Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Meeting Minutes, Interim January, 2022Randomized and Changing MAC addresses (RCM) |
| Date: 2022-01-21 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Graham SMITH | SR Technologies | Sunrise, Florida |  | gsmith@srtrl.com |
|  |  |  |  |  |
|  |  |  |  |  |

Abstract

This document contains the minutes of the IEEE 802.11bh telecom Interim meeting January, 2022.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting Jan 8, 2021 13.30 to 15.30 pm ET**

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

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

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

**Secretary: Graham Smith (SRT Wireless)**

**Editor: Carol Ansley (Cox)**

**The teleconference was called to order by Chair 13.33 hrs. EDT,**

Agenda slide deck 11-21/1995r2

1. **Policies and procedures were presented by the chair. (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:
		+ January Interim meetings: Tuesday, 13:30-15:30; Wednesday, 19:00-21:00; Thursday 13:30-15:30; Friday 09:00-11:00
		+ Approve Nov plenary and December/January teleconference minutes
		+ Timeline reminder/review
	* 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)
		+ Response draft: TBD
	* Issues Tracking: [11-21/0332r29](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-29-00bh-issues-tracking.docx)
	* Contributions (slide 22)
	* Draft 0.1 (Proposals, slide 23)

Nothing yet prepared for WBA Response.

**Issues Tracking/Contributions**

* [11-21/1634r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1634-00-00bh-private-identifier-requirements-for-tgbh.docx) : Private identifier requirements for TGbh (defer?)
* [11-22/0085r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0085-00-00bh-irma-and-spoof-discussion.pptx) : IRMA and spoof discussion
* [11-22/0117r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0117-00-00bh-secure-device-id-exchange-concept.pptx) : Secure Device ID exchange concept
* [11-22/0118r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0118-00-00bh-irma-with-id-query.pptx) : IRMA with ID Query

Any comments, any objections to agenda, Agenda accepted.

4 meetings at this Plenary.

1. **Approve Minutes**
	1. Nov Plenary session: [11-21/1892r1](https://mentor.ieee.org/802.11/dcn/21/11-21-1892-01-00bh-minutes-tgbh-november-plenary-2021.docx)
	2. Teleconference minutes:
		1. Dec 7: [11-21/2025r0](https://mentor.ieee.org/802.11/dcn/21/11-21-2025-00-00bh-802-11bh-telecon-minutes-dec-7-2021.docx)
		2. Dec 16: [11-21/2026r0](https://mentor.ieee.org/802.11/dcn/21/11-21-2026-00-00bh-802-11bh-telecon-minutes-dec-16-2021.docx)
		3. Jan 6: [11-22/0072r2](https://mentor.ieee.org/802.11/dcn/22/11-22-0072-02-00bh-802-11bh-telecon-minutes-jan-6-2022.docx)
		4. Jan 11: [11-22/0071r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0071-00-00bh-802-11bh-telecon-minutes-jan-11-2022.docx)

Any concerns, discussion? None

Moved: Jerome Henry

Seconded: Kurt Lumbatis

Result: Unanimous Consent

1. **Timeline**

PAR approved Feb 2021

First TG meeting Mar 2021

D0.1 Nov 2021

Initial Letter Ballot (D1.0) Mar 2022

Recirculation LB (D2.0) Jul 2022

Initial SA Ballot (D3.0) Nov 2022

Final 802.11 WG approval Mar 2023

802 EC approval May 2023

RevCom and SASB approval May 2023

Chair pointed out we are behind for D0.1. Hopefully D0.1 can be started this week. Maybe end of March ready to start LB with D1.0.

Q – Would we circulate D0.1 or go straight to D1.0

A – Not sure we need to as it should not be that big.

C – Reasonable to stick to March for D1.0

Update timeline changing D0.1 from Nov to Jan 2022.

Any objections? None

1. **Response to WBA**

Nothing done but hope to come back to this later this week.

1. **Issues tracking Document now at Rev 29**

Focussed on updating section 5 on the last few teleconferences. Tables 1 and 2 are agreed to be a reasonable list to evaluate contributions.

At the moment we have 4 potential solutions.

1. **Contributions**

**22/0117r0 Secure Device ID Exchange concep**t. Luther Smith presented.

This proposal is an extension to 11-21/1378 & 11-21/1379r3

C – The exchange of ID is it intended to be a layer 2 ID or higher layer? What kind of ID is this?

A – It’s not for user ID but more as a replacement for the MAC address. Associated to the currently used MAC Address.

C – Not sure we need a public key. Already encrypted as the frame is encrypted.

A – Provides an additional layer of security. Also used for open network.

