IEEE P802.11
Wireless LANs

|  |
| --- |
|  TGbi Minutes Electronic **Interim Session 9-17 May** 2022 |
| Date: 2022-05-18 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Amelia Andersdotter | Sky UK Group | 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 Interim Session 9-17 May 2022.

Motion results and counts verified against working group voter list on 17 May 2022.

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 Henri, Cisco; Stephen McCann, Huawei**

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

**1st slot. Wednesday 11 May 2022, 11:15 ET.**

Chair calls meeting to order at 11:17 ET.

Agenda slide deck: 11-22-0606r0:

1. Reminder to do attendance. Reminder to register for the session and to not attend the virtual meeting without paying appropriate meeting fees.
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 11-22-1974r1 (slide #17)**
	1. Agenda approved by unanimous consent (57 participants).
5. **Administration**
	1. **Motion #10:** Approve previous minutes

Approve the minutes for:

2022 March 802.11 Electronic Plenary: 11-22/481r0,

TGbi Teleconferences: 11-22/628r1, 11-22/664r0, 11-22/665r0, 11-22/698r0

Moved: Jerome Henry (Cisco)

Seconded: Kurt Lumbatis (Arris/Commscope)

Approved by unanimous consent (60 participants)

* 1. **Motion #11:** Vice-chair reaffirmation

	Current vice-chairs are willing to continue serving the group. No further nominations.

	Reaffirm Jerome Henry and Stephen McCann as TGbi vice-chairs for two years.

	Moved: Amelia Andersdotter
	Seconded: Dan Harkins

	Approved by unanimous consent (62 participants)
	2. **Motion #12:** Recording secretary reaffirmation

	Current recording secretary willing to continue serving the group. No further nominations.

	Reaffirm Amelia Andersdotter as TGbi recording secretary.

	Moved: Po-Kai Huang
	Seconded: Jarkko Kneckt

	Approved by unanimous consent (64 participants)
1. **Technical Presentations**
	1. **Enhanced Randomized and Changing MAC address (ERCM) (11-22/0114r2),** Stéphane Baron (Canon)

Discussion:

**A:** On slide 5 the ECRM Key is sent from the non-AP STA to the AP. Why don't you use an already established key?
**A:** We could re-use existing keys but the question is whether we should be re-using keys that are mainly used for some other purpose. Usually we have keys established to encrypt data communication, right, but here it's to generate a MAC address, so that's why it's a new key.
**C:** I agree that we shouldn't re-use keys derived for one purpose for a different purpose. But when we do PTSK we already generate keys, and new keys can be generated by the non-AP STA or the AP without having to find a way of protecting the exchange you're showing here.
**A:** It's a good comment.
**Q:** What is the benefit of this compared with just changing the MAC address randomly? It seems very complicated for something that could otherwise be simple.
**A:** The point here is that we get rid of the frame requesting a MAC address to be changed, and that would make it more difficult for an observer to intercept that a MAC rotation is about to happen. There's no transmission so you can't even try to guess when or where the MAC address will be changed.
**C:** But if you have an RSNA you can still send your MAC address and it's secure?
**A:** That's true.
**Q:** Do you signal here when the MAC address change will occur?
**A:** It's an option.
**Q:** Is this specifically for post-association rotations or do you see it as being used cross-associations too?
**A:** It's designed primarily with the post-association use-case in mind, but some of our requirements also address this roaming situation.
**Q:** So I want think we may need to think more about these change address time and how to synchronize initiations of a MAC address change?
**A:** We already have this discussion in the past if I remember. Some people feel that we sometimes need to change everything at the same time, but it creates a computation problem for the AP if there is a very large burst of MAC address computation requests. We could support both the case of gradual and simultaneous MAC address, so that the AP can make the best choice to protect privacy in a given situation.
**Q:** In my opinion the most important thing for requirements 7 and 8 is the transition period and what happens there. We're going to have an old address and a new address in this transition period between addresses and the AP needs to manage this somehow, TX, re-transmission, etc.

