IEEE P802.11
Wireless LANs

|  |
| --- |
|  TGbi Minutes Electronic **Plenary Session 7-15 Mar** 2022 |
| Date: 2022-03-11 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Amelia Andersdotter | Sky UK | Brussels, Belgium |  | amelia.ieee@andersdotter.cc |

Abstract

This document contains the minutes for the IEEE 802.11bi task group meeting that took place during the IEEE 802 Electronic Plenary Session 8-12 November 2021.

Note: Highlighted text are action items.

Q – proceeds a question

A - proceeds an answer

C - proceeds a comment

Yellow highlight - action point

**Chair: Carol Ansley, Cox Communications**

**Secretary: Amelia Andersdotter, Sky UK**

**Vice-chairs: Jerome Henry, Cisco; Stephen McCann, Huawei**

**Technical editor: Po-Kai Huang, Intel**

**1st slot. Wednesday 9 March, 11:15 ET.**

Chair calls meeting to order at 11:20 ET.

Agenda slide deck: 11-22-273r0:

1. Reminder to do attendance.
2. The chair mentioned the call for essential patents
	1. No one responded to the call for essential patents
3. The chair covered the IEEE copyright and participation rules.
4. **Discussion of agenda 11-22-273r0 (slide #17)**
	1. Request to add 11-22-463r0 to the agenda by Duncan Ho (Qualcomm).
	2. Agenda approved as amended, by unanimous consent (102 participants).
5. **Administration**
	1. **Motion #9:** Approve previous minutes

Approve the minutes for:

2022 January 802.11 Electronic Interim: 11-22/164r1,

TGbi Teleconferences: 11-22/318r1, 11-22/409r0, 11-22/410r0

Moved: Jerome Henry

Seconded: Amelia Andersdotter

Approved by unanimous consent (105 participants).

* 1. **Timeline**
		1. We are currently on target with issue document motion passed (see 11-22-409r0 minutes).
1. **Presentations**
	1. **Initial Privacy Enhancements Requirements (11-22/107r2),** Philip Hawkes (Qualcomm)
	After discussion requirements are now split into Client privacy enhancements (CPE) and BSS privacy enhancements (BPE).

**Discussion:**
**Q:** Slide 5 has a list of features, and some of them are not being addressed in the client PE. Is this something you're waiting to address in a later set of requirements, or is this the full list of features already that you're presenting?
**A:** These are the set of requirements that we want to focus on, so we're not necessarily saying there are no other requirements possible - we're not presenting any solutions to Issue 7 or Issue 8, for instance, but we're open to having solutions presented for those issues by other people.
**C:** I think Issue 7 and Issue 8 are important and maybe we can work together to identify similar requirements as you've done here.
**Q:** On slide 5, again, in requirement CPE-C, it addresses issue number 3, don't you think it's also related to issue 6? Because of the simultaneous MAC switch issue, where if all devices don't change MAC at the same time you can still track someone?
**A:** You have a point. The way we've done the division of issues here this was only part of our CPE considerations, but it needs to be a BSS privacy enhancement as well.
**C:** So I think we already have agreement that the MAC addresses need to be simultaneously rotated in the BPE case.
**C:** If an AP changes BSS to avoid being tracked, and all the clients do the same but there is a legacy client, that might expose the PE clients to privacy risk. So I think it makes sense what you're saying that a legacy device should not connect to these new BSS.
**Q (from technical editor):** I want to have a clarification, that in many of the requirements presentations we're now converging on "PE" (privacy enhancement) for describing new features, but in the Chair's presentations it's still "EDP" (enhanced data privacy). I'm just looking for a clarification on this.
**A (chair):** We've talked about this. The Working Group chair indicates that she prefers "EDP". I have no strong interest either way.
**C:** We don't need to worry about this detail at this point.
**C:** I agree.
**C:** We are stuck with EDP from the PAR but I personally believe we can use whatever in the draft text. The technical features we're developing are more PE than EDP in my view. However, I do also agree we should not worry about this detail at this point.
**C (Working Group Chair):** I agree with the direction of this discussion: let's understand the direction of the features we're developing and name the feature later. The name for the feature should be aligned with the feature and does not need to be aligned with what is in the PAR. The name in the PAR can be changed, so we would only submit a PAR update at that time. What should be made is progress on the technical content, rather than spend time churning the adjustment of a name.