C – OK for open, but wonder how the STA gets the public key that is trusted.

A – Assumption is that the STA selects to attach and already has the MAC address. Based on going back to the MAC address for that SSID

C – Think the ID Query works as is and does not need a public key.

Q – Do you send the ID every time?

A – Only on association or pre-association. Only when associated with the MAC Address. When AP wants to know ID, the AP sends request with the public key.

C – Don’t need a different protocol to transfer this.

C – We did not want to restrain the use of the ID, yes is layer 2 but coming from higher layer. That is why device may choose the ID.

C – Have concerns with open networks and ability to spoof and steal IDs.

A – Just sniffing and taking public keys, they have no real use.

C – Not the key pairs, but stealing the IDs themselves.

A – Does not define what the ID is.

C - If this is just for the AP to have a MAC replacement then the AP needs to have control over the name space. The STA should not choose the ID. Should that be a security requirement that the ID be chosen by the AP or a combination of AP + non-AP STA. Could ID be “Joe’s I-Phone” and duplicates. Is public key bound to the AP?

A – Per AP, core device ID is the same.

C – So each time connect need to request the key pair? Does not work for, say, the grocery store.

A – Based on idea that there is a unique ID for each STA. Could be the permanent MAC Address encrypted.

C – What prevents the STA from sending a RCM each time? ID can be sent over the encrypted connection, so why define a new layer?

A – Device ID not defined in the original proposals.

C – If simple use of public key anyone can copy the public key. How would prevent copying of an identity? Problematic direction.

C – If every device needs an ID? Maybe not true, but other parts want an ID? Is that the intention? What is intent of the ID? Should we resolve that? Which entity assigns the ID?

A – Discussion to be taken back to the Issues document. Only when the Use case needs an ID.

C – Per Station public key or per AP? Depends on which one you are assuming.

A – Could be anyone of the 3 options. AP could use static key pair then public key is locked in to that AP. If randomized, then during any association a new public key. If STA changes address, then need a new key pair.

C – Generating per client public key this can generate a leak.

A – Could be static for that client but better if new key pair for each new association.

C – The key pair is equivalent of OWE. No authentication at all. STA needs a reason to trust the key. Fundamental security missing from this proposal – trust.

A – If user selects that SSID then has some trust of it – but see the point.

C – Only concern is that we have public Wi-Fi as open networks that won’t go away.

Chair – could make the IDs a topic for discussion in Issues document.

C – Need to agree what are expectations for security. There are open networks, but if you need to work in open networks then might need something like OWE.

C – Agree open networks but to have any sort of meaningful ID then need to have some degree of security. Open networks can supply security but not at layer 2. Have to rely on higher layers. Could add hooks that higher levels could use.

A – That is wrapped up in discussion we need to have.

C – In favour of simple security ID.

C – This higher layer stuff is not TGbh.

A – Many schemes used the MAC address as the ID, so could be TGbh.

C – Some broken is not due to RCM but to the scheme not being secure.

1. **“IRMA and ID” -** 22/0118r0**,** presented by Graham Smith**.**

Q – This is based on the AP. How does ESS work?

C – ESS uses same SSID.

C – Is there a cryptographic link between ID and IRMA. Seems to need a lot of calculations. New PDK each time,

A – No, I don’t see that. No calculations at all for the first time connection.

C – A little confused by concept that there is a lot of protocol. Decrypts MAC address using the key it has made the association. It then knows what to do. Once done, the re-keying is a simple protected message.

C – The IRMK Check field does put a burden on the AP. Proposal inTGbi to reduce work on AP. Symmetric crypto.

C – IRMA could use a fixed offset for the IRMK Offset.

A – Did originally consider just providing 8 bits of the key. Much easier to check, but does expose real bits – seems wrong but maybe not a problem.

C – Why not use a constant offset?

C – Offset can’t be constant because it becomes an identifier.

A – Constant offset might allow the AP to be ready and quickly find key. Would love suggestions on possibilities.

**Out of time**

**Meeting recessed at 3.30pm ET.**

**Meeting January 19, 2022 19.00 to 21.00 pm ET**

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

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

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

**Secretary: Graham Smith (SRT Wireless)**

**Editor: Carol Ansley (Cox)**

**The teleconference was called to order by Chair 19.03 hrs. EDT,**

Agenda slide deck 11-21/1995r3

1. **Policies and procedures were presented by the chair. (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:
	+ January Interim meetings: Tuesday, 13:30-15:30; Wednesday, 19:00-21:00; Thursday 13:30-15:30; Friday 09:00-11:00
* 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)
	+ Response draft: TBD
* Issues Tracking: [11-21/0332r29](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-29-00bh-issues-tracking.docx)
* Draft 0.1 status
* Contributions (slide 22)
* Draft 0.1 (Proposals, slide 23)

Nothing drafted on WBA Liaison and nothing to review today.

