimous consent

1. **Approval of meeting minutes**

The meeting minutes of the January interim meeting ([11-23/0199r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0199-00-00bh-minutes-tgbh-interim-meeting-january-2023.docx)) and the teleconferences of January 31 ([11-23/0233r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0233-00-00bh-802-11tgbh-telecon-minutes-january-31-2023.docx)), February 7 ([11-23/0200r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0200-00-00bh-802-11bh-telecon-minutes-february-7-2023.docx)), February 14 ([11-23/0234r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0234-00-00bh-802-11tgbh-telecon-minutes-february-14-2023.docx)), February 21 ([11-23/0235r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0235-00-00bh-802-11tgbh-telecon-minutes-february-21-2023.docx)), and February 28 ([11-23/0264r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0264-00-00bh-802-11tgbh-telecon-minutes-february-28-2023.docx)) were approved by unanimous consent.

1. **Identifier Status Codes**

Kurt Lumbatis (Arris/CommScope) presented [11-23/0083r06](https://mentor.ieee.org/802.11/dcn/23/11-23-0083-06-00bh-identifier-status-codes.docx) on “Identifier Status Codes”. This revision now covers CID 8. It replaces the term “ID Blob” with “Device ID”.

Q- What’s the meaning of the Device ID here? The obfuscated value? Something from the Annex? An opaque identifier?

A- During the pre-meeting yesterday, it was agreed to change all of these terms to “device ID”, which can be implementation specific.

C- I had a different interpretation of yesterday’s discussion. I don’t think everything was supposed to be changed to “device ID” [note lowercase “device”], particularly the last sentence on page 4 (where “opaque identifier” has been replaced with “device ID”).

C- If we are going to allow encrypted or unencrypted ID values, then we need another bit in the figure to indicate which version is in use.

C- No we don’t.

C- Bottom line, this is a terminology question. There’s the concept of an identifier that can be (or not) obfuscated via Annex Z or something similar.

C- I think it has to be obfuscated, otherwise we are allowing tracking. It’s obfuscated to hide the identifier from a tracker. What the STA gets back in the IE is not an identifier, but an obfuscated version of it. And every time it gets passed back, it will different. That’s the whole point. Only the AP can interpret what the STA sends.

C- In our currently approved draft, it’s always encrypted. The previous commenter is talking about an extension to the existing text. There’s no requirement for always obfuscating the Device ID. That’s an option. That’s why there’s a question about what is in the device ID – is it the output from the Annex Z process or the input?

C- It makes no sense to pass this thing back and forth in an encrypted frame and that’s it. When you get to the 4-way handshake, you have to have authenticated (and been identified). This is supposed to give the STA something to use later to identify itself to the AP. Why would I want to get something that’s only in encrypted frames? Then the device doesn’t need it because it already authenticated, which implies identification. The whole point is to send Device ID in a frame that is not part of the 4-way handshake.

C- That’s not what’s in our current draft.

C- What we have in our current draft doesn’t match that statement. We’ve defined sending the Device ID from the AP to STA in an encrypted form. I don’t think this is pointless. As for this agenda item, it covers what’s in the current draft, not what we would like to do in the future. And my question of whether “device ID” makes sense in that last sentence on page 4 still stands.

C- This isn’t pointless. When the STA rejoins with a different MAC address, it provides back the ID it was given and the network recognizes. Whether we want to say that the device ID field contains a Device ID or an opaque identifier, I’m willing to change that now, just to get on with life.

C- I thought I understood it, but I’m getting confused now. I don’t like the “from an AP”. If a STA is sending this, then it is going to provide the ID allocated by the AP or an AP, but if an AP is sending this, then it is allocating a new one, if I recall correctly.

Q- So, “allocated by an AP”?

A- Yes. This is a protected IE used in the FILS case, not something in the open. It’s a variable length field which is known as the device ID. If it is opaque or not, the STA doesn’t know. It just knows what it was given. It’s only there if the AP is giving the STA a new one. In the case the AP is not providing a new Device ID, then the STA can keep it and not use a new one.

C- That’s covered in 11-22/1329.

C- Whatever is in there, as has been said, could be an opaque identifier. The STA doesn’t know. The AP understands it.

C- Let’s get back to point of this statement. We don’t need the Annex if this IE is used only during the 4-way handshake. It’s supposed to hide the device ID from a 3rd-party tracker by changing it each time. If it’s encrypted, there’s no need to do so. If all we are going to do is not authenticate devices and just use the Device ID, there’s no need. But I think it’s very limiting to constrain this field to a small number of AKMs. I don’t think we should be doing all this work if this is the end result.

C- That gets back to what further we want to do with the draft. What we are talking about is what’s in the draft right now.

C- You made a good point in last week’s email exchange. Using the opaque identifier in the pre-association use cases requires the obfuscation. But these aren’t covered in the draft currently. We don’t deal with the identifier in an IE in a frame that’s not encrypted. We could do that in the future. I’m just trying to deal with comments on the current version of the specification. We shouldn’t get caught up in future-looking concepts. Let’s focus on the resolution to comments on the existing draft.

C- I agree that the current draft doesn’t require the annex. We could even delete it if we don’t agree to handle pre-association use cases. The draft does have value in EAP cases where IEEE 802.1X is used, especially if the AP is not part of the authentication server or able to be party to the authentication. So, I think there’s more value than has been claimed in this discussion. I’d like to return the meaning of the sentence in question.

Q- Within the context of this sentence and resolving the comments we have in front of us, can we live with the text that’s on the screen? Any objections? (Include a reference to Annex Z to the sentence after obfuscated identifier).

C- I’ll make a similar change on page 5 for the Device ID KDE.

A- [No objections.]

C- I’ll make the changes and post a r07 for presentation for a straw poll, hopefully before the end of the plenary.

C- We can probably do it tomorrow morning.

Q- You have the recognized/not recognized bit. How is that used?

A- I’ll show that in the 11-22/1329 document. This is setting up for that presentation.

Q- Did you want the two documents merged?

C- It’s a little confusing to have separate documents that are that closely tied yet don’t reference each other.

C- We could ask for a merger of the documents.

