Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Meeting Minutes, October 25, 2022Randomized and Changing MAC addresses (RCM) |
| Date: 2022-10-25 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Peter Yee | NSA-CSD | Mountain View, CA |  | peter@akayla.com |

Abstract

This document contains the minutes of the IEEE 802.11bh telecon meeting of October 25, 2022.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting October 25, 2022 9:30 a.m. to 11:30 a.m. ET**

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

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

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

**Secretary: Peter Yee**

**Editor: Carol Ansley (Cox)**

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

Agenda slide deck [11-22/1805r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1805-00-00bh-agenda-tgbh-2022-oct-25.pptx)

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

There were no patent declarations. The copy policy slides were presented (slides 10 and 11).

1. **Agenda**
* **Attendance, noises/recording, meeting protocol reminders**
* **Policies, duty to inform, participation rules**
* **Organization topics (see Backup slides)**
	+ Sept to Nov teleconferences: Tuesdays, every other week, 9:30-11:30 am ET (this time slot)
	+ Timeline reminder (slide 20)
* **Issues Tracking: 11-21/0332r37**
* **Results of Comment Collection on D0.2: 11-22/0973r12**
* **Continue discussion on resolutions of ones that are NOT on topics: Opt-in, Pre/un-association, Non-AP STA-generated ID**
	+ 11-22/1665r0 – Device ID renaming discussion (Antonio de la Oliva)
	+ 11-22/1599r3 – Revisions to RSN Extension element (Kurt Lumbatis) (ready for motion?)
	+ 11-22/1329r6 – CID resolutions for 12.2.11 (Kurt Lumbatis) (pending discussion on 11-22/1218)
	+ 11-22/1588r0 – Resolution comment 32 (Antonio de la Oliva)
	+ Walk-through CIDs status
	+ ~1 hour
* **Contributions on topics: Opt-in, Pre/un-associated, Non-AP STA-generated ID (slide 16)**
	+ ~1 hour
* **WBA liaison response**

Any comments?

C- No need for presentation of [11-22/1218r05](https://mentor.ieee.org/802.11/dcn/22/11-22-1218-05-00bh-device-id-synchronizatoin-and-control.pptx) or [11-22/1620r03](https://mentor.ieee.org/802.11/dcn/22/11-22-1620-03-00bh-device-id-ladder-diagram.pptx).

Q- For the presentations on slide 16, which one of Graham Smith’s make sense to present?

A- [11-22/1650r04](https://mentor.ieee.org/802.11/dcn/22/11-22-1650-04-00bh-discussion-on-maad-and-all-that-goes-with-it.pptx) makes sense as a precursor to the motions in [11-22/1584r02](https://mentor.ieee.org/802.11/dcn/22/11-22-1584-02-00bh-more-than-one-scheme.pptx). 1650 deals with all of the pre-authentication systems, but it might take a long time.

C- With Antonio de la Oliva needing to leave the meeting early, let’s put one of his presentations first.

Any objections to agenda? [None]

Agenda approved by unanimous consent.

1. **Device ID renaming discussion**

Antonio de la Oliva (InterDigital, UC3M) presented [11-22/1665r00](https://mentor.ieee.org/802.11/dcn/22/11-22-1665-00-00bh-deviceid-renaming-discussion.pptx). This is a proposal for changing the term “Device ID” to something else. Perhaps Persistent Opaque Identifier, Persistent Identifier, or maybe both, depending on the context.

Q- I think the only time the Device ID is put in the Association Request and Response is for FILS. Not for the non-FILS case. Or as was pointed out, it’s also used that way for SAE for authentication.

A- True, but not really important for the discussion on the slide 3.

Q- What do you mean by opaque? Encrypted?

A- I mean opaque can be achieved by encrypting. The key point is that someone intercepts the message doesn’t know what the Device ID means.

The Device ID is obtained from someone/something. The initial Device ID is termed DeviceID1 and is sent as part of the Association Request. DeviceID2 is given back to the non-AP STA as part of the Association Confirm.

Q- Are you talking about the opaque that Dan Harkins put into the document?

A- Any algorithm. It’s just not cleartext.

Q- I’m struggling with the opaque definition. People seem to be dwelling on the fact that it is encrypted in some way. In my view, it’s meaningless outside of the two parties. Anyone else can’t understand it. It doesn’t matter that it is encrypted or not. It’s opaque. Not secure.

A- We need something more than just opaque. It has to be resistant to replay attacks, not just incomprehensible to others.

Q- Should we have a discussion of the definition of opaque?