Issues Tracking document has not been updated since last meeting. Any issues? None

Any comments, any objections to agenda - None - Agenda accepted.

1. **Draft 0.1**

Not yet started but do have a number of solutions with text. Suspect that authors are waiting for direction form the group. Need to think on how to select.

Any questions on D0.1 – None

1. **Contributions**

22/0085 – Graham Smith declared that not ready to present as written some time ago and things have changed.

21/1634r0 – Kurt Lumbatis declared not ready but hopes to present later. Noted might rename to ‘Non-MAC device identifier’. Kurt mentioned could have a freeform discussion, but it was decided not to.

1. **Text for D0.1**

How do we prepare text, how do we select? What ideas do we have for text selection?

C – Comes down to what we want. Do we have informed consent?

Chair - One of the first criteria was that user must have opt-in. So what is the next step?

C – Could a network demand an identifier? If not available could the network deny access.

C – APs must show support. Think this is a higher layer.

C – We did discuss Nuclear Power Plants or such and denial of access.

Note: This is Use Case 4.10.

C – dot 1X would be better security.

C – Absolutely yes, network can refuse you. When I look at the issue tracking document, clients don’t have problems with RCM, it’s the networks. We ask the client to give an ID, I think network should supply the client with an ID and the client gives it back when asked. Uniquely bind the STA to the network. Allows for control of the identity space. Network says, “if you want to get on network this is the identity you must have”.

C – Don’t view it the same way, there is a need for the STA to identify itself and the network knows who it is. These are services for the users of the STAs.

C – STA randomizes MAC and does not lose anything. Problems were that the network relied on something and did not have it anymore.

C – RCM are used in many places, and if AP effectively allocates MAC to the STA ths would cause problems. AP decides its own address and so does the STA.

C - The STA loses the ability of the Network support/services - and is gaining privacy. STA needs to be tracked by the network but not clear who loses.

C – Idea of network assigns ID is OK as long as user can still opt-in.

C - That's what the SLAP does (assigns a quadrant for just that purpose assigning MAC addresses) but I wasn't talking about MACs exactly, it was identifiers.

C – If using SLAP still no identifier.

C – Static MAC does not indicate what services you are getting?

C – Example of captive portal does. Used RCM but want to still be on the hotel network

C – But could use the SLAP assigned MAC.

Note: SLAP (Structured Local Address Plan) is in 802 c-2017 Amendment to 802. Does not have a mechanism for assigning addresses, just creates quadrants.

C – We need an ID that is agreed by client and network, hence give both input into that. No need for one side to control? Could that work?

C – Multiple proposals for the ID. Could be a negotiation. Nothing has been defined.

C – STA is requesting services. Giving network control of its assignment space and does not really worry about what MAC it gets. Same as an IP address.

C – All of the problems that TGbh has identified are network problems. Up to the network to come up with an identifier that works for it.

C – But STA has a need to be private, that’s what it is all about. If an allocated MAC then it uses it each time, that is not private.

C – Use Case of Grocery store and identified to get specials. If STA does not have a say, or cannot use a group ID, then may not work if network assigns IDs.

C – Discussions getting muddy. The thing that occupies the place of the MAC address, would be handy if the system could track the device, but whoever assigns it, it is only an identifier. Can go either way. Need to clarify between an ID exchanged behind a wall and the thing that goes into the MAC address space. Better that the MAC address space is random. Only after associated then ID’d.

C – STA is doing this for privacy. No STA can access a network unless it uses the policy of the network. A network could say “can’t use an RCM”. STA can choose to connect, connects, gets ID then goes away. Comes back, says never been here before, give me another ID. Hence STA has it in hand to subvert.

C - P802.1cq was looking into assignment of MAC addresses

C – Don’t think it is within MAC level to create the identifier. Look at IP Address, it’s an identifier. Need to provide a mechanism to facilitate the upper layer identifier. Maybe a certain set of frame exchanges? Leave it to upper layers.

C – This example argues against your statement. IP address is an L3 identifier. They are assigned by the network without any input of the client. An L2 identifier would, similarly, be assigned by the network without any input of the client.

C – Client can always switch to legacy.

C – Leaving identifier to higher levels is a good direction but MAC can still be used to track it. MAC can be used to set it up.

Chair – Is an identifier needed, what do we need to answer before we proceed? If so we need to structure this a bit more. Does the group feel we should pause and go in another direction?