1. **CID Resolutions for 12.2.11**

Lumbatis presented the related [11-22/1329r16](https://mentor.ieee.org/802.11/dcn/22/11-22-1329-16-00bh-cid-resolutoins-for-12-2-11.docx). We had previously agreed to accept the text for the resolutions. He replaced the generic term “identifier” with “device ID” throughout the text. He also added a term “participating network”, which refers to 11-22/1599, which talks about a device being active.

Q- What’s meant by “participating”?

A- This is a high-level description. We describe it better in 12.2.

Q- Using those words? Probably not.

A- I can remove “participating”.

C- I thought Clause 4 was supposed to have normative language. Replace “may” with “can”. But the opt-in isn’t needed. The STA implicitly opts in by using the identifier it was given. If it doesn’t want to opt in, it won’t use that identifier.

C- I think this goes back to the MIB variables indicating usage. I can change “may” to “can”. Is it germane to define something in clause 4.5 that is not mentioned elsewhere in the specification.

C- I think opt-in is implicit through use. No separate statement of “Hi, I set the bit, I’m opting in” is needed.

Q- This is supposed to be just a high-level overview in clause 4. We are saying that the STA can send a device ID. It’s not required. Doesn’t this seem consistent with what you’re asking?

A- I don’t agree, but let’s move on.

C- Change “STA” to “non-AP STA”.

C- That’s existing text. If you want to change that, submit a request to REVme.

C- If you want to make a change to baseline spec, you do not need to go to REVme.

C- I’m not sure you “exchange” an ID. The non-AP STA provides an ID that was previously provided by the network to be pedantic about it. I think words could get this text a little bit closer.

Q- So you want to put “non-AP” before all “STAs” here?

A- Yes.

C- I don’t think doing so is that critical. Adding “non-AP” before “STA” doesn’t add a lot of value. Non-AP STA makes sense in section 12, but in the high-level explanation, it’s unnecessary. I don’t feel strongly about that, however.

C- This is in the 3rd paragraph of text in the baseline that does say “non-AP STA” in the first paragraph.

Q- Shouldn’t “While discovering network” be “During WLAN discovery”?

A- Yes, that’s fine.

C- I believe you’ve addressed the scope of the comment. There may be bigger concepts to deal with, but we can hit those the next time around.

In 12.2.11, a generic “identifier” was changed to “device ID”. And text for recognized/not recognized has been added, going back to the previous question about that.

Q- Did you clarify what the last paragraph in 12.2.11 means?

A- We discussed that, and we made a new contribution to add “identity state” to 12.2.10. Section 12.2.10 talks about identity states. This is used by the AP to tell the STA it has no idea who he is. So, the STA must go back and (re)establish a shared identity state with the AP.

Q- So what do I do with this information? I’m not recognized, okay.

A- Whatever you were trying to do by establishing your identity will have to be redone.

Q- Why do we need this text?

A- It’s possible that you deleted an SSID’s information or your entry with the SSID timed out after two years. There were several CRs that asked for passing back and forth state information to indicate where the identity had been recognized.

C- But we aren’t specifying any actions. It’s just “nice to know”. I can live my life without knowing that I’m identified or not identified. Either specify actions or drop this text. If there’s something broken on the network, should I present this information to the end user? What should I do?

C- I appreciate your comments, but you are revisiting previously agreed upon comments. We agreed to pass this information.

Q- It’s okay to satisfy CIDs. I don’t remember if we had a vote on this facility. I’m in the same camp as the previous commenter. You need to have two IEs or KDEs for each connection because you’re always acknowledging it. Did we actually vote in favor of this? Or a straw poll.

A- We’ve had straw polls, but I don’t recall if we had a motion.

C- This text means you have to send a KDE always, just to signal the status.

C- It’s not a new KDE. It’s new fields in an existing KDE. As part of the text in section 13.29, I say what should be done by the AP if the STA is recognized. That could be “I know who you are. Use this ID the next time.” We have hashed this text out over and over. It has been straw polled, but it has not been motioned.

C- This presentation is responsive to the request made to the presenter.

C- I think we should accept this document as is. We have been discussing this document for way too long. Get it in the baseline document for further discussion. It’s close enough. Let’s not continue to edit the redline version.

1. **Results of Comment Collection on D0.2**

C- I’d like to have a motion tomorrow morning that approves the resolutions to CIDs that are covered in the document’s that Kurt just briefed. Those CIDs are marked in green in the comment collection spreadsheet (currently [11-22/0973r16](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-16-00bh-cc41-comments-against-d0-2.xlsx)).

C- I read CID 24 in your motions list. It has been withdrawn.

C- That’s fine. The motion approves the actions taken, including withdrawal. I know this is a big pile of CIDs, so please look at it offline and come back to the next meeting.

The notes column categorizes the items that have not been done. If we don’t want to add a solution to resolve the comment, we will have to reject them by saying the group didn’t want to do so. Otherwise, we will need to have text ready to go to put into the draft.

C- Annex Z still uses “identifier”, so we may need to clean that up.

C- After we figure out the way forward, we can consider dealing with that.

1. **CID 32 resolution**

Antonio de la Oliva (InterDigital) presented [11-23/0452r00](https://mentor.ieee.org/802.11/dcn/23/11-23-0452-00-00bh-resolution-cid-32.docx), which aims to resolve CID 32. It changes the description of Device ID. MLME-SAP has been updated to indicate the Device ID is only included if active and using FILS.

C- This will be added to the comment collection resolution spreadsheet for motion tomorrow.

1. **Resolution for CID19 and CID20**

Okan Mutgan presented the previously presented [11-22/1732r01](https://mentor.ieee.org/802.11/dcn/22/11-22-1732-01-00bh-resolution-for-cid19-and-cid20.pptx), which covers CIDs 19 and 20. CID 19 is about the Device ID mechanism for unassociated PASN operation. CID 20 deals with multiple FTM sessions. In FTM (Fine Timing Measurement), an unassociated STA doing FTM does not go into the 4-way handshake and will thus not get a Device ID. Mutgan proposes three possible solutions termed “unencrypted solution”, “encrypted solution 1”, and “encrypted solution 2”. The group has not shown consensus on the preferred option.

C- Regarding the use case for the PASN mechanism. As for the ways of doing it, I don’t like the part of sending without encryption. Encrypted solution 1 would be all right. I prefer to start with PASN message 3. Note that PASN can be run fully unauthenticated. We need to make sure not to use that mode unless we are using an obfuscated value.