A- I can move forward.

Q- Are you going to sort that out?

A- Not really.

C- Opaque means the message passed between the STA and AP is untrackable by a third party. Something has been done to the ID so that it is only meaningful to the two parties, not a third party. It’s an out-of-band establishment of a credential, like a password. Whatever that technique is, the network is going to take that identity (see the Annex) and wrap it in a secret that is only known to the network and returns it to the device. The device knows his identity, but the value he gets back from the AP is an opaque blob. That will be passed back to the AP when needed. It’s a wrapped, opaque blob. When it arrives at the AP, the SME gets it, it can unwrap and know what to do with the identity. And I’m going to re-encrypt the identity with a new key and send it back the device to prevent tracking. The non-AP STA will then have a new, unique identifier to use next time.

Q- Let me see if I understand. The “something” in slide 5 creates an opaque identifier that is sent in the Associate Request. And it receives a new Device ID2 on the Confirmation.

A- Yes. The AP’s “something” understands the blob and knows the underlying identity of the non-AP STA. It can then send the non-AP STA a new opaque blob by which it will be known.

C- If that’s the case, then we don’t need an algorithm to make the Device ID opaque. It just is opaque.

C- The mechanism above is described in the annex, which is \*a\* way of making an opaque blob. It isn’t the only way this could be done.

Q- Is that correct?

A- Yes, the annex describes what the right hand “something” block in slide 5 does. If you don’t do what’s in the annex, you have to do something else that makes the Device ID passed in the Association to be untrackable.

C- Our challenge is to enumerate what the requirements if not using the annex’s mechanism.

C- The annex describes them explicitly. We could move them to a “Security Considerations” section.

Q- Isn’t what the annex describes out of scope?

A- No, it’s a way of satisfying the requirements of the lines in the center of slide 5. There are requirements on the Device ID for privacy and untrackability. It’s how the SME ensures that the Device ID is opaque when passed in the Association Request and Association Response.

Q- So you are saying that the feature that provides opaqueness to the identity is the SME.

A- Yes.

Q- In the fast mode, the Device ID is already encrypted. I think we could say it’s opaque and that’s enough, right?

A- You are saying that encryption is enough to make it opaque. But that’s not everyone’s point of view.

C- We can decide to use the annex or not. From the specification, we should be more flexible.

C- It seems like we are circling around what is meant by opaque. I suggest we stop talking about the definition. It’s just muddying the waters. It’s just a question of when the Device ID is being passed. I see a comment that says opaque means not trackable to a third party. You could say that the current RCM is non-trackable since the device comes up with a new RCM each time it associates. Would we call that opaque? Is it using opaque IDs. Opaque means that the ID has no meaning, it’s just something passed.

C- I agree that everything that is passed through encryption is opaque. But is the Device ID opaque without encryption? Or does it have to be encrypted to be opaque.

Q- If you take the current RCM, is the RCM opaque? Is the Device ID the thing that makes it opaque?

C- We haven’t discussed that the Device ID has some persistence and meaning to the two ends that they understand, but others do not.

C- That’s why in the presentation, the left “something” that sends Device ID1 is sending something that is unknown to third parties.

C- I suggest we first look at how the identifier is used. The mechanism to give it the required properties is separate. The annex is just one way to do it.

Q- I think we all understand the current RCM. I’m trying to get that into here. The device that doesn’t want to be tracked, how is that secret being kept?

Q- Is it sufficient that this thing identifies a shared context between the AP and STA that cannot be tracked by a third party?

A- I think that’s what it is and what it does. We are trying to find a name for that.

C- I think we are muddying the waters by naming the Device ID.

C- RCM is muddying the waters because it is orthogonal. The identity agreed upon by both sides is used with the assumption that RCM is there, but RCM is not used for identification.

C- This is totally confusing. Looking at slide 5, the top Device ID (DeviceID1) is sent. Coming back is DeviceID2 which, even if it is opaque, can be copied and searched for in a future connection. I don’t think that’s what the annex means. I don’t know why they should be in the clear. If they are encrypted, than the Device ID won’t be trackable because they will look different between the Association Confirm and the subsequent Association Request. I don’t see why it should even be in the Association Request since it will be in the 4-way handshake (where it will be encrypted). When would a non-AP STA want to send it in the clear? That’s what I’m saying.

C- This diagram isn’t trying to discuss that. It’s trying to discuss the relationship of the Device IDs and that they are opaque.

C- My point is that the opaqueness quality of the identifier doesn’t matter.