*Kurt Lumbatis shared 21/1634. In particular, the “Definition” (Note, the displayed text was not the same as that in r0 what was on Mentor)*

C – Addresses some but not all of the Use Cases. For example, the troubleshooting case. This does not address that at all.

Author did text changes on the fly. Secretary noted that he could not follow this as the document displayed differs from that posted.

Chair asked that the document be posted as r1.

**Kurt Lumbatis posted and shared 21/1634r1 and made changes on screen during the following discussion.**

C – If assigned by other people how do I know that it satisfies the recommendation? What is the condition. Seems to be too much.

C – We have a definition followed by implementation.

C – Do not know how to combine these two rules. Nobody has proposed a bunch of defined rues that the identifier need to satisfy.

C - We have to define the identifier in the Standard.

C – Note says could be email, UUID, etc. “used by the network, so makes no sense that the user configures it. Different implementation could use different rules to define or assign. Client need not care.

C – Disagree, grocery store identifier for the entire family then user has control and has assigned the identifier.

C – How do you guarantee that the network has something useable?

C – Identifier is passed as a text file “XXX family”

C – Then network has to know what “XXX family” means, how does it?

C – I hear common threads; issues are idea that it is unique – what does that mean? – within whatever purpose the network needs. The network needs to control the style and how generated but need not generate it. Sometimes network may allocate an ID. Sometimes says “this is what I want”.

C – Not sure the Private ID should be provided to the network every time you join.

C – I go back to Address is this Local, SLAP, I don’t believe that STAs can randomly decide its random MAC address I unique. But MAC address started this as people worried about privacy. Discussion on grocery store and types of IDs shown here are likely to be used at the higher layers above 2, and do not really concern us. As long as the hook is there.

C – Correlation between this device and this ID, a mechanism that network understands who this is. Maybe needs to be at the higher layer.

C – Identify a device that can still be private and still be identified. Private identifier, or unique identifier. Wanting a family ID not for the network which might want to know if maybe different devices allocated to a user. Recommend get narrower to ensure privacy and still identify a device. Anything past that I would push off.

C – Are we solving problems that need not be solved? We have spent time on all these Use Cases.

C – If an ID gives me a coupon, OK but if you want to do troubleshooting etc. retaining privacy needs to be kept at layer 2 and not passed up the stack.

C – MAC gets sent up the stack

C - Precisely and that is why RCM. Don’t need IKEA to know how many times I’ve been there

C – That’s why user consent.

C – Valid for the period of association – surely for longer than that? I suspect that this is dangerous and could hold us up for a long time with text that would not actually go into our Standard. Why is this new? Seems to me a lot of this either exists already probably in higher layers. The features and Use Cases are existing. If the MAC address was good enough in the past what’s changed. Also this appears to be tied up with the ID Query scheme, and if so, fine, but does it need all this, valid or not?

C – This was response to Table 2. Tried to relate to the identified Use Cases.

Chair – Tied up with what is the problem we are solving, and what are we trying to solve. Please go through the Use Cases and check that we have captured the right issues.

C – Have suggested the network creates the identifier, now TGbh is solving problems caused by RCM but these seem to be new use cases that we should not be working on. Namespace has to be controlled by the network.

C – Are we feature creeping this? Very difficult to keep to a narrow set of features. Need to stay focussed on what TGbh was created for.

Chair – Not sure how to organize now. Will try to organize for tomorrow’s meeting.

**Out of agenda**

Meeting recessed at 8.58 p.m. EST.

**Meeting January 20, 2022 13.30 to 15.30 pm ET**

**Chair: Mark Hamilton**

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

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

**Secretary: Graham Smith (SRT Wireless)**

**Editor: Carol Ansley (Cox)**

**The teleconference was called to order by Chair 13.33 hrs. EDT,**

Agenda slide deck 11-21/1995r4

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

There were no Patent declarations.

Copyright policy slides were presented (Slides 10 and 11)

1. **Agenda:**
* Attendance, noises/recording, meeting protocol
* Policies, duty to inform, participation rules
* Organization topics:
	+ January Interim meetings: Tuesday, 13:30-15:30; Wednesday, 19:00-21:00; Thursday 13:30-15:30; Friday 09:00-11:00
* Issues Tracking document: [11-21/0332r29](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-29-00bh-issues-tracking.docx)
* Contributions (slide 22)
* Draft 0.1 (Proposals, slide 23)
* 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)
	+ Response draft: TBD

The Chair reviewed the agenda.

The proposed agenda was adopted without objection approved by unanimous consent.

