Minutes IEEE P802.11
Wireless LANs

|  |
| --- |
| IEEE 802.11 TGbh Meeting Minutes, Sept 2021 InterimRandomized and Changing MAC addresses (RCM) |
| Date: 2021-09-15 |
| 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 802.11 bh telecom Interim meeting September 2021.

Note: Highlighted text are action items.

Q- proceeds a question asked at the meeting

A- proceeds an answer

C- proceeds a comment

**Meeting Sept 15, 2021 19.00 to 21.00 am 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 19.03 hrs. EDT,**

Agenda slide deck 11-21/1294r5

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

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:
	+ September Plenary meetings: Wednesday, 19:00-21:00; Thursday 13:30-15:30; Friday 09:00-11:00
	+ Approve July interim and August teleconference minutes
* Scope of TGbh and TGbi: [11-21/1470r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1470-00-00bh-scope-of-tgbh-and-tgbi.pptx) **, (**[**11-21/1395r2**](https://mentor.ieee.org/802.11/dcn/21/11-21-1395-02-00bi-view-on-private-identifier.pptx)**?)**
* Consider 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) (any issues we missed?)
	+ Response plan
* Issues Tracking: [11-21/0332r13](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-13-00bh-issues-tracking.docx)
* Contributions:

The Chair reviewed the agenda.

Any comments? None

Agenda accepted

1. **Approve the minutes of**

July Interim session: [11-21/1174r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1174-00-00bh-minutes-tgbh-plenary-july-2021.docx)

Teleconference minutes:

* + Aug 10: [11-21/1361r1](https://mentor.ieee.org/802.11/dcn/21/11-21-1361-01-00bh-802-11bh-telecon-minutes-aug-10-2021.docx)
	+ Aug 19: [11-21/1403r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1403-00-00bh-802-11bh-telecon-minutes-aug-19-2021.docx)
	+ Aug 31: [11-21/1504r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1504-00-00bh-802-11bh-telecon-minutes-aug-31-2021.docx)

Moved: Graham Smith Seconded: Peter Yee

No discussion Result: unanimous consent

1. **Contribution 21/1470** “Scope of TGbh and TGbi (Mark Hamilton and Carol Ansley

Background

* Both TGbh and TGbi were started by the RCM TIG and study group, and they have related scope
* This has resulted in some confusion over which group is appropriate for consideration of some contributions
* This document is meant for discussion, to try to reach consensus

Presented by Mark Hamilton.

Main points:

* Must be within 802.11 scope
* Support mechanisms within MAC/PHY (sub)layers
* TGbh defined by PAR
	+ Facility or behavior disrupted by MAC randomization
	+ Any modifications must not expose user information, presence or behavior
* TGbi
	+ specify new mechanisms that address and improve user privacy

C – Basically from PAR, second and third bullets are different angles of Randomized MAC. Presentation in TGbi this morning hit on this. There is a relationship and do not want to do two solutions for the same thing. Private identifier may be addressed in both.

A – Also timeframes are such that TGbh is expected to complete quickly. With time more thigs may be identified, maybe from work by TGbh, then TGbi may spend further time on it.

C – Not sure we can charge ahead with both groups.

C – TGbh is trying to solve random MAC problems with a private identifier. As long as this works then there may be no need for TGbi to take it up unless implementation shows it may have privacy issues.

C – Very clear, TGbh is not here to state whether random MAC is a good thing, or not, but to recognize it is happening and some features that were supported may now not be. The PAR clearly states no new privacy issues. If a private identifier happens, then fine, then it must not create any new privacy issues. TGbi should only be looking at new privacy issues. If these have been solved by random MAC then these are not new.

C – I think the concern is that some additional privacy concerns identified for which a unique ID with random MAC could address. If TGbh solves its problem with one identifier, and TGbi comes later with another identifier, then multiple solutions may occur.

C – That is no different to any two TGs happening at the same time.

C – TGbh is the foundation for TGbi to continue. Same as two PHYs running at same time interfacing to common MAC. Amendment ahead is the base for the second. Scopes are well written and clearly are different with TGbh being ahead of TGbi and hence can create any mechanism it wants within its PAR.

C – Track users using MAC was an unintended consequence. Need to specify use cases to be addressed and find a mechanism.

A – The tracking document does exactly that.

C – Identifier concept in both TGbh and TGbi.

C – Any identifier that gets defined should be done in TGbi which begs question as to what

C – It is clear what the difference is. The PARs are clear. TGbh is ahead and fast, so if you want to offer a private ID then do it in TGbh as that is the fastest way to get it into the standard. Wish members would simply accept what the PARs say and not try to create new ones.