Phillip Hawkes has dropped from the call and is intending to return, but queue is discontinued for the time being.

**(re-opened queue after Phil rejoins at 12:45ET)**
**Q:** I thought there is no cover for the situation where not all MACs are rotated at the same time. If the third-party can track any BSS participant it can track the whole BSS. There are also other parameters associated to the BSS that we should look into to make sure no ancillary parameters go over the air that can be tracked. Like TWT agreement or membership for isntance.
**A:** OK, I'm making notes.
**Q:** I'm wondering if we for instance could get rid of words like "easily" and other superlatives, because it's a bit confusing to me.
**A:** Just to explain the rationale for having these words here at the moment. We've looked at various solutions for hiding the SSID. There seems to be a trade-off between how complex the solution is and how easy it is for the attacker to identify the ESS. So some of our solutions had certificates or asymmetric crypto, stuff like that, and this can provide good protection against the identification of the ESS. But. It's not without a cost. there's quite a lot of operations that need to be performed either on the AP side, mostly actually, or on the client devices. Every probe request would require the AP to perform an asymmetric operation before it even knows if it's a genuine request, and that's fairly burdensome. We have some other solutions that make it less directly obvious what the SSID is, but it doesn't take too much computation for an eaves-dropper to check if they already know what to look for. Somewhere in the middle I think we need to make a trade-off and that comment was already made. Not everything here has the same benefit, and some thing will be too complex to be worth it. Particularly for this feature, the benefit we're looking for is increasing the complexity of performing the attack, but maybe we can't accept however much complexity at all.
**C:** I agree that there is such a trade-off and that we need a discussion on our aim here. A very simple privacy thing would be not to provide any OTA from the AP at all, encrypt also beacons and things. We could compare with things like bluetooth, where we already encrypt bluetooth in a lightweight manner. Maybe we could do this also for APs in these cases?
**Q:** Some things cannot be protected like the AID and other things and so we're saying that if we can't change the identifiers we should rotate them. But in general I would say when we're moving into the privacy of post-association, we probably just protect parameters with PMF right? So what I'm reading here is that we should rotate the PHY headers, AID, and we start by rotating identifiers that can't be encrypted?
**C:** So when I mentioned TWT agreements and membership I was assuming that the frames will be protected, yes. So we have an AID and it will always be there in the trigger frame. If you change to a different MAC address the TWT agreement is not being changed, so we'll have to somehow compensate for that. The trigger frame is periodical so it can be fingerprinted.
**C:** But you're saying that tracking could be done here even when there is no other parameters known by a potential eaves-dropper?
**C:** Well yes because it's a periodical trigger frame so there's a pattern to be identified.

* 1. **(Re)association Protection for 11bi (11-22-463r0),** Duncan Ho (Qualcomm)