**Contributions**

* [11-22/0117r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0117-00-00bh-secure-device-id-exchange-concept.pptx) : Secure Device ID exchange concept (Jan 18)
* [11-22/0118r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0118-00-00bh-irma-with-id-query.pptx) : IRMA with ID Query (Jan 18)
* [11-22/0145r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0145-00-00bh-sta-identifier-way-forward.pptx) : STA identifier way forward

--

* [11-21/1634r2](https://mentor.ieee.org/802.11/dcn/21/11-21-1634-02-00bh-private-identifier-requirements-for-tgbh.docx) : Non-MAC device identifier requirements for TGbh (defer – partially reviewed Jan 19)
* [11-22/0085r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0085-00-00bh-irma-and-spoof-discussion.pptx) : IRMA and spoof discussion (defer)

Any questions or comments on Issues Tracking Document? None

1. **STA identifier way forward** – 22/0145r0 presented by Mark Hamilton

Presenter noted discussions have led to numerous opinions, for examples:

* Agreement that the identifier should be “private” and secured, but variety of opinions on “secured from whom?”
	+ This includes whether the identifier can/should be shared above layer 2
* Is the identifier style/semantics controlled by the device (user) or by the network?
	+ The interaction models have not been evaluated, however, such as how a network generated identifier is provided upon leaving and returning later
* How unique does the identifier need to be/in what scope?
	+ The global MAC address “abuse” came with some assumptions.
* Etc., etc.

How to make progress?

* Have we answered these questions in the Issues Tracking section 6 (and if so, are some saying our conclusions should be revisited)? If so, we need contributions to discuss
* Are these/are there new use cases that we haven’t captured, which generate new/different opinions?

Also, observations that

* None of the proposed solutions (so far) have made any assumptions about the identifier or its use, other than that it needs to be secured from third party tracking
* There is/has been no debate that protection from third parties is a requirement

C – At high level, agree. Fixed length MAC address could be one identifier. PAR is clear need to preserve the existing mechanism with no less privacy. Clearly cannot expose this information. Provide means maybe to exchange MAC address but against trying to expand our scope. Want TG to finish soon. Can continue in parallel with solutions.

C – Are we to allow for opt-in if user does not want to use an identifier?

A – That is a requirement on a solution

C – Want identifier to be secure from third party tracking so would this preclude a protocol to provide MAC addresses from the SLAP AAI, which would be visible,

A – First response is how does device gets the MAC address for OTA, is not in our scope

C – Could be an action frame exchange, “need a SLAP”

A – Interesting but not in our scope. Analyzing only features broken by not using universally assigned MAC address.

C – Surely address assigned could be in-scope

A – I suppose so, needs discussion.

C – I would not rule it out. Third party tracking is grey area. Need something STAs willing to use. If ESS would assign STA an address and expect it to be used each time, that may problem. If short term address, then may be viable. Is trackable as we do not encrypt the MAC address.

C – Question of how to assign and share identifier, but secured from 3rd party. Any exchanges need to be behind the encryption layer. Could add “WM passive observation”?

C – Back to SLAP, is this generated per association?

A – Could be assigned for single association but link it for subsequent associations. Not good for long periods

C – Is that not against what we want which is a static identifier?

A – Next time come back could get new address but linked to the identifier.

C – Confused, are we talking about ID as in ID Query or ID as per the TSID or the IRMK?

A – Must use the Use Cases as per the Tracking Document. Need to stay focused on solutions based on those decision criteria.

C – Problem is the permanence of the ID. A permanent ID is needed so that the network has the credentials or such to recognize the user or device when it associates. E.g. home network

C – Open on third party definition. If we are talking about long term then hesitant to use a MAC address at all. Home case would probably need a permanent ID and not use MAC address. Look at each use case to see if need for long term identifier in each case. Some may work with assigned MAC address where others would not work. May have more than one solution. Do need to be clear.

C – Idea of more than one solution has come up before.

C – Third party – need tighter definition. Case in Europe on ‘right to be forgotten’ and disappear off the internet. May be problem if identifier lasts a lifetime. Could be negotiable. Could be a criterion we need to account for.

A – Yes that would be a great contribution.

C - I think we have at least 3 types of IDs: User ID, Device ID, Application ID - I think we need to refocus and decide which ID or IDs we will address in TGbh - this probably needs to be added to our criteria. Need to avoid problem s because we use the same terminology. May be we only solve the device ID problem in TGbh.

Chair – We need to be clear what identifier we are solving. If not clear, then we must have contributions showing the issues. Open ended discussion is in danger of going in circles.

C – Group formed for problems with RCM because MAC address was being used as an identifier. Was that a device, User or application ID?