C – MAC randomization fixed some things but created other problems. What would happen if TGbi decided that TGbh has created new problems?

C – TGbh PAR is clear, no new privacy concerns to be introduced.

C – Not sure there is consensus on the PARs, one way forward is to prioritize TGbh and slow down TGbi.

C – The Tracking Document is trying to do that in that issues identified and then sort solutions. It is up to the TGbi group to decide its speed. Agreed that TGbi follows TGbh in amendment order, so automatic throttling mechanism. But always room for co-operation.

C – We had to have consensus to get the PARs accepted, so take issue that “not sure on consensus”. The votes were very high. Also read the CSDs to see the distinction between the TGs. I support the Chairs in their efforts so far. Decisions have been made, no re-considerations need to made.

C – Have some joint sessions?

C – May be a good idea if mechanisms that work in both groups but differently.

C – Anything on a private identifier should be presented in joint sessions.

C – Difficult to know which are identifier proposals.

C – Need specific proposals. TGbh needs to get to the place where TGbh has something concrete to discuss.

1. WBA Liaison **:** [**11-21/0703r0**](https://mentor.ieee.org/802.11/dcn/21/11-21-0703-00-0000-2021-april-liaison-from-wba.docx)

Chair - Did a pass through the document, but need to check again. Then decide how do we want to respond. First thought is that if we have considered all issues then could respond point by point, which ones to address etc., or simply point at Issues Tracking Document. Document 21/1141 looked at the WBA points.

1. **TGbh Issues Tracking document: 11-21/0332r13**

Chair introduced latest version of the Tracking Document 21/0332r13.

Noted that document is complete but needs clean up and review. Captures discussions rather than clear text.

This document lists the issues and identifies which issues are within scope and need a fix.

If overlap of similar problem to be solved these are combined. A matrix 21/1140 is an aid.

So close to wrapping up the requirements phase and can start to look at Spec amendments.

One text proposal not yet reviewed.

Any questions/comments?

C – It’s all about an identifier.

C – Not a proponent of joint sessions and do not want a solution too fast. Need to take time. Want to see many different solutions. Find best one(s).

C – Sent email with list of conditions that an identifier need meet.

C – Agree, good set of conditions and suggest should be a presentation and discussed.

C – Reflectors tend to be quiet.

C – Members may be encouraged to attend both but there are conflicts.

Chair – Call tomorrow (Thursday) has no conflict and encourage TGbi members to attend. Could look at buttoning up the tracking requirements’ document (plus WBA issues) and look at the list of requirements for a private identifier.

1. List of requirements

Was written to address the suggestion that BLE uses an resolvable address. As it is an address this list was written to address an address.

i.e. is visible to others.

Should we step up a level and look at some features of identifier.

C – We should not look at solutions before we have requirements but could be less rigid in looking at possible techniques and see how they may be used for Use Cases.

C – User should also have a say in whether to use a feature or not.

C - Yes, we have used the opt-in process.

C – Yes I will produce something for tomorrow’s meeting to discuss features for identifier.

**Out of agenda**

**Next calls Sept 16 13:30 ET**

**Meeting recessed at 20.48 ET.**

**Meeting Sept 16, 2021 13.30 to 15.30 am ET**

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

**Agenda slide deck 11-21/1294r6**

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

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:
	+ September Plenary meetings: Wednesday, 19:00-21:00; Thursday 13:30-15:30; Friday 09:00-11:00
* TGbh requirements discussion:
	+ Liaison from WBA, and our analysis: [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)
	+ Issues Tracking document, section 4: [11-21/0332r13](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-13-00bh-issues-tracking.docx)
	+ (Resolvable random address: [11-21/1535r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1535-00-00bh-resolvable-random-address.pptx) – Graham Smith)
	+ Private identifier requirements: [11-21/1531r0](https://mentor.ieee.org/802.11/dcn/21/11-21-1531-00-00bh-private-identifier-requirements.docx) – Dan Harkins
	+ Relationship to TGbi discussions – Consider any apparent overlaps (are they
	overlaps in requirements, or common/leveragable solutions?)

The Chair reviewed the agenda.

Resolvable Random Address presentation can be delayed. Contributor explained that it was posted as a background for the Private ID requirements presentation

Any comments? None

Agenda accepted

1. **WBA Liaison document**

Chair gave background. Call for any inputs – none

1. **Issues tracking Document**

Chair showed Rev 14 which is not yet uploaded.

Pointed out list of use cases. Called for any new cases.