**Discussion:**

**Q:** Firstly, the question we should ask from a requirement point of view, do we really need to protect everything in the association frame or only some things? Are there some things we want to leave out? I don't know the answer but my gut feeling is that your proposal here is a hammer solution. Secondly, I'm also wondering if we have a better approach to this that's maybe less heavy-weight and that also addresses the same issue? I also don't know the answer here but I think we should look at it. Lastly, if we are going down this approach we should look at WiFi Easy-Connect as well because it's another association mechanism that we would need to cover through this work.
**C:** Easy-connect, isn't that DPD though?
**A:** To your two questions, we're trying to re-use mechanisms that are already existing in the .11 specs so this is the point.
**C:** I agree with that, it's just that putting them together like this makes it quite heavy-weight.
**A:** Agree, so our reasoning here is that we're also trying to make things future-proof.
**C:** But are we then addressing privacy and security? We're doing privacy here, not security.
**A:** To me, security is a route towards having privacy. And it also seems more convenient not to have this selection of stuff that we should encrypt, not encrypt, etc. It makes for an awkward selection procedure.
**C:** I'd just like to see it better mapped towards our requirements though.
**Q:** I think this direction looks promising. Related to the previous comment, I would say that we have so many potential fingerprinting problems that picking or choosing which elements could contribute to the entropy isn't really possible at this stage. Encrypting everything and going down this route seems to me to be the only way to provide this holistic approach that we're looking for. Now, within the PASN authentication phase we could need to protect EAP exchanges and PKMIDs - maybe we have individual solutions for at least those, and we could go through. Is it the case that you're imagining PASN key hierarchy to be re-used in re-associations too?
**A:** Yes.
**Q:** With these symmetric key approaches, we trade off computational complexity but increase storage if we end up with scenarios where APs cache keys for long periods of time. I see a few places in your slides where you could do SAE every time and not have to cache and this would reduce complexity. But we should check if this increases the burden on APs to store keys, in my view.
**A:** Agree that we could look in to.
**Q:** You mentioned that your plan was to have restricted PASN to restrict fingerprinting opportunities. But PASN is coupled with PKMID so you would already have something with which to fingerprint, is that not the case?
**A:** I thought there were already solutions for this around that maybe we could add here.
**C:** If that's the case, that's how it is.
**Q:** I support the general direction of this as well. But two questions, if I recall correctly the authenticator or AP side derives the PTK from the first message, so if this is the case isn't it true that you don't need the third message really? I think this is the case for at least PKMID and that maybe we need this tweak.
**A:** At least my intention is to re-use PASN as much as possible. And I've understood it's always a three-way handshake so we can't remove the third message. But you're saying it's not the case?
**Q:** Well, currently in PASN you derive the key after the first message…
**A:** I will look into this further, but you could be right, yes.
**Q:** To me this seems like a lot of messages. I don't think you need all of this complexity for the hand-shake. After beacon you can open association request and response and just allow the STA and AP to exchange the four-way handshake to create the PTK and GTK kind of stuff, then use the current one whatever that is. Do the real association and encrypt those requests and response so you don't need to change AKM.
**A:** So you say do open, then do another association encrypted with those?
**C:** This is correct, that seems to me a smaller change.
**A:** I can look into this alternative, yes.
**Q:** It's an interesting and thought-provoking proposal. I like that this addresses a key drawback of the 802.11 architecture that we're using data frames for authentication. So we should be moving the authentication into authentication frames. But we need to really ensure that after authentication and association are done, we should fold the four-way handshake into something like association frames. What I don't like about PASN is that SAE is already quite heavy-weight, but PASN is going to do another Diffie-Hellman - why? So an improvement here I think is that we just acknowledge that we need a good PTK. If we want to start extending AKMs then we can do that, and the KDF can churn out another set of keys if we want. Another thing about PASN is that it doesn't support all the features of SAE - it doesn't support denial of service and also doesn't support FILS public keys. If we're anyway doing two Diffie-Hellmans then why not just support FILS public keys. And a question: this will not work on DMG STAs, right? Because they don't do authentication? Or do we impose on DMG STA to do authentication now?
**A:** I will check.
**C:** I made some notes here and will try to answer in order. Firstly, I think the benefits of having this security towards privacy approach is in everyone's interest so I think that is justifiable. We're proposing this to enhance privacy but it also improves security. As far as the Wifi alliance work progresses, sure. In other mechanisms, we are trying to replace the four-way handshake so yes. On dropping the third handshake in PASN, the Diffie-Hellmans are in the first two exchanges so that makes sense. On the last point, we may want to change PASN more of course and we're open to doing that. Moving the key generation and exchange to before association is really the point here, and it's not super-relevant for us what exactly we call it - we could call it something other than PASN of course. PASN also isn't the main point we're trying to get at here, it was just convenient and already there. It may be more convenient to just look at SAE separately, of course, but would certainly not be adverse to looking at that. On the FILS public key comment, it's the same - if we have that in authentication frames that's also fine. On DMG STAs, they can use authentication frames for SAE so I think that's already solved, and the key point is that we have agreement on whether to encrypt all the things in the association the way that we propose here.