C- If this FILS, as was pointed out, then the Device ID is encrypted and will not be trackable since each association will use different keys to encrypt it. Initial state is a question in my mind, however.

C- This diagram is assuming the support for pre-association discovery requirements. Otherwise, you would exchange the Device ID later in the protocol sequence.

C- I would change the title of this slide to “FILS Device ID”.

C- Let’s stop talking about mechanism (again).

Q- Is it an indicator that’s kept secret that the device uses to identify itself to the AP?

A- We are going in circles. We should agree that the Device ID has a meaning and for whom.

C- It should be between the blue boxes [on slide 5].

C- It’s pointed out that the blue boxes are part of the SME.

C- No, they are an application.

C- Well, some use cases are at layer 2, so you probably need a layer 2 entity in the definition of “something”.

Q- Which use cases?

A- Some access mechanism ones and some troubleshooting ones.

C- I understood that an enrollment was required for those use cases. So, the device ID may have a meaning for applications, and it may have an internal meaning.

C- That’s my understanding from the issues tracking document. Layer 2 use cases are likely to remain in our scope.

C- Even for troubleshooting, you need to know the ID of the device. So, that’s like an application. So, the meaning is not internal.

C- Based on the discussion we have had, I’d like to take us back a little bit. We are talking at cross purposes here. The level of opaqueness and trackability seems to vary amongst participants. We are trying to put in some ID to allow the level of privacy obtained from RCM to be used consistently by IEEE 802.11 devices while allowing the blue boxes to understand the common meaning of the device ID. Whether that’s encrypted or not, that’s the basic requirement. I think we need to know at each point in this process whether what we are calling the device ID is encrypted on its own or it is in an encrypted message (so that it is a shared secret between the two blue boxes) or if it is a random number but both blue boxes know what the random number means. I think we can allow for multiple views of this in our standard and we can allow for multiple levels of tracking protection. The question if we will stay within the bounds of our PAR to be at the protection level of RCM or will be go beyond that because we can. Some of us want to move to a next level, but I’m not sure that’s in our scope. We might be able to do that as long as we address the basics. I think we are only talking about RCM-level of blob protection.

C- I think our PAR was written to be “solve the problems that RCM created”.

C- I understood the PAR to mean that RCM broke the ability of the two blue boxes to identify each other and we are trying to provide a fix so that the blue boxes recognize each other, allowing the ID to have meaning, hopefully to just the two blue boxes.

C- Let me build on that, my view is that I agree with that comment. Before there was RCM, the two blue boxes (regardless of where they are) had some persistent understanding of each other’s identity and could be used across associations. RCM took that away. We are trying to allow the two parties to have that understanding again, but in a manner that cannot be tracked by third parties. The two blue boxes just want to recognize each other and then have the appropriate context. I believe some of that context is layer 2. Some of it may be at upper layers, which is nice to have. It’s the layer 2 stuff that is within our scope.

C- Through discussion, my last proposal on the last slide will have the blue boxes as the final consumer of the identity. What goes between the SMEs will be the opaque identifier. The blue boxes could be SMEs. The presentation needs to be updated by use case to show what is opaque and what is not.

C- To show that what goes over the air is opaque.

C- Yes.

1. **Revisions to RSN Extension element (Kurt Lumbatis, ARRIS/CommScope)**

Please review the latest text as it is believed ready for motion. And then read 1329r06 for a deeper conversation.