1. **Private identifier requirements**

Dan Harkins presented 11-21/1531

Idea is that requirements should drive the solutions. Agree what we are expecting from a private identifier.

Dan went through the 10) questions/requirements:

Note: Dan added responses and comments to his document as comments were received. These may/will differ from what is captured below.

1. How often should it change?

C – May be different for use cases. Some, such as home, can be static, identify same device indefinitely. Other such as Hotspot may provide semi-persistent. Depends on trust.

C – Could be static per ESS. STA provides info per ESS.

C – Whether dynamic must be chosen by user. True for some networks, unchanging as trusted. ID should be assigned by the user.

C – Agree give user the most control. If I had a shared ID with network, I have made that decision.

But no-else can track me. I want my Starbucks coupon and my animosity.

Q – How is that different from a random MAC address?

C – Can track a Random MAC via RSS/location, for example, so nice to change the ID regularly

C – Should there be authentication of the network?

A – That comes later.

C – First question goes to the PAR, what is the exposure of the identifier. If exposed to 3rd parties, then PAR says no privacy issues. If protected, then only sharing with ESS.

1. Is it invertible such that the "real" address/identifier can be determined from a private address/identifier?

Any binding? Could get identifier from a hotel, for example, and not bound to its real ID.

C – Most of use cases in TGbh, no requirement for such mapping, but maybe for TGbi.

C – Two types of problems, recognition when you come back, and enterprise case, with neighbors above and below. Mappable identity that helps scale to enterprise.

C – Don’t know if needed.

C – If user name relates specifically back to private information, then may be needed for say enterprise/office, but in other cases no need to relate to actual identity.

C - My thought is that the Private Identifier would be co-related with the association MAC address and be utilized in upper layers.

C – Need to work in opposite direction, need to make sure any identifier is not bindable or may be correlated back to the user.

C – In my view should not be invertible

C – Should be completely under user control.

1. Can a 3rd party determine whether an address/identifier is private or not?

For example, 3rd party knows a random MAC is in use.

C – Depends how the identifier is passed encrypted, then 3rd party cannot capture

A – not the question being asked.

C – Think No. No-one else aware of exchange.

C – No, should be entirely private. Does expose that I am using a private ID. Reveals I am using a private identifier.

C – But that is same as knowing that a STA is using a random MAC.

C – Is it a problem if others know you are using a private identifier?

A - THAT’s the QUESTION!!

C – Rephrase to be “do we need to prevent exposure that a STA is using a private identifier”. I don’t see that this is a problem.

C - The third party can use the knowledge that I am using this identifier. his should not happen, i.e. the fact that I am using this address should be opaque to anyone outside of the AP-STA

C – Say 10 STAs in a room, 9 use real MAC and one uses random. Then problem that this STA is hiding something?

A – Even more sensitive than using a VPN or random MAC?

C – Everyone using local addresses, changing time may indicate a PCI. Cannot prevent PCI from being exposed.

C - I think we should aim to make this opaque if we can, but if we can't it's not a showstopper.

Discussion took a side step into TGbh vs TGbi

C - creating an invertible identifier is beyond the scope of bh, we create a new method to identify the real users, not just as "the same user that logged in yesterday", and this is a slippery slope. Networks could start demanding that the users would use that identity in order to connect.

C - but we are supposed to avoid creating new privacy issues in TGbh

C – could re-purpose this document into a TGbi document but we just need answers to these questions and where the work is done is irrelevant.

C – TGbh is supposed to fix problems of RCM and TGbi may take it over.

1. Is it assumed that only certain entities can figure out the "real" address/identifier?

C – what separates this from 2)?

C - work for 3rd parties to be able to determine the private identifier?

C – Obvious answer is yes.

C – Can we define tracking?

1. Is the private address/identifier bound to a secure connection or is unencrypted (poss. unassociated) use of this functionality required?

C – Yes whenever possible, avoid exposing PII on first use. Careful not to have a solution that may only be used in secure solution.

C – Want to be recognized when we come back. Protected first time, maybe when coming back can send before association

C – Need to assume secure. Non private first use not acceptable.

1. What are the assumptions on forgery of such an address/identifier?

C – Depends who is forging.

C – Hotel use case, allows guests things, can someone not staying at hotel get access by forging?

C – If you know the identifier, you get access. If 3rd party can figure it out, it must be hard.

C – No notion of forging a random MAC address.

C – If mutual authentication has been carried out, then difficult to forge.

C – Need to set rules for the identifier that makes it difficult to forge.

1. Are there any requirements to force STAs to do a scheme like this? Is co-existence (with other schemes, or no scheme) necessary?

C – No. Client decision.