**Go back to point 6.1 for continued discussion on 11-22-107r2 (12:45ET).**

1. **Review of requirements introduction procedure (11-21-1848r2) Carol Ansley (Chair)**We have a procedure for approving requirements inside the group.

Requirements in 11-22-107 will be straw polled in entirety. We'll track them individually as well.
2. **Recess at 13:12 ET.**

**2nd slot. Thursday 10 March 2022 11:15 ET**

1. **Call to order 11:17 ET.**
2. **Reminder of policies, procedures, attendance (see also point 2-3 above).**
3. **Review of agenda 11-22-273r2 (slide #17)**
	1. No comments on agenda. Unanimous proposal (42 participants).
4. **Review of document 11-21-1848r3 Requirements Tracking, Carol Ansley (Chair)**
	1. Revision 3 has been produced and updated with requirements presented, including during timeslot 1 of this plenary session.
	2. It would be helpful with more references to the date when requirements were presented.
	3. The document numbers for requirements should also be included.
	4. Question on sorting: by issue addressed? Could help in identifying conflicting requirements.
5. **Presentations**
	1. **Enhanced Randomized and Changing MAC Address (ERCM) (11-22-114r1), Stephane Baron (Canon)**Previously discussed in January interim session (see point 11.2 in interim minutes document 11-22/0164r1). **Discussion:
	Q:** Two things. Firstly you already have a mechanism for simultaneous change of MAC address, but we need this only for the mobile AP case, correct?
	**A:** The AP and non-AP STA can both request the computation of a new identifier, to be done simultaneously but the language here should be clarified you're right.
	**Q:** Secondly, on bullet 4, slide 4, what is the duration of this period when the identifiers are simultaneously valid?
	**A:** Well, there is a need to make sure that old transmissions that were done prior to the switch can still be delivered so there may still be some time period when both identifiers are valid. Two unicast MAC addresses will be decoded by the PHY during this transition period, but there will need to be some form of time-out period here that permanently deactivates the old MAC. It's absolutely NOT the intention that we'll just be switching back and forth between old and new computed MAC, it's just a transition.
	**C:** So I think step 2 in slide 4 is the critical aspect here, then.
	**A:** But before I go deeper into here I'd just like to know that more people think this is a good direction, so that feedback is what I'm looking for with the group here.
	**Q:** You have a calculation formula for the MAC addresses, right?
	**A:** It's based on a random number generator that is already available, and the formula is only that we use the old MAC to compute the new MAC. So that's it.
	**Q:** So then you need to be in sync on how many transitions there have been in the past, so that you can reach the current MAC address, correct?
	**A:** Yes, that's why we count the number of beacons so that we can synchronize the AP and non-AP STA.
	**Q:** I think this might be a good idea. Let's say we know how many transitions there have been, is there a way that we could just immediately calculate the current MAC address based on the original seed for the random number generator without having to go through all of the iterations?
	**A:** Could look into.
	**Q:** Have you also looked into a formula to calculate the next change time?
	**A:** If you look at slide 9 we have this counter value. Does it address what you're looking for? We're using an RNG for this as well so that the counter does not initiate a change at periodical intervals. It is a calculated value with a seed and output, but the first change might occur when the counter is at 4, and the second when the counter is at 6 or 7.
	**Q:** So we could make this an autonomous process that just keeps running and running?
	**A:** Yes, that's the idea.
	**C:** Sounds like a good principle to me. The scheduling and the calculations that you're proposing here make sense to me the way that you've been presenting them.
	**Q:** Have you thought about if extending the STA to be an MLD STA? Would that still work?
	**A:** We didn't go into detail for the MLD STA. But I think we could just do the same mechanism for the MLDs on both the AP and non-AP multi-link side. We could apply it separately even on the logical multi-link level or for each of the components of the multi-link.
	**Q:** When you said there's a random cascade of changes vs everything changing at once. Isn't it true that if everything changes at once it's more difficult to track? If you're recording the traffic you'd see one MAC address stop and another start?
	**A:** I agree that if all the STA change their MAC address at the same time it will be a real mess from the outside. We should consider all these situations which is why we're proposing this mechanism. Changing everything at once creates a computational pickle for the AP though, so we'd make some trade-offs there.
	**Q:** I want to understand the dynamics of the data frames going out as the address changes. Given different parties and queueing delays, over-the-air as the change happens you'll have different frames that go out, right?