C- Looking at the CID 20 part, the problem that I see is that if the opaque identifier is used, then that has to be set already from a previous association. I’m worried this scheme could blow up a bit.

C- This use case is a bit different from normal use cases. Here, the STA wants to use a different RCM for each AP its talking to with FTM.

C- So you go to the first AP and get an opaque ID. Then you use that every time you talk to each AP?

C- Perhaps we should hear from the commenter why he wants this mode of operation.

C- You are correct that if we use the obfuscated value in a non-encrypted frame, we need an indication from the AP for which type of value was supplied. PASN could obviate that, but we need to hear more from the commenter. Once associated to a network the STA could get an ID, allowing it to do FTM with the APs in the network, with different MAC addresses per AP and the supplied Device ID. If you use secure PASN, the AP will know who you are anyway. I’m not going to promote this use case strongly, but I can come up with one example use for it.

C- This FTM is for location measurement. A device can figure out how far it is from APs and determine its exact location. I don’t see much need for that use case.

Q- Do you want to defend the use case or go back the commenter and see if we have to do it.

A- Can we put the CID on hold?

C- Short answer is that it’s up to the group. I’d like to determine this week that we go to a letter ballot. We could reject the comment and say we don’t understand its rationale.

C- I see the use case. Just because an AP has RSTA functionality enabled doesn’t mean it is used every time. Perhaps we can send email to the reflector.

C- I will take the action to contact the commenter and ask him to explain it to us, in person or on the reflector.

C- If the STA wants to know where it is, it can get the distances from each one if it knows where the APs are. We need this use case to be really defined. I’m not sure if we are helping the STA or the network.

C- It’s possible the network won’t provide the service until it knows who the STA is.

**Meeting recessed at 3:29 p.m. EST.**

**Meeting March 15th, 2023, 8:00 a.m. to 10:00 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 meeting was called to order by the Chair at 8:16 a.m. EST.**

Agenda slide deck [11-23/0180r04](https://mentor.ieee.org/802.11/dcn/23/11-23-0180-04-00bh-agenda-tgbh-2023-mar-plenary.pptx)

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

There were no Patent declarations.

Copyright policy slides were presented (Slides 11 and 12)

* **Agenda:**
* **Attendance, noises/recording, meeting protocol**
* **Policies, duty to inform, participation rules**
* **Organization topics:**
	+ March Interim meetings: Monday, 8:00-10:00 (pre-meeting); Tuesday, 13:30-15:30; Wednesday, 8:00-10:00; Thursday 8:00-10:00
* **Issues Tracking:** [11-21/0332r37](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* **Motions record:** [11-22/0651r13](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-13-00bh-tgbh-motions-list.pptx)
* **Results of Comment Collection on D0.2:** [11-22/0973r17](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-17-00bh-cc41-comments-against-d0-2.xlsx)
	+ Presentation/discussion on CIDs 19 & 20 (Okan Mutgan/Jonathon Segev) [11-22/1732r1](https://mentor.ieee.org/802.11/dcn/22/11-22-1732-01-00bh-resolution-for-cid19-and-cid20.pptx), [11-22/1806r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1806-00-00bh-cr-for-pasn.docx)
	+ Presentation/discussion on CIDs 5 and 62 (Mark Hamilton) [11-23/0461r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0461-00-00bh-cr-for-cids-5-and-62.docx)
	+ Presentation/discussion on CID 16 (Jay Yang) [11-23/0459r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0459-00-00bh-cr-for-cid16.docx)
	+ Updates on remaining assigned items
* **Motion on remaining CC resolutions (Motion 15(?), slide 26 of motions deck 11-22/0651r13)**
* **CAD document proposal:** [11-23/0430r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0430-00-00bh-tgbh-coexistence-assessment.docx)
* **Way forward to D1.0 (slide 22)**
* Presentation on IRM (Graham Smith): [11-23/0421r1](https://mentor.ieee.org/802.11/dcn/23/11-23-0421-01-00bh-irm-proposal.pptx)
* Presentation on “IE-based solution” (Okan Mutgan) [11-23/0441r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0441-00-00bh-ie-based-pre-association-identification.pptx)

Any comments? [None]

Any objections to agenda? [None] – Approved with unanimous consent

1. **Updates on CIDs 19 and 20**

With the TGaz chair (Jonathan Segev, Intel) present, Okan Mutgan (Nokia) presented [11-22/1732r01](https://mentor.ieee.org/802.11/dcn/22/11-22-1732-01-00bh-resolution-for-cid19-and-cid20.pptx) again. The hope is Segev can explain what’s needed from a TGaz perspective (or at least his own) in order to resolve these comments.

Segev explained the use of IEEE 802.11az, which is an expansion of the previous ranging/location services. IEEE 802.11az allows a device to locate itself or allow the network to locate a device. Ranging measurements are performed independently to each AP. Multiple measurements are needed to derive a location. IEEE 802.11az ranging does not require a STA association with any of the APs. PASN (Pre-Association Security Negotiation) allows the secure ranging services without, obviously, the need for an association.

Q- Is there an expectation that PASN is authenticated or are we talking the opportunistic encryption variant? The former would require there to be keys available for authentication.

A- Sometimes IEEE 802.1X is used with pre-existing trust between the STA and the AP/infrastructure, such as in an enterprise setup. Another option is a mechanism similar to open roaming. A third case is no authentication, but you want encryption so that the STA can’t be easily located by other STAs. Admittedly, with an antenna array, a STA can be located outside of FTM, but in this case we are just looking at protection from a traffic sniffer, not a direction finder. And protection from a false location reading due to inserted traffic.

C- This type of location measurement is privacy related and should be well controlled. Generally, many devices don’t want to share their location with the network, even if they are using the network. I think there are few devices that want to share their location with the network.

Q- As far as I remember, 11az is built on top of 11aq. Did you expect for the non-AP STA to maintain its MAC address for all of the APs in the ESS? What were your assumptions? What would the STA sacrifice in order to obtain location services?

A- 11az relies on the MAC address to identify the non-AP STA.

C- I don’t like that it’s necessary to use the unencrypted part of solution 3 (aka encrypted v2). I don’t think we need to update the Device ID between the set of ranging measurements. Just use the encrypted versions for every message in every direction. All that said, other pre-association use cases may have an impact here as well.

C- We use FTM extensively, so it’s not a minor use case from our perspective.