**A:** On requirement 6, I think it's true that we can address this at this stage but our current proposal would be compatible with requirement 6. For the requirements 7 and 8, you're right about the salient point: how is a MAC address changed without breaking existing communications? I think when a STA will use a new MAC address, then the STA will take the time it needs for that.
**Q:** What's the advantage of using the previous MAC address? Is it to do with making it harder to re-synchronize?
**A:** The random number generator needs a changing parameter to compute the new MAC address, so using the old MAC address is one such parameter here. Different parameters could be used, though.
**Q:** Going back to requirements 7 and 8, I think we need to support the case where the non-AP STA requests a MAC address change. So isn't the most simple and straight-forward solution here to use a frame request and response?
**A:** If we set up a mechanism for regular or randomized change of MAC address then I think it can be re-used for initiated changes as well. I think that has been discussed briefly in TGbh as well.
**C:** My thinking for now is that we might want to reduce complicated signalling.

**Q:** I'm wondering about the counter on slide 8.
**A:** Your point here, is that the counter is public information, right?
**C:** Yes.
**A:** So there needs to be some way of communicating between parties to initiate a simultaneous MAC address change, and this counter can either be communicated in encrypted form or in public.
**Chair:** Do you want to run your strawpoll?
**A:** Yes. I think I already have a pretty good idea about the temperature in the room.
**C:** This seems like a pursuit of high-level direction, and I heard a lot of questions on specific implementation details. So I think the high-level direction of having two associated entities change their MAC addresses on certain times without signalling that change, I think it's an interesting concept.
**Q:** I have a question on the strawpoll - do you want to know if the options specifically presented in this presentation, like on slide 9, are interesting or is it really a high-level idea?
**A:** There are a lot of details that can still go either way. This strawpoll is more about the general idea of using pseudo-random MAC address changes without signalling the addresses, and we can discuss if synchronization should happen through beacons, frames, or some other ways. I do think I already understand the general feeling of the group, but to go further with inquiries in this direction.
**Q:** Would this strawpoll preclude other solutions?
**A:** It's a strawpoll so it doesn't preclude anything at all. It's just polling on whether this line of pursuit is worth taking further.
**Q:** Could you specify that it's for post-association?
**A:** It's not a problem for me.
**Q:** Isn't it the case that we've already agreed that we will do post-association MAC address changes?
**A:** Yes, but this strawpoll goes a bit further and asks if changing the MAC address without exchanging it is a good idea.

**Strawpoll:** Is there interest within the 802.11bi WG to pursue the idea of defining and specifying the use of a pseudo random generation after association of OTA MAC address without exchanging it?

Result: 27 **Y /** 5 **N** / 9 **A** / 31 **NA** (total 72)

1. **Review of proposed requirements from document 11-22-1848r7**
	1. **Requirements related to issue 3 (cont. from 11-22-0698r0 p. 7.2)

	Chair:** We had previously covered some issues under issue 2, and went ahead with issue 3.  **C:** The proposed requirement 9 may need some small rewording.
	**C:** I have a personal problem with requirement 9 - this requirement is fine, but I feel it shouldn't be sorted under issue 3 (MAC address permanence within a ESS), or if this is actually a broader issue.
	**C:** For me I'm not really sure what we're talking about here, since the spec already says that scramblers, sequences, etc should be re-set when the MAC addresses are randomized. Did I miss something with this?
	**C:** I thought that we are adding this because we're dealing here also with post-association, while the current spec test only covers pre-association.
	**C:** So I think it brings us to this issue that we're actually splitting the concept of a MAC address, one which is in the distribution system and the other which is over-the-air. It could be that we have other places in the standard would be less interpretable given this new split too. We'll have to come back to this at some point in the process, is my assumption.
	**C:** Then I'd propose the requirement should cover also scrambler seed.
	**C:** We're also working on requirements for the scrambler seed.
	**C:** I understood we'd put in more conditions, that it should be the CPE Client that changes these parameters, for instance.
	**C:** What is the relationship between these requirements and the behavior within an ESS?
	**C:** That was my previous point too, that I think this is more related to issue 7. But some people feel that this is also related to issue 3, since this is related to values that are changed when you change the MAC address.
	**Chair:** I will mark the reworded requirement 9 as ready for motion.
	**C:** I think requirements 10 and 11 also should be sorted as issue 7 in addition to issue 3. Also it should be clarified that it's the CPE Client that changes its OTA MAC address in the requirement in question.
	**Chair:** I will mark the reworded requirements 10 and 11 as ready for motion. This is also a reminder that we will be running these motions on Friday of this week.
	**Chair:** I will mark requirement 12 as ready for motion.
	**C:** I believe it should be explicitly mentioned that the private MAC address is carried for the distribution system.
	**Chair:** I will mark the reworded requirement 23 as ready for motion. [secretary's note: see p. 13.1 below]
	**C:** I have the same comment for requirement 24 as for requirement 23. It should be clarified that it's the DS that carries a private MAC.
	**C:** I have an issue with defining the mechanism (protected (re)associated request frames) in the requirement itself. I think we could pretty much just leave it after the observation that it's in the DS.
	**Chair:** I will mark requirement 24 as needing further discussion.
	**Chair:** I will mark requirement 25 as ready to be motioned.
2. **Recess 11:15 ET.**