C – Some network requirement could be to force an ID. Use can decide to connect.

C – Opt in on both sides

C – Opt in but network tells STA what is expected.

1. Are there any collision resistance requirements?
What's the probability of collision of private addresses/identifiers with 10,000 associated STAs? 20,000 STAs

C – Skip as already covered

1. What about protecting client identities from the network?

C – condition to connect is in the hands of the STA.

C – Network must make it clear what is expected.

C – If network, after connected, says I need your real ID. Then lost privacy.

1. What other requirements do we have on usage of this address/identifier (aside from “private”)?

A - cut-and-paste attack, substituting one address/identifier for another, must be prevented. Impersonation, attacker using someone else’s address/identifier, must be prevented. Traffic analysis must not be enabled, the greatest extent possible. Solution must not enable DOS or CPU exhaustion attacks on either AP or STA.

Time ran out

**Next calls Sept 17 9:00 ET**

**Meeting recessed at 15.30 ET.**

**Meeting Sept 17, 2021 09.00 to 11.00 am ET**

The teleconference was called to order by Chair 09.03 hrs. EDT,

**Agenda slide deck 11-21/1294r8**

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

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
* Having reviewed [11-21/1531r1](https://mentor.ieee.org/802.11/dcn/21/11-21-1531-00-00bh-private-identifier-requirements.docx) (Dan Harkins), what do we with it? Use as a “metric” to evaluate proposed solutions? Something else?
* Reminder: 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) , and our analysis: [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). What sort of response should we provide? Volunteers?
* Review status of Issues Tracking: [11-21/0332r14](https://mentor.ieee.org/802.11/dcn/21/11-21-0332-14-00bh-issues-tracking.docx)
* Contributions (that haven’t been reviewed): [11-21/1379r2](https://mentor.ieee.org/802.11/dcn/21/11-21-1379-02-00bh-proposed-text-for-id-query-action-frame.docx) , 11-21//1535r0
* Next Steps:
	+ Timeline review
	+ November plan – D0.1 target
	+ Teleconferences

The Chair reviewed the agenda.

Any comments?

C- 21/1535 should be added to Contributions. Agreed , Done

Agenda accepted

1. **11-21/1531r1**

Have there been any new comments – no

Chair – what should we do next?

C – We should discuss requirements before discussing solutions. See how the solution tracks with the requirements. Also could notify TGbi that this is TGbh’s opinion.

C – Did we finish? Document should be distilled down into a set of requirements.

A – We did get through all points. Distill down – if we use to evaluate solutions then useful but not spend time coming to a set fixed parameters that constrain the solutions.

C - We could add “must have” or “desirable” or we just leave it and each solution must make a response against each point.

Chair - Other thoughts, comments, any volunteers to distill down to a set of requirements, desired etc

Kurt Lumbatis volunteered and Jerome Henry offered to assist

1. **WBA Response:**

Chair volunteered to help in response to WBA.

C – Think we do need to craft a response. Could be we simply say that we took into account their inputs

Chair – options are a simple letter of thanks, or could go through each point and provide our responses, or perhaps liaise the documents.

C – First option is perhaps easiest as we do not have real consensus and things may change.

C – Generally we do not send liaisons back with a simple “thanks”. We typically as a TG ask WG Chair to send a thank you. Hence we need to add something to it.

Chair – we could respond but say we are still working on it.

C – Providing a pointer to what we are doing may go astray if we change our thoughts. We could at least point out those cases that we feel are not in our area and we will not be doing anything with it.

C – WBA are also looking at this issue, don’t like if each side thinks the other will solve it.

Chair – We can be clear it is a work-in-process. There is not a specific deadline

Chair and Jerome Henry volunteered to help draft a response.

1. **Issues tracking Document**

Version 14 is posted. Chair showed the contents and Section 4 is the list of Use Cases with real world descriptions and impacts. Then we state if we feel if the case is one we will address

When document was started we had problems with terminology. At this point do we need to worry about this, or can we come back later? Suggestion is to maybe drop the terminology section.

C – Agree do not need to discuss again. We do not need to define the terms

C – Agree, it could be rat hole. Better to wait and see if needed, doubt it.

C – If we want a D0.1 in November we should avoid this until then.

C – Let draft contributions drive this

Splitting use cases and high level discussion may not be useful.

Chair went through the document showing the text as result of discussions. Chair made on screen additions and notes during discussions.

Opt-in?

C – We discussed that some networks may require an identifier. This may impinge on privacy.

C – Still user opt in control/decision, but without agreement, no access is allowed

C – AP can reject association for any reason.