Q- Obviously, there are two scenarios. One is the STA wants to know where it is, but it doesn’t want the network to know. It that case it can use a different MAC address for each AP. The APs won’t realize one STA is talking to them. That one is covered automatically. But for solution 3, the network wants to know where the STA is. What does the STA need in terms of privacy. Why not just use the same MAC address. For a mobile device, where both the STA and AP want location information, then privacy might matter. The Authentication Message 2 is encrypted, right? (This is believed not to be the case.) You have to get an ID in the first place, without associating. You go to the first AP and get an ID. Then, when ranging with the other APs, you return an opaque ID to them, assuming the STA knows it has an opaque ID.

A- I agree there’s equipment not being associated with a person in an enterprise environment. But there is equipment that is associated with a person. There are cases where you want to know that you are indoors, but the AP doesn’t want to share more than that.

C- For the unencrypted version (solution 1), it’s pretty straightforward. This exposes the ID twice over the air. It’s assigned the first time the STA talks to the AP and then when the STA returns it to the AP. We could use two opaque IDs. The encrypted solutions require encryption of the payload (the device ID elements). It’s safer but more work. If we don’t want to change the PASN procedure too much and we want to use the existing PASN mechanism, then the two opaque ID generation would work here.

Q- But then both IDs are in the clear, right?

A- Yes. This is brainstorming.

C- I think there was a proposal to reuse a single Device ID for all of the FTM sessions for a single ranging measurement.

C- Yes, that’s what I was proposing. On slide 13 (encrypted v1), I don’t think there’s a need to provide a new value. Message 2 in the second auth doesn’t need to send another (encrypted) device ID. Also, we don’t have to encrypt the full frame in PASN. With a PTK, we can just encrypt fields in message 2 and message 3. We can easily add device ID encryption to these messages with a suitable key in place. That seems like the cleanest option. It doesn’t require any specific encryption design. Use the available key and the minimal change (encryption the IE being protected only). That’s it.

Q- You first propose to encryption device ID, meaning the authentication message ID needs to be encrypted. Then for the multiple FTM sessions, we use the same device ID. Since each authentication will have a different PTK, the encrypted device ID will be different.

A- Right.

Q- So we have now decided that part of message 2 is encrypted?

A- We are suggesting allowing encryption of parts of message 2.

Q- So the FTM procedure is itself encrypted. If we have an ESS and we use the same ID as you jump around the ESS, we’re happy to have the same ID used within the ESS. The FTM procedure is protected, so no one can locate the STA based on the device ID. How far do we want to go? We know there’s a STA in the ESS. The ESS is an FTM ESS. You don’t know what data is there. You know the STA is in the vicinity at the RF level. So, let’s have the same ID, for ranging, just like you use the same ID in an ESS. Why is it different here for any ESS?

A- Okay, it’s a new IE. We already have means for protecting IEs for FT or FILS. The encryption here could be the same. I think there’s something missing in the use case. This would prevent accurate measurement of the device. Third parties won’t know the device ID if the device is using RCM. More likely, when you go through the set of FTMs, use the random MAC address as protection against 3rd party correlation. Use the device ID so that the network can correlate the session. I think that’s a significant improvement for when the STA wants the network to track it.

C- So, encrypted v1, without Authentication message 2 is the proposal. But the 2nd auth might be done with a different RCM, so a new device ID is needed in message 2 until the AP realizes it’s really the same STA.

C- We would have to describe the use of an opaque ID here. In a realistic deployment, it’s not the first FTM AP that gives you the device ID. It’s the prior association with the ESS. I think message 2 would likely be wholly unnecessary.

Q- Does the group feel like this is a good direction for Okan to proceed in?

A- If this is the direction, I have text ready.

C- However, it’s been proposed to get rid of the opaque IDs and drop message 2 in the 2nd authentication. Your text would need modification to match that.

C- We can look at the text, which isn’t 100% ready in any case.

C- I’m confused. If we get rid of the opaque stuff, in the 1st authentication, the STA would have an opaque ID of ‘aaa’. It could put that in message 1 and get a re-encryption of its device ID in the second authentication. We don’t have to have new device IDs that we throw away. Perhaps I’m missing something.

C- That seems to be the encrypted v2 style.

C- In general, if the AP is assigning a device ID to the STA, we need to make sure that the STA only does PASN and not full associations. So, assigning IDs through PASN signaling doesn’t sound like something we should be addressing here.

C- In my suggestion, I’m not throwing out any device IDs and there’s an association. The association is used to configure the device with the device ID. That device ID is used in future PASN sessions without getting a new device ID. Only message 3 needs to provide the encrypted device ID from the prior association. Sure, the opaque ID could be used in message 1 without encryption, but you would still need to associate first to get the device ID and then use it. That seems unnecessarily complex. I think it would simpler to do the association first and convey device IDs in message 3 only. That’s good for PASN only, if we don’t deal with other pre-association use cases.

C- On the assumption that authentication is done in message 3, then it would be best for the STA to provide the device ID. It can do that in message 3 each time. It would be encrypted. That’s my suggestion. A STA-provided ID is the answer.

C- STA provided IDs tend to have an upper layer binding. That’s why I prefer AP assigned ID. I’m not against STA-generated IDs, but they do have multiple issues including unicity, etc.

Q- We have a couple of variants being proposed. Is there objection to heading in this direction? Or are we coming around to this being a use case we want to solve?

A- I have a slight feeling of support for this use case. But I don’t know where we will go with other pre-association use cases. If we do PASN only, then things are clear. But if we want to do both, then the direction is unclear.

C- Let’s not spend too much time on details – we’ve modifying things on the fly. Let’s catch up to that. Let’s focus on the general direction here and then get to the pre-association discussion and consider them together.

Q- We have the PMK set up between the STA and AP. Isn’t that enough to identify the STA? Adding a device ID here where we have to do an association first, isn’t that enough identification?

A- For some uses of PASN that’s true. The unauthenticated PASN case has no authentication and no binding to a past association.

Q- Then we are saving one-time association via a lot of complexity?

A- I don’t agree it’s particularly complex.

C- The proposal is for slide 13 or slide 15. Can we decide which way we want to go? I have text for both.

C- To be clear, we have changes to both designs. Those changes don’t match the slides and the ready text.

Q- Does the group want to set this aside for the moment and get to the rest of our pre-association discussion?