A – 802.11 always used it as device ID

C – Then that is all we need resolve?

C – But discussions are not just in that direction, they are directed at the issues that arose.

C – Are User and Application IDs out of scope? (to Chair)

Chair – We have Use Cases that the TG has agreed to fix. Noting there is nothing about what sort of ID is used. We have simply agreed that these are in our scope.

C – We should just depend upon device ID. Then we can make fast progress.

Chair – We have had the conversation and captured the Use Cases. If we believe scope creep, then need to clean up the document.

C – Agreement that device ID can be solved, so do that and then keep going if necessary.

C – Makes sense to re-visit the Issues tracking document and consider multiple solutions.

C – Could go through the Use Cases and identify the identifier – is it ‘device identifier’.

C – User ID and Application ID are upper layer as to who the user is. We are looking as to identify the device, which was the MAC address. If the AP wants to use that in any upper layer application, then that can be associated to the physical device. MAC Address identified the physical device is what we should be looking at.

Chair – Worried we might have slippery slope as to definition of a device ID.

C – Yes, what is a device ID? To my mind it is a MAC Address.

A - Let’s look at the analysis of our use cases and not spend time on definitions.

C – Issue we seem to be addressing is various uses of MAC Address must not be used for identification. Only used for directing packets. Fact is that random MAC has no problem at network level. Other uses of that address were not layer 2 specific uses. But our user base has real issues so we must be responsive.

A – Similar conversation early on that features in .11 used to solve problems outside layer 2.

C – Our PAR was to solve the user problems raised by RCM. If we assume that once the network knows the device is the same STA as far as the network and the use cases are concerned, our work is done. No need for definitions. We have solutions on the table that do this. If the network recognizes the device, is that good enough?

C – Pick a use case and come up with solution for that, see if this is OK, rather than revisiting everything.

C – Wandering off towards user IDs and getting too far into that and wandering away from what we are trying to address, i.e. MAC address being used as identifier. All about recognizing the device the second time. All use cases boil down to that. Figure out secure way for device to share some token of device ID with the AP so it can be recognized. It was the second visit that was broken (if random MAC used). Should it be real MAC address or some other mechanism. Need to recognize the STA the second time.

C – We do have ‘nice to have’, and if we don’t make progress we could drop these and only concentrate on post association.

Chair – maybe we focus on Use Case 4.2 (Post association device identity) and then build from there. Look at our solutions and see how they fit.

Chair – Does that seem a way forward?

Consensus.

Chair – We have 5 proposed solutions, one builds on another, one is a combination. What does group feel is way forward?

C – All seem to be complex. Could be made simpler.

A – Need a proposal. Don’t see how that is different from ID Query.

C – Is time past for proposals?

A – No such agreement. Anything that gets us unstuck.

C – May be simpler methods using existing message exchanges.

C – Agree cannot support any proposals so far. Whatever we do will not work for open networks. Are we OK with that?

A – That is question for the group.

C – User opt-in if user aware that ID may be shared in open, then solved. Could we review each solution to check that TG feels they could not be used to move forward?

Chair – could use straw polls and down select but that assumes no new additions along the lines of this discussion.

C – One observation on private ID discussion, it seems agreement on identifying returning STA is same STA, is a service we expect the network to provide. Could add primitives etc. Might miss fact of storage. Example a huge ID could be prohibitive.

C – Open networks is not important. Inclined to say let’s drop open networks, we have OWE to solve this. Simple solution for the one use case.

C – We need some simple solution as we are slipping. New proposals to put something on the 4-way HS we need user input for opt-in. Not to allow AP to force something on the 4-way HS.

C – Seems to me the ID Query s pretty simple and satisfies.

C - Also extensible. Expanding the action frame.

C – Maybe a subset of ID Query, needs to be simpler. Maybe drop the query and just use response.

C – Refer to email suggesting a method to fold something into the 4-way HS using an encrypted blob with single operation. Need to make a presentation.

Chair – Need a presentation for device and returning device.

C – The simpler we can stay focused on just solving RCM the better. Do not add new features.

C – So people will bring new presentations. No need to go through all the submissions on the table.

C – Meeting tomorrow can we get a simpler solution proposal?

Chair – still need criteria considerations as per the Tracking Document. If concerns on the issues tracking need a contribution. Have left margin comments in the issues tracking document which may need to be revisited.

**Out of agenda**

**Meeting Recessed at 15:26 ET.8**

**Meeting January 21, 2022 9.00 to 11.00 pm ET**

**Chair: Mark Hamilton**

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

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

**Secretary: Graham Smith (SRT Wireless)**

**Editor: Carol Ansley (Cox)**

**The teleconference was called to order by Chair 9.02 hrs. EDT,**

Agenda slide deck 11-21/1995r5

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

There were no Patent declarations.