	**A:** Yeah, if you have queues for uplink STA or downlink AP then that could be the case that you have new and old addresses, but not exactly at the same time. The fresh MAC address is always used for any new traffic. We're using also that the transmission is omnidirectional, so when the STA responds with a new MAC to a transmission from the AP using an old MAC, it will not be obvious to whom the STA is responding or why.
	**Q:** But you're not expecting re-addressing of already queued frames right?
	**A:** I'm not really in favour of that, no. So you talk about having several queues and we should consider this. Probably we change some stuff to give priority to the old MAC-queues for transmission, and that's that.
	**C:** So the AP and over-the-air load will be affected negatively if you do this sort of prioritisation change though.
	**A:** We can compare different mechanisms here, we're happy to do that.
	**Q:** So a previous question raised if you really need to iterate though all the MAC. Could we use just the original MAC and just a counter? For computing the OTA MAC?
	**A:** Yeah, the only thing is we need a different value over time. It could also be number of seconds or whatever.
	**Q:** So I'm wondering if we could use two parameters instead of one.
	**A:** We didn't want to change the number of arguments in the function since it's already standardised.
	**C:** Concatenate two arguments perhaps into one.
	**A:** That's certainly possible. This is helpful.
	**Q:** When does the MAC address get appended in this changing MAC address world? Just because things are sitting in the queue waiting to become PPDUs, doesn't mean they've been assigned a MAC yet. Should we look at this when we deal with this? I don't think this is as big of a problem as was previously alluded to. I could see MAC being appended after the access queue and being popped out to the PHY.
	**A:** There may be frames that need to be retransmitted or something, but we could see also with different vendors when addressing is being done. Until now we didn't really have to ask this question but you're right we might need to raise it now.
	**C:** It becomes an implementation question and how the queues are managed, etc. I agree that change in MAC address for retransmission is a pain, that would complicate matters.
	**A:** As long as an already addressed frame, however that was done, remains addressed the same way I think we could be heading for fairly simple rules here. But we need this discussion, and we need the input of vendors on how they have issues here.
	**C:** I have some comments on this retransmission queue issue. I want to be able to implement this in existing devices so for me I'd be a priority to have this implementable in general. Having multiple MAC addresses and prioritising queues and such has large implications, potentially, especially if these changes of address happen several times per minute rather than once per hour. Let me come back on this later though.
	**Q:** Are you having a separation here between the over-the-distribution system MAC address and the over-the-air MAC address? What happens if two non-AP STA are having a direct link between them in same BSS?
	**A:** We only consider in this case RA and TA. AP communicating with a STA. We're not considering sending things to the internet, etc, and that's a different issue with a different solution. On the other QoS comment above, and the frequency of rotation, that is an issue too that we can discuss - should the AP or the STA decide and we'll just need more discussion on this.
	**C:** There are frames where the SA and DA are in the same field, and so we'll need to go through all the frame fields here and check what the implications are of changing. So that's the first thing I'd like to raise, and also the use of TDLS.
	**A:** We didn't consider peer-to-peer transmission and TDLS cases, so different mechanisms may need to be used there indeed. TDLS sessions will simply just be broken if two non-AP STA rotate their MAC address I think.
	**Q:** So the DS side of the world sees the "true" MAC address, correct?
	**A:** For a given period of time the AP might see the true MAC address.
	**Q:** But the AP always has to know the "true" MAC address when it's bridging, no?
	**A:** Let me think about this though.
	**Q:** Do you have any thinking on acknowledgements and how they will be transmitted?
	**A:** To avoid too much disturbance of the acknowledge we should use the same MAC as was used to receive the package, in my view.
	**Q:** What about BlockAck across transmissions?
	**A:** We should avoid that. Acknowleding for different MAC addresses in the same Block seems very impractical so we need a separation mechanism there. We'd have different BlockAcks for different series of transmissions.
	**C:** That will be some implementation challanges. Hours of fun discussion!
	**A:** Indeed I just wanted to know if this was generally a good direction to work in, but there's for sure a whole host of issues like sequence numbers etc.
	2. **Proposed .11bi Requirements (11-22-109r3), Po-Kai Huang (Intel)**This was previously presented in the January interim session (see point 17.1 in interim minutes in document 11-22-164r1).