A- [No objection]

C- We’re getting closer, and we will come back to this.

1. **Presentation/discussion on CIDs 5 and 62**

Mark Hamilton presented [11-23/0461r00](https://mentor.ieee.org/802.11/dcn/23/11-23-0461-00-00bh-cr-for-cids-5-and-62.docx). CID 5 asks to define the MIB to save and obtain the identifier sent in EAPOL-Key messages 3/4. Saving is done locally on each side. CID 62 requests a simple PICS update, which is provided. For CID 5, an identifier is associated per SSID. So, the MIB needs a pair of tables, dot11DeviceIDTable and dot11APDeviceIDTable. The latter table is a bit simpler than the former.

C- I don’t think zero-length SSIDs are allowed. On the AP side, the assignment is going to happen from the network. We have to further consider opaque ID handling.

C- For the AP device ID table, I assume a separate SME on an AP that handles multiple SSIDs.

C- In the 802.11 world, that’s multiple APs.

Q- You have “SSID” here. Why?

A- I believe that was the agreement within the group. A STA has different IDs for different SSIDs.

Q- Aren’t you troubled that someone could spoof the SSID? That gets us to the question of whether clients want to have a better way of identifying a network. That sounds like an IEEE 802.11bi question.

A- I’m concerned about that and how much information is being stored here.

C- You already store the SSID and various security settings you’ve seen in the past. From a practical perspective, we’re just adding a device identifier.

C- In our MIB, we don’t store different profiles for different ESSes. We don’t need a table, we just need the dot11deviceIdentifier. That matches how we do security parameters.

C- I think you’re right. We’re not very explicit. We push a lot of stuff into the SME and hope it is managed outside of our scope. That can simplify the resolution. Probably put the device identifier in the station configuration.

Q- On the AP side, is the proposed text all right?

A- I’m tempted to say it is out of the scope side, due the network assigning things or vendors doing strange things. I would rather not define a MIB variable or table for that information.

C- That’s going in the direction of the AP having nothing and the STA only having a variable, not a table. That would greatly simplify things if it works.

C- We would have to have info for the current use cases that says where the device ID is coming from. I don’t think that’s there now. Are we not giving the upper layers a mechanism to push things down. For the KDE we have no method for pushing identifiers up and down.

C- Maybe we say it’s implementation dependent and out of scope of IEEE 802.11bh.

C- That’s related to our MLME-SAP discussion. This thing is a Supplicant authenticator. We could use MLME-ASSOCIATE.request (or one of those) to receive the device ID from FILS. For other cases, it is out of scope or needs another primitive.

C- It needs to be both way.

C- For KDE, I’m fine saying it is out of scope. For FILS we need to decide if we want to do it properly.

C- I thought we agreed yesterday to do it through the MLME.

C- I don’t want to reopen the question.

C- It was pointed out that the way things are done in dot11RSNAConfigPasswordValueTable might be the right way to do things.

1. **Presentation on CID 16**

Jay Yang presented [11-23/0459r00](https://mentor.ieee.org/802.11/dcn/23/11-23-0459-00-00bh-cr-for-cid16.docx) to resolve CID 16. That CID requests a new MLME-SAP primitive to allow the passing of the device ID to and from the upper layers. To that end, Yang proposes new MLME-DEVICEID primitives. He notes that his changes do clash with some other resolutions (see [11-22/1599r03](https://mentor.ieee.org/802.11/dcn/22/11-22-1599-03-00bh-revisions-to-rsn-extension-element.docx)), and he would like input. It’s not clear that there’s a real clash because 1599 is somewhat reproduced in this document. There might be a clash with [11-23/0452r01](https://mentor.ieee.org/802.11/dcn/23/11-23-0452-01-00bh-resolution-cid-32.docx). Yang will update his text. The group otherwise finds the resolution as suitable.

1. **CAD document proposal**

Hamilton has put together [11-23/0430r00](https://mentor.ieee.org/802.11/dcn/23/11-23-0430-00-00bh-tgbh-coexistence-assessment.docx) as the task group’s Coexistence Assessment Document, which will go out together with the first draft for ballot. The short take is that IEEE 802.11bh does not introduce any new coexistence concerns as it does not change PHYs or MAC operating procedures. With no objections from participants, Hamilton will check with the IEEE 802.11 chair to verify that it meets the new requirements for CADs.

Q- Is a CAD still needed for a MAC-level specification?

A- It seems to be for us based on our PAR, but ducking the requirement is probably more work than just submitting this simple document.

**The meeting was recessed at 10:00 a.m. EST.**

**Meeting March 16th, 2023, 8:00 a.m. to 10:00 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 meeting was called to order by the Chair at 8:03 a.m. EST.**

Agenda slide deck [11-23/0180r05](https://mentor.ieee.org/802.11/dcn/23/11-23-0180-05-00bh-agenda-tgbh-2023-mar-plenary.pptx)

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

There were no Patent declarations.

Copyright policy slides were presented (Slides 11 and 12)

1. **Agenda**
* **Attendance, noises/recording, meeting protocol**
* **Policies, duty to inform, participation rules**
* **Issues Tracking:** [**11-21/0332r37**](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-37-00bh-issues-tracking.docx)
* **Motions record:** [**11-22/0651r14**](https://mentor.ieee.org/802.11/dcn/22/11-22-0651-14-00bh-tgbh-motions-list.pptx)
* **Results of Comment Collection on D0.2:** [**11-22/0973r18**](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-18-00bh-cc41-comments-against-d0-2.xlsx)
	+ Presentation/discussion on CID 5 (Mark Hamilton) [11-23/0461r1](https://mentor.ieee.org/802.11/dcn/23/11-23-0461-01-00bh-cr-for-cids-5-and-62.docx)
	+ Presentation/discussion on CIDs 19 & 20 (Okan Mutgan) [11-22/1732r1](https://mentor.ieee.org/802.11/dcn/22/11-22-1732-01-00bh-resolution-for-cid19-and-cid20.pptx), [11-22/1806r0](https://mentor.ieee.org/802.11/dcn/22/11-22-1806-00-00bh-cr-for-pasn.docx) ??
	+ CID 35 (Amelia Andersdotter/Dan Harkins) ??
* **Motion on remaining CC resolutions (Motion 15(?), slide 26 of motions deck 11-22/0651r14)**
* **Way forward to D1.0 (slide 22)**
	+ Presentation on IRM (Graham Smith): [11-23/0421r1](https://mentor.ieee.org/802.11/dcn/23/11-23-0421-01-00bh-irm-proposal.pptx)
	+ Presentation on “IE-based solution” (Okan Mutgan) [11-23/0441r0](https://mentor.ieee.org/802.11/dcn/23/11-23-0441-00-00bh-ie-based-pre-association-identification.pptx)
* **Next meetings plan (slides 23, 24)**
* **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)

Any comments? [None]

Any objections to agenda? [None] – Approved with unanimous consent

1. **Presentation/discussion on CID**

Mark Hamilton presented the updated [11-23/ 0461r01](https://mentor.ieee.org/802.11/dcn/23/11-23-0461-01-00bh-cr-for-cids-5-and-62.docx) based on yesterday’s discussion. The group did not object to the update being used as the resolution to CID 5.