Copyright policy slides were presented (Slides 10 and 11)

1. **Agenda:**
	* Attendance, noises/recording, meeting protocol
	* Policies, duty to inform, participation rules
	* Issues Tracking document: [11-21/0332r29](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-29-00bh-issues-tracking.docx)
	* Contributions (slide 22)
	* Approve Draft 0.1 (Motions)
	* Response to Liaison from WBA:
	* Other use cases not covered yet/notes in Issues Tracking document?
	* Next Steps:
		+ Timeline review/update
		+ March plan
		+ Teleconferences

The Chair reviewed the agenda. Noted that TG is probably slipping its Timeline again.

The proposed agenda was adopted without objection approved by unanimous consent.

1. **Issues Tracking Document**

Any comments or observations – None

1. **Contributions**
* [11-22/0117r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0117-00-00bh-secure-device-id-exchange-concept.pptx) : Secure Device ID exchange concept (Jan 18)
* [11-22/0118r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0118-00-00bh-irma-with-id-query.pptx) : IRMA with ID Query (Jan 18)
* [11-22/0145r0](https://mentor.ieee.org/802.11/dcn/22/11-22-0145-00-00bh-sta-identifier-way-forward.pptx) : STA identifier way forward
* [**11-22/0154r0**](https://mentor.ieee.org/802.11/dcn/22/11-22-0154-00-00bh-opaque-device-id.pptx) **: Opaque device ID**
* [**11-22/0157r0**](https://mentor.ieee.org/802.11/dcn/22/11-22-0157-00-00bh-mac-address-designation-maad.pptx) **: MAC Address designation MAAD**

**--**

* [**11-21/1634r2**](https://mentor.ieee.org/802.11/dcn/21/11-21-1634-02-00bh-private-identifier-requirements-for-tgbh.docx) **: Non-MAC device identifier requirements for TGbh (defer – partially reviewed Jan 19)**
* [**11-22/0085r0**](https://mentor.ieee.org/802.11/dcn/22/11-22-0085-00-00bh-irma-and-spoof-discussion.pptx) **: IRMA and spoof discussion (defer)**

22/0158r0 “STA generated Device ID” added to the Contributions list

1. **Presentations**

**“Opaque Device Identifier”** Dan Harkins presented 22/0154r0

C – Sending at M2 why not M4?

A – As no M5 no way for STA to give back substantiation of the blob

C – M2 blob is in the clear, but not usable. Tweak would be different.

C – Tweak every time?

A – Yes. Last teak used with the device identifier. The tweak is different every time. The protection is the 64-bit tweak.

C – What happens if someone does replay an old blob. Does network recognize?

A – Yes, the tweak is validated

C – There is back end sharing

C – How to handle potential collision on identifier.

A – Device ID is assigned by the network, can’t duplicate. ID can be anything, nothing to do with what the STA thinks it is. Network owns the ID space

C – The Tweak is used to protect against replays, and padding

A – Tweak prevents reuse. 232 protection is extremely high.

C – It is random or does not matter

A - Probably does not matter. Looked at, it is random but maybe could be monotonically increasing.

C – Key is distributed to network. Is it constantly updated? The client does not know what the ID is as it is encrypted

A – STA does not care what its ID is. Just used to track connections.

C – Is M3 if STA does not have a blob, then AP will put one in?

A – Yes. Tool for tracking connections across associations. First time association does not have a blob. Using the tool is different for use case as first association may be differently handled. M2 on first association there is no blob.

C – STA has to maintain the blob, based on the ESS and then when it comes back it must use it. What happens if it forgets – it must get new blob?

A – Yes

C – Parental control, say child’s device loses blob (resets?), so gets access again?

A – If no blob then could flag a quarantine. If you want to opt out, then omit blob. Will get a new blob, but just throw it away. Use case can use the tool on a use case basis.

C – Potential to track is very implicit – opt out rather than opt in. How to inform user that blob is being included?

A – We do not concern ourselves with user interfaces

C – Way to have blob included beforehand or inform STA that AP will send it a blob.

A – Not important that getting a blob is important. If not wanted to track, then throw away the blob. To network, blob is meaningless.

C – Would like to inform the user.

C – Nice if STA knows that the network will supply you with a blob

A – Does not affect the user at all. Is a Layer 2 tool.

C – Whether this blob update is on re-associations or just associations

A – Does not matter

C – If something to announce capability. If STA does not support is gest a blob it does not know. If grocery store assigning blobs but not being used. How does AP see this?