C – Opt in concept is important

C – Do we need another Use Case for post association network access?

C – Require you to provide identity? Check your credentials before allowing access.

C – Informing client of situation may be helpful to the client as to what networks to join.

C – If complicated ways for opt in opt out mechanisms can be difficult for operator or user.

C – We are confined to the dot 11 layer.

C – Not sure if this document needs to deal with this. Issues matrix may be better way to deal with this. There are ways to do get kids time, based access to the network for example. I though we agreed not to work on Home automation and parental controls. Products exist, not our business to solve their problems for them.

C – For lawful intercept, different countries may have different requirements to force tracking.

C – Checked solutions for parental control that log into the cloud.

C – Not our job to assist police.

Chair jumped to Lawful Intercept Case in the document noting that we did agree we did not need to fix it.

Home Automation

C - did document capture points, opt-in? No response so assumed OK

Airport Queue – we agreed out of scope as privacy

Grocery Store - without opt-in, out of scope, but frequent shopper then is in scope.

SSIDs for different bands – agreed problem caused by deployment issues.

Probing with different addresses – was considered out of scope

4.9 and 4.10 Rogue detection – not affected by RCM

C – We had a discussion on further describing case where a Laptop goes to another SSID is a problem but not sure we can do anything.

C – not sure of difference between 4.9 and 4.10

A – Originally did not the two but on discussion decided to split them out.

C – Against declaring user ID between two SSIDs/ESSs.

Soft APs - nothing we can do but could make a recommendation.

C – Soft AP is still an AP.

4.12 Onboarding a known MAC address

C – Just do not use MAC address. SAE password identifier can solve this.

C – Use case is schools allowing students to connect to portal. Registration in advance so only thing they work from is the MAC address.

C – Excellent example when not to use MAC as identifier.

C – Is the idea we use this document to explain solutions? If we feel there is a solution already in the standard, then should we point this out more formally?

C – WFA do publish performance guidelines. Do support we do explain and documenting this correctly.

4.13 Customer Support and troubleshooting.

C – One case that RCM breaks badly is the enterprise case. Need to know same device over different days.

C – Maybe we do nothing at dot 11, but suggest at IP 6 layer, DHCP, for example.

C – 4.21 DHCP pool exhaustion came from WBA.

C – Worried when we say we do nothing and rely on others. We are the front line. Could devalue our position. If we can do the work, we should.

C – Should not be supplying a solution that only works with IPv6.

C – Believe IETF has identified DHCP as suspect and is addressing. If someone has a service problem, they should have an identity on the network that ties it back to the MAC at the time. Typically, pre-association i.e., trouble connecting. Rather than performance.

C – Using MAC is easier and tracking of device is also used and needed. It is an important problem

C – Customer support, need diagnostics on device side and this is the only way to solve it.

General

C - We should look through list and decide if an Annex is required with explanations.

C – One of our updates may be simply an informative Annex.

C – Are there any similar Annex already? Mostly examples

C – Two I can think of, interworking (Annex R) and TDLS. Not recommending we entirely go down this route.

C – Could modify PAR into Recommended practice.

C – Not entirely clear when we say this is our problem or not. Need to look into perspective of what we could do and what if market develops something we don’t like but at least can prevent the worse of two solutions being picked.

C – Better in Annex than a Recommended Practice document.

C – Noted that several Annexes have sub sections with recommendations.

MAC Address collision

C – very low probability

C – Out of our scope, we look at problems with RCM not how to do it. Any volunteer to respond on this to WBA?

C – Has this ever been observed?

C – Have seen 3 examples. City wide in Singapore. Seen same address on different sides of the city. We can agree there is a chance this can happen, but 802.11 does not define how MAC is selected. Probably more randomization scheme.

C – This is a dot 11 response not TGbh

QoS and QoE (WBA)

C – Forcing clients into particular QoE. Similar to case 4.2. Action to ask WBA further questions.

DHCP pool exhaustion and DHCP address assignment

4.23 ACLs

C - similar to previous but WBA pointed out may be IP based.

C – Using MAC based ACL for blacklisting clients. So is something that should be addressed. Don’t know of an IP based ACL.

C – In my opinion must not be part of our scope.

1. **Other business:**

**Timelines as per Slide 26.**

Any comments or concerns? Think we are on track

**November Plenary Session Plan Slide 21**

Will be held remote.

3 slots, any comments?

**Teleconferences Slide 22**

3?

C – Suggest we add one more, we have not had any technical presentations.

C – Avoid Golden week in China

**Any other business?**

None

Out of time

**Adjoined at 11.01 am ET**