1. **Presentation/discussion on CIDs 19 & 20**

Okan Mutgan spoke with a PASN expert and was told that encrypting an IE in Authentication message 2 is not reasonable because the AP does not know which cipher suite the STA will select.

C- I thought we had a solution for IE encryption.

C- We ended up with a plan yesterday that we didn’t need to use the Annex Z obfuscation, but with this new information, we need to reopen that discussion.

C- I don’t think we need to change the device ID in any of these PASN exchanges. I also don’t think that nothing can be encrypted in message 2. I disagree with that so-called new information.

C- It sounds like we need some more offline discussion to get all the right people together at once.

C- I’m confident in my statement above.

C- Let’s table the discussion for now and look at pre-association matters.

Q- Having device ID in message 2 sounds like an alternative to the normal association with the device ID shared in the 4-way handshake. I don’t see a need for sending a device ID in message 2 and prefer to do it in 4-way handshake. Is there a gap analysis on PASN signaling?

A- What gaps do you mean?

C- Where you use device ID with PASN, what’s the use case for putting the device ID in PASN. Networks could use the PMK for device ID processing.

A- The use case is described pretty well. It’s for secure ranging where the network wants to locate a specific device (asset tracking). The desire was there not to expose the device location to 3rd parties. That’s the only use case for that. No association is needed. To hide from 3rd parties, you need to be able to change your MAC address between FTM sessions, while using the device ID for the network to correlate the FTM requests. As for the PMKSA, in PASN, you can use an existing PMKSA, like from EAPOL or SAE. If you have such a PMK produced by device credentials, then you wouldn’t need device ID. But SAE with shared credentials or PASN without authentication, you have no suitable PMK and would need a device ID. Without access to a device-specific, previously generated PMK, and a desire to hide from 3rd parties, then you would need device ID in PASN.

C- You’re providing authenticating and location. User consent is needed here. We might have device ID for the infrastructure case while not agreeing to use it for PASN. That complicates things. There are networks in general that will use device ID but giving your exact location to such a network is unlikely.

C- We’ll table this discussion for now but thank you everyone.

1. **CID 35**

Dan Harkins (HPE) has supplied (via email) some text to resolve CID 35. Mark Hamilton showed the email on the screen. The text reads:

An opaque identifier can optionally be constructed by the network using the procedure in Annex Z or can employ a different mechanism provided it affords comparable security and privacy.

C- We have not defined specifically what’s included in the IE and KDE for Annex Z operations. It’s not clear whether the device ID is the input or output for Annex Z. We just need to spell it out. I’m sure we can work it out.

C- Annex Z has not been changed so far.

C- We decided that what the AP gives to the STA is Device ID.

C- Gives is too vague a word.

C- The field that in the IE and KDE is the Device ID. That’s decided. Yesterday’s discussion was that the opaque ID could be in a field in certain cases.

C- I don’t agree that we decided that detail. It could be okay, but it we need to specify clearly when the device ID field carries an opaque ID. What was described means that opaque ID is the output of Annex Z. There’s consensus here, so I’m not going to continue this discussion.

C- We don’t have consensus or detailed wording. If anyone can work on this offline in the next hour, that would be handy.

C- I couldn’t care less about the naming, but for Draft 1.0, we need to have sufficient precision about terms, although we can clean them up. I don’t believe we will be able to pick something easily.

1. **Presentation on IRM**

Q- Can we carry over CRs to the next ballot?

A- This was a comment collection with little formalism to the resolution process, so we can carry them over or indicate that they should be raised again later.

Graham Smith (SRT) showed [11-23/0421r01](https://mentor.ieee.org/802.11/dcn/23/11-23-0421-01-00bh-irm-proposal.pptx) on “Proposed Text for IRM”. He’s raising the topic again based on recent voting, discussion on the reflector, and some support expressed. This is not a presentation about how IRM works. It’s an advocacy for not abandoning this type of mechanism. Smith said that the default mechanism is “Same MAC Address” (SMA) – reuse the same MAC address when returning to a network. The problem is that copying that address is simple, which may defeat our privacy requirement. One step up from SMA is IRM (Identifiable Random MAC), in which the STA controls the address presented and sends a new one (via an ID) to the AP each time it associates for use in the subsequent association. This scheme is complementary to Device ID and meets all use cases. The device ID can be fixed, but the IRM ID must change per association. The two IDs should be kept separate by the STA and not further confused.

C- I’m not a fan, but I’m not unwilling to see this in the draft in order to make progress and then clean things up during balloting.

1. **“IE-based solution”**

Jay Yang (Nokia) and Okan Mutgan (Nokia) presented their STA-generated ID solution ([11-23/0441r00](https://mentor.ieee.org/802.11/dcn/23/11-23-0441-00-00bh-ie-based-pre-association-identification.pptx)). Mutgan noted the straw poll during the Bangkok mechanism that showed strong support for working on pre-association identification. For pre-association identification, the (protected) device ID can be supplied in an IE. Two MIB variables (dot11PostAssocDeviceIDActivated and dot11PreAssocDeviceIDActivated) can be used to signal how the device ID is being used. The proposal offers two schemes, one simple, one more complete. The simple one has the STA and AP deriving a pairwise key from the PTK. Both sides then generate two blobs based on that pairwise key, which are installed locally with the key. Upon return, a STA sends the first blob in the identification IE for pre-association things like directed probes. The AP returns that blob in the IE of the response as an acknowledgement. The STA follows that by generating a third blob and disposing of the first one. Then, the STA sends the second blob while associating. This is acknowledged in the response with the STA then generating a fourth blob while deleting the second one. The more complex solution is shown on slide 11 and adds MIC and PN fields for, respectively, authentication/validation and replay protection.