1. **Discussion on MAAD and all that goes with it (Graham Smith, SRT)**

Smith presented [11-22/1650r04](https://mentor.ieee.org/802.11/dcn/22/11-22-1650-04-00bh-discussion-on-maad-and-all-that-goes-with-it.pptx). Nothing here is new. It’s been presented before. But it depends on whether you turned up during the right teleconferences. But I get the same negative comments before I open my mouth about pre-association schemes. I think those schemes can be reasonably allowed. I will address the objections to them. This presentation is a lead-in the motions in [11-22/1584r02](https://mentor.ieee.org/802.11/dcn/22/11-22-1584-02-00bh-more-than-one-scheme.pptx). I’ll describe MAAD and how it co-exists with Device ID. I think MAAD is simple, secure, and an apt solution for TGbh. [Smith ran through how MAAD works, on slide 5.] MAAD has two MAC addresses, one used for associations, the other for probes when the STA wants to be identified. These two addresses are changed every time the STA associates. The MAC addresses are protected in the 4-way handshake or FILS. MAAD co-exists with Device ID. The AP makes that decision to use one, the other, or both. No selection mechanism is required. For probes, generally a random MAC address (RMA) is used. If the STA wants to be identified, it can use the second MAC address. That’s when the STA is in the vicinity of an SSID that it wants to identify the STA. Active Directed Probes are discouraged, because that advertises interest to spoofing APs. If you are looking for a specific AP or network, just use broadcast probes. The identifiable TA MAC value can be used in the vicinity of a known AP for steering purposes. If you probe and then associate that way, two different addresses are used, and those addresses will be changed during the association for use in future associations and/or probing. The same TA must be used across the ESS. All pre-association schemes (“pre-schemes”) use one-time addresses, so there is no trackability. Spoofing APs aren’t solved by RCMs – the attempt to associate declares interest in that network and means the associating STA knows the real AP that is being spoofed. The only protection is that the STA has to know that the AP is the real deal before attempting to associate. This knowledge can be obtained by 1) GPS (not an IEEE 802.11 solution, however), 2) SSID profile – profile the real AP and then compare that with what the spoofed AP is transmitting and the local environment, 3) identifiable beacon (using a beacon protection key), and 4) allocated MAC address ID, and wildcard probe (this is a new proposal). That last point requires the allocation of two addresses and a random ID. The random ID is known to the STA and the real AP. The real AP can send a probe response with the correct ID. If the STA gets a bogus ID, it knows the AP is a spoofer and doesn’t associate. The AP uses a random ID value in every probe response, only using the real ID value if it recognizes the STA’s probe address. Overall, this defeats the spoofing AP problem, which even RCM didn’t help. Cloned STA addresses don’t seem to be a problem in this scheme, because the cloner doesn’t have the key to the SSID. Basically, there aren’t privacy problems with the pre-schemes (pre-association steering, home control, steering/configuration). IRM and RRCM could also use the ideas in this presentation. For a nonce-using scheme, IRMA can be used.

[11-22/1584r02](https://mentor.ieee.org/802.11/dcn/22/11-22-1584-02-00bh-more-than-one-scheme.pptx) asks a bunch of questions to gauge the group’s interest in the proposals given above.

Q- I think the pre-schemes will have to be handled at layer 2, not passed up the layers. How much additional memory do you think this require?

A- No more than is currently used. Pre-RCM, the AP had to remember all the MAC addresses it cared about for pre-association use cases. There’s no higher complexity introduced by these schemes.

Q- Is there sufficient interest in having Graham bring this up at a face-to-face meeting as motions?

Q- We have several different schemes. Will we consider all of them or focus on the most palatable to the group? Should we take a straw poll?

A- That’s what [11-22/1584r02](https://mentor.ieee.org/802.11/dcn/22/11-22-1584-02-00bh-more-than-one-scheme.pptx) is attempting to do. All of the pre-schemes have been changed from their previous versions.

Chair- We will plan to discuss this at the next face-to-face meeting unless someone wants to talk about it during the next call. We will then move on to unaddressed presentations during the next call.

1. **WBA liaison response**

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

**Meeting adjoined at 11:27 a.m. EDT.**

**Attendance**

|  |  |  |  |
| --- | --- | --- | --- |
| Breakout | Timestamp | Name | Affiliation |
| TGbh | 10/25 | Ansley, Carol | Cox |
| TGbh | 10/25 | De la Oliva, Antonio | InterDigital, UC3M |
| TGbh | 10/25 | Hamilton, Mark | Ruckus/CommScope |
| TGbh | 10/25 | Harkins, Dan | HPE |
| TGbh | 10/25 | Kneckt, Jarkko | Apple |
| TGbh | 10/25 | Levy, Joseph | InterDigital |
| TGbh | 10/25 | Lumbatis, Kurt | ARRIS/CommScope, Inc. |
| TGbh | 10/25 | Mutgan, Okan | Nokia |
| TGbh | 10/25 | Orr, Stephen | Cisco |
| TGbh | 10/25 | Petrick, Al | InterDigital |
| TGbh | 10/25 | Riegel, Max | Nokia |
| TGbh | 10/25 | Sam, Harvey | Broadcom Corporation |
| TGbh | 10/25 | Sevin, Julien | Canon |
| TGbh | 10/25 | Smith, Graham | SRT |
| TGbh | 10/25 | Smith, Luther | CableLabs |
| TGbh | 10/25 | Thakur, Sidharth | Apple |
| TGbh | 10/25 | Yang, Jay | Nokia |
| TGbh | 10/25 | Yee, Peter | NSA-CSD |