A – Could put bit in RSNE that it supports blobs. STA says “don’t give me blobs”.

C – In association request say “do not give me blobs”. Give STA opt out.

C – Blob per SSID needs to be retained. Does the STA still share an assigned SSID. Once STA is assigned there is some sort of identifier. Parental control if child resets each time, “Johnny is in quarantine”.

A – Depends on how the UI is constructed. Captive portal can provide many IDs, credit card, name, etc.

C – Slide 3 if STA wants to stop being tracked. How does STA know?

A – received in 4-way HS. If you get KDE and don’t want to be tracked, throw away the blob.

C – How does this compare to PTK as shared secret, i,e, the blob is the PTK (shared secret). Since used in encryption PTK is a shared secret, is that not similar to the blob idea? Is there a problem to hold on to the PTK? Could the PTK be the blob?

A – Don’t think that works, blob is passed in the clear so do not declare PTK

C – Could PTK not be used as ID for future connections?

A – Not sure how to hold on to the old PTK that is secure. How does AP know which PTK?

C – Once disassociates PTK no longer used, but in future connection could be used.

A – Can’t see how the AP remembers of how does STA tell AP which PTK to use? Something needs to be sent in the clear. All previous messages using that PTK can then be decrypted when the PTK is declared

C – Would opt out be based on ESS or overall? On re-association the blob is maintained not forgotten

A – Blob is a tool. How you throw it away is up to you.

C – If look at TSID proposal can derive form PTK without sharing. Back to option if added some element to advertise the capabilities might useful

C – Is symmetric key another key

A – New key.

Chair – might be useful to go through Table 2 and answer criteria

**STA Generated Device ID** 22/0158 presented by Jouni Malinen

C – Could use M2?

A – M1 cannot be encrypted. M2 could be used. Used M4 because it is easier and saw no need to generate earlier. Rather not send in M2.

C - In re-association request why only in FILS

A – FILS does not have 4-way HS.

C – Like idea but similar to ID Query concept but moved ID to piggyback on other frames. This does not include Clause 6. Saves a message exchange.

A – Not claiming to be simpler.

C – One other thing in ID Query was supplying a hint for time validity.

A – Agree, idea was to use minimal.

C – In previous M2 is unencrypted, if it is encrypted blob proposal can be simplified.

C – If STA tells network an identity needs to be useful for say the troubleshooting case. All STAs should provide ID in similar format. That requires a unique value per ESS to be retained per device.

Chair – Needs to be compared against the criteria list

C – This addresses secure networks, not open networks.

A - Use OWE if open.

C - Should we address open networks?

C – Overhead is minimal but need to have restrictions on length of ID as could be used to track STAs. Could be extended for pre-association. ID generated on first association from the PTK or such. OUI could advertise what sort of scheme in use.

A – Yes worthwhile pursuing.

C – On previous scheme, if encrypting M2 the tweak can be omitted? But isn’t the tweak used to identify?

A – Tweak would still be there, but stateless. AP required to remember the last tweak. If M2 unencrypted the blob can be seen. Hence if encrypted M2 observer cannot see the blob.

C – In Association Request frame, is it encrypted?

A – Only in FILS which means it is encrypted. In all cases the STA can supply the ID if RSNE.

C – Does it make sense to add Time to live (TTL) (8 bits say)?

A – Yes, would be happy with that.

C – If tweak removed from the Blob then essentially the two proposals are similar.

A – Tweak is not removed. AP need not remember the tweak from the last ID.

C – Is the same device ID as in previous presentation?

A – No, this is generated by the STA. Can be global or unique identity.

C – Originally do not randomize address when at same ESS.

Chair – Summary - possibly add network generated and criteria statements plus TTL

**MAC Address Designation** **– MAAD,** 22/0157r0presented by Graham Smith

C – 802.1 cq defining a protocol for MAC address assignment.

A – Yes could align with that.

C – Did discuss this before. Network assigned. Action frame has to be encrypted?

A – yes, after association

C – could be included in 4-way HS

C – Post association, yes, everything encrypted

C – Up to AP to link the assigned MAAD request frame, with STA.

A – Uses MAC address as the identifier (as is done now).

C – May cost serious overhead issue. With a lot of STAs. Other schemes do not use exchange frames

A – Same as many other schemes, no more.

C – Use of some other Identifier?

A – Then same as ID Query. This is simpler and fits perfectly with how it is done now with the MAC address as the identifier.

Out of time

1. **Chair final points**

Timescale is slipping

Need to agree how many meetings at next Plenary

**Out of Agenda**

**Meeting Adjoined at 11.00 am ET**