Q- The way you use pairwise keys between the STA and the AP is problematic because we want the STA to be able to use the device ID with all the APs in an ESS. How does the pairwise key get shared among all of the APs? Otherwise, the STA will have to maintain state per AP in the ESS, which could be a lot of storage.

A- The current Device ID is ESS level. The pairwise key here could also be stored per ESS, with the first AP sharing the key with the other ESS APs.

C- In that case, I wouldn’t consider this a pairwise key, but I would be concerned about the network-side complexity, requiring a full switch design or synchronization amongst all of the APs.

C- This is like the PMK cache, shared between all APs.

C- That’s not correct.

C- We need an offline discussion on that.

Q- I share the concern about the pairwise key in the ESS. I like the idea in general. Could we design an FT (Fast Roaming Transition, IEEE 802.11r) mode that does a pairwise key with an AP and then when you move to a different AP, you pass the blob over to the new AP?

A- As far as the key is concerned, I just don’t like the name. I’m sure we can figure out how to do the key nicely. The FT part, I have no issues with, but the blob is concerning. It works between two entities. But the need to synchronize with multiple APs, that needs more thinking. While I like the idea of always changing easily derivable things, without a sequence number, I could see a problem. I don’t want to solve these problems right in this meeting. We should have an offline discussion.

C- Maybe we can try to build on the proposal and figure out moving between AP scenarios?

Q- Especially for the ranging use cases, can all of the APs remain synchronized that quickly?

A- For the key part, I’m sure we can think about something. In Annex Z, there’s a key 2 that’s assumed to be shared in the ESS. Maybe this proposal shouldn’t have a pairwise key, but should have one that is shared across the AP. The key isn’t the big concern. The generation of blobs or not is the question before the group. This looks a bit like an Annex Z solution, sort of protecting the Device ID, but with dynamic generation. From an Annex Z point of view, the STA and AP should use it for blob generation. For the synchronization, with dynamic generation, there may be a problem. Since the blobs are sent in pre-association management frames, we can add a status code to note synchronization issues.

C- There’s a significant difference with the AP-side generation and the blob generation here. Completely different scales of complexity. I like this kind of dynamic approach as it has good security properties and I prefer it to IRM, but I don’t know that it’s practically implementable in real-world AP designs. We don’t have a lot of time to address the technicalities here, but maybe we should move to the high-level question of whether we want to use an IE-type design.

C- In general, we have Draft 0.2, which provides a protocol for device identification. I don’t see value in the pre-association use cases. They can allow bad steering. We have tools for steering. I think the pre-association use cases might damage the Wi-Fi ecosystem. We’ve had motions on all of the proposals before and they have all failed. Let’s move to letter ballot on Draft 0.2 instead of continuing to flog pre-association use cases.

C- There are a lot of pre-association identification use cases that have been discussed. I’d like to see them addressed. I don’t care which proposal ends up being adopted, but I want to meet Wi-Fi industry requirements.

1. **Way forward**

Mark Hamilton indicated that Graham Smith’s text is more mature, but the IE-based solution looks like it has interesting properties. We could just vote on what’s in Draft 0.2. We’ve been going in circles for quite some time. He’d like to see us get to a letter ballot soon. Hamilton has a new version of the comment resolution spreadsheet update ([11-22/0973r19](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-19-00bh-cc41-comments-against-d0-2.xlsx)) . We could reject the comments advocating a pre-association solution because we could not arrive at consensus on a solution.

C- We should move to letter ballot. We haven’t agreed on anything to add to Draft 0.2. If we do go to letter ballot, then those with contributions on things they want to add to the draft can raise them. Then we can address those things during letter ballot comment resolution. I want us to press forward in the remaining time to get agreement on the letter ballot. Otherwise, we will be in the same situation in May.

C- I’ll point out that there’s suggested resolution text for CIDs 19, 20, and 65 in the comment resolution spreadsheet.

C- I agree with the proposal to move to a letter ballot. My crystal ball says that when we go to a Draft 1.0 letter ballot, we will get the same proposals for pre-association use cases and perhaps some fresh comments. Let’s do something else than rehashing the same old thing.

C- If we agree to go with post-association Device ID then there’s no way to add new features for pre-association use cases.

C- The problem is that if you go to Draft 1.0, you’re expected to be feature complete. Given what TGbh was meant to do (as expressed in the PAR), if we don’t want to cover everything and we want to ignore elements of the PAR and the WBA’s request, then we need to change the PAR before going to Draft 1.0. Otherwise, we will get comments about not meeting the PAR. So, we might be longer fixing Draft 1.0 then a Draft 0.3. If we feel that a solution to what was asked of us by the market is Device ID only and that’s worth putting into the market, fine. But let’s not pretend that meets the PAR. Let’s vote to amend the PAR or agree that we have go back and get a pre-association solution. We can’t have both. I’d be embarrassed if Draft 0.2 was our answer to the WBA after 2.5 years. I’m torn. I don’t know how to go forward with this.

C- We should remember why we are here. TGbh was supposed to be a short exercise. We’ve been slipping 10 months on the timeline. This is not a short process. TGbe is generating MLD addresses that will be used in authentication/association. TGbi is dealing with the privacy. We are not leading the charge. IEEE 802.11 is moving beyond IEEE 802.11bh, with TGbh only dealing with legacy networks. In order to close down this effort, we should move onward for Draft 1.0.

C- Personally, I’m okay with either approach, and that we will get comments on the letter ballot. As for the PAR, we can argue over the scope. Sure, we have industry use cases. We can say ‘no’ to some of those. I’m getting to the point that time is not on our side and that we are becoming irrelevant. I’d like to get a ballot with or without pre-association use cases. I’d like them there, but I want to get to that ballot too.

C- Regarding the PAR, if we go to letter ballot, that’s purely internal to IEEE 802.11. The question is “is this draft ready for SA ballot?” So, we won’t be in trouble if we don’t meet the PAR yet. We have time to align the draft and the PAR before the SA ballot. Let’s move to letter ballot if we believe that’s the right move regardless of the PAR. Sure, we will see the comments again. Hopefully, we’ve had time to mature and figure out how to respond.