	**Discussion:
	Q:** In issue 2 for the requirement, the word "protect" do you mean encryption or something else?
	**A:** I use protect because I think encrypt is too specific. The Frame Body field needs to be "protected" but I'm not sure encryption is always the right way here.
	**Q:** So what is the word protect meant to imply? Is it open for discussion in this case?
	A: The intention is that we have a consensus for somehow hiding the Frame Body field from third-parties, and different thoughts in different directions. We know that there should be a choice to "protect" this entire field, not just individual elements, but we may not know yet that this protection consists in encryption. But we saw presentations also yesterday that went in this direction with encryption.
	**Q:** So this document serves something like an SFE type of thing, the type of work we need to do. So we should then be more specific on the things that actually need to be done, rather than just putting the TBD on them. That helps to weed out the action items. Since "protect" already has a specific meaning in our standard, and "encryption" also is well-understood, I would rather see that clarity here with respect to what we actually want to do.
	**A:** For me the TBD here is less urgent since it's not a spec writing time.
	**Q:** I do not understand clearly how these requirements are presented. To me a requirement should say what we're creating solutions towards, while your requirements seem much closer to the solutions you want to see. If you see on slide 6, for instance. You're giving a solution to a requirement. I'm agreeing with what you're trying to say, but I don't think requirements should give solutions.
	**A:** Thanks for that feedback, I understand this. I can look into this.
	**Q:** I would like for these requirements to be narrowed down to just address privacy rather than going into the specifics of every element privacy.
	**A:** On element fingerprinting I think it might be really difficult to speak only about address privacy.
	**Q:** I have a more general question on what the difference is between the work of this group and TGbh with respect to requirements of randomized MAC.
	**A (Chair):** So TGbh is trying to quickly give an option for different actors to work around negative impacts of MAC randomization while we're trying to look at larger issues of reducing harmful privacy exposures. So they're looking at adaptation to an existing situation, while we're working on improvements.
	**Q:** Separate from the MAC stuff I understand this group, information elements, OK that's fine. But with respect to the MAC I don't really see the difference.
	**Q:** I agree with the previous comment that some of these requirements are a bit too specific.
	**C (Chair):** So just as a comment, all of these requirements are just being proposed at the moment so we can have that perspective on things too. They may still be narrowed down. Maybe our next exercise is narrowing down these requirements, and run several strawpolls, etc, to get to that place. We finally need to motion them by July by our time-line.
	**C:** I think this level of requirement is absolutely fine. It will help our technical editor structure the basis for a draft later and in other groups we do not have this problem with narrowing down the solution space. In my view having requirements at this level will help advance our work more quickly, and I don't see the problem at all.
	**C:** I agree with the last comment.
	**A:** I would like to run a straw poll.
		1. **Strawpoll**: Do you support the following requirement?

"11bi shall define a mechanism for the 11bi non-AP STA to refrain from transmitting Probe Request frames containing elements except TBD element(s)"
Y: 15
N: 7
A: 14
N/A: 27 (63 attendance)

1. **Teleconference schedule**
	1. Meeting every week? Should we continue with this cadence?
	2. No meeting for 17 March 2022, but following 17 March 2022 will cover every Thursday 9AM ET before TGbe.
2. AoB?
	1. Cancelling Friday plenary session.
3. **Adjourn at 13:08 ET.**