C- We’ve spent two years and only arrived at Device ID. Once the STA associates with the AP, in a lot of use cases, an L3 or higher identification will be used for the device. So, I don’t think Device ID is all that helpful. That’s why I want TGbh to focus on pre-association use cases. Those are the true market requirements. We spent too much time on post-association and Device ID.

C- We’ve been discussing these other schemes a long time ago. IRM was 18 months ago. Other schemes came in and muddied the waters. The text is there, and we could put it. If the group wants to push forward with a Draft 1.0, we might be stuck in comment resolution for a long time if we use Draft 0.2 as the basis for Draft 1.0. I think the group has missed an opportunity and is rushing to ballot.

Q- If we reject some CIDs, they can be resubmitted for the first draft?

A- Yes.

Q- Do we need to address all of the CIDs to get to Draft 1.0?

A- This was a comment collection, so we are free to address them how we see fit. Or not. We’ve not reached consensus yet. We can respond to comments noting that lack of consensus on a resolution. It’s not like we are going to a letter ballot without discussing the comments. We just didn’t reach consensus. I’d like to, but there’s no hard requirement to do so.

C- I’ve observed this discussion about Draft 1.0 with quite some interest. I see the arguments on both sides. I’m afraid that going to Draft 1.0 just means we are throwing the issue to someone else to resolve. I think the same comments will just come back. I see a risk that the workload on many members will cause them to vote in favor instead of really addressing issues. What kind of message would that be? We have a long story of abstaining for lack of technical expertise, which many will refuse to select. Thus, we might get a high approval rate that isn’t real. The discussion will then be drawn out. We need a clean version of the draft and not hope for others to resolve the controversy.

C- I will point out that it’s standard practice to in IEEE 802.11 that getting 75% means we are done. The TG and WG choose when we go to SA ballot.

C- Yes, we aim for higher confidence before an SA ballot. But it would beg the question as to what kind of message is being sent by a 75% vote. We put drafts for sale when they hit 75%. It seems weird that we say we can’t agree on our own issues and ask others to do so.

C- On the other hand, I understand the public perception concern. Allowing other organizations to look at our draft might give us useful input. I wouldn’t say that was letting others solve our problems. The input might be helpful to solving the problems.

C- I’m in favor interoperability. I’m not looking for optional protocols to be included. I’d like to see a clear path to MLO, which is the next big thing in Wi-Fi.

C- I’d like to suggest we get a motion to go forward with the draft as we currently have it without adding anything that doesn’t have real consensus. I’d like to see what we can do with that path. We clean up the detail CIDs that we have and then get feedback from other organizations.

**Motion**: Move to approve the resolutions to the “Way forward?” CIDs in [11-22/0973r19](https://mentor.ieee.org/802.11/dcn/22/11-22-0973-19-00bh-cc41-comments-against-d0-2.xlsx), as Rejected. “TGbh discussed at least 8 unique proposals for such a mechanism, across almost a year of teleconferences and sessions, and could not come to consensus on a proposal that provided such a solution. (See minutes and agenda decks for recent TGbh calls/meetings for details.) Points of debate remain on whether to use a MAC address-based method or an IE-based method, how much security /privacy is required or provided by the proposals, how much computation or storage is required, and exactly which use cases are or are not addressed by each proposal.”

Moved by Stephen McCann, seconded by Kurt Lumbatis. Vote 17/6/5 (Y/N/A). Motion failed for lack of a 75% majority. Voting results are found in the table at the end of the minutes.

C- In the next meeting, can we have only two slots with TGbh so that we are more prepared and not getting new, on-the-fly proposals. We can use the first one to discuss if there’s consensus on the comments, and the second for the ballot process and way forward. No more fooling around. I think this is a waste of time.

C- I hope we can resolve the remaining items before the May meeting. I strongly suggest we continue the conference calls. We can even run motions with prior notification. That would allow us to formalize consensus during the May meeting.

C- I will plan for every Tuesday conference calls when there aren’t major holidays in conflict.

C- I will point out that we had a lot meetings, only one hour was spent looking at additions. If you go back, you’ll see presentations covering each of the scheme and how it dealt with everything.

Q- What do people think of 4 meeting slots in May? I’ve heard the one suggestion for 2 slots.

A- I’m not against more sessions. If we don’t use them, that’s fine. We should have more space to talk.

A- I like 4.

A- I don’t think we need more than two teleconferences or two meeting slots.

C- I’ll think about all of that and get things scheduled. Anything else for this week?

**Meeting adjourned at 10:01 a.m.**

**Motion voting results:**

**-------------------------------------------------**

 **[V] Stephen Orr, Cisco | X | | |**

 **[V] Kurt Lumbatis, ARRIS/CommScope | X | | |**

 **[V] Massinissa Lalam, Sagemcom | X | | |**

 **[V] Peter Yee, NSA-CSD | | | X |**

 **[V] Okan Mutgan Nokia | | X | |**

 **[V] Graham Smith SRT Wireless | | X | |**

 **[V] Hitoshi Morioka, SRC Software | | | X |**

 **[V] Jarkko Kneckt, Apple | X | | |**

 **[V] Jerome Henry, Cisco | X | | |**

 **Yong Liu | X | | |**

 **[V] Stephen McCann, Huawei | X | | |**

 **Reza Hedayat | X | | |**

 **[V] Alexander Krebs, Apple | X | | |**

 **[V] Jim Petranovich [Viasat] | X | | |**

 **[V] Guido R. Hiertz, Ericsson GmbH | | X | |**

 **[V] Max Riegel - Nokia | | X | |**

 **[V] Carol Ansley Cox | X | | |**

 **[V] Antonio de la Oliva | X | | |**

 **[V]Jay Yang Nokia | | X | |**

 **[V] Stephane Baron Canon | X | | |**

 **[V] Jouni Malinen Qualcomm | X | | |**

 **[V] Patrice NEZOU, Canon | X | | |**

 **[V] Darshak Thakore - CableLabs | X | | |**

 **[V] Julien SEVIN Canon | | | X |**

 **[V] Yuki FUJIMORI Canon | | | X |**

 **Peng Yan - Wi-Fi Alliance | | | X |**

 **[V] Dan Harkins | | X | |**