**2nd slot. Thursday 12 May 2022 11:15 ET.**

1. **Meeting called to order at 11:17 ET.**
2. **Reminder of policies and procedures (see para 1-3 above under 1st slot).**
	1. Reminder to do attendance issued, together with reminder to register for meeting.
	2. No response to call for essential patents.
	3. Reminder of policies and procedures.
	4. Copyright policy was presented.
3. **Agenda review (11-22-0606r1, slide #17)**
	1. Agenda approved by unanimous consent (47 participants).
4. **Administrative items**
	1. Review of teleconference cadence. Explore moving to 10AM ET when TGbe schedule becomes less intense.
5. **Review of proposed requirements from document 11-22-1848r7**
	1. **Requirements related to issue 3 (cont. from above p. 7.1)

	Chair:** We continue with the review of requirement 24.
	**C:** Some of us have discussed offline and produced a new proposal for what this requirement could look like.
	**C:** I don't understand the point of having a private MAC address for the DS. It doesn't seem to me that it conforms with the general goal of enhancing privacy either. Could someone explain this?
	**C:** My interpretation is that this is related to an ESS where you have a station roaming around between different APs and needs to have a stable MAC address over that association. Then you have an over-the-air MAC address that is visible to outsiders and it can be rotated to increase privacy.
	**C:** My continued issue with this is that this seems to assume that the only threat to privacy would come from outside of the network, while privacy includes a threat from the network to the individual. I think it goes against the grain of this group to have this sort of requirement. Maybe the task group bh could deal with this, which tries to find ways for networks to track consenting users. But it's not for this task group.
	**C:** I think a DS MAC address is needed for two purposes: in the roaming case, to forward traffic from the right client to the right destination, and because it's connected to the IP address. It's true that having a fixed MAC address allows some tracking but we also want traffic continuity.
	**C:** But this assumes that the attacker is only passively outside of the network. That is not the case. If a STA roams to another AP, even if you don't have a fixed MAC address that is secret, the worst effect is that you do a re-association, you drop some frames, but the traffic doesn't need to be interrupted. The IETF has also been working on this IP address and MAC address connection issue to deal with privacy, so we need to work on our side too. We're hoping to have this coordinated up and down the stack, but if we now introduce this trackable internal MAC address, especially if we justify it from the IETF, we're doing the opposite of consistent, endurable privacy management up and down the stack.
	**C:** If what we're doing here is introducing a fixed identifier, I think that should be fixed or reworded somehow. The other thing I heard here is that there is a scope issue and I think we need to take that seriously if requirement 24 is not in scope.
	**C:** I had the same thought. I didn't see requirement 24 as defining a sticky MAC address, in the sense of permanent, but more as a separate MAC address from the OTA MAC address. So you'd have two MAC addresses - one for the ESS that's internal and then another one which is transmitted as before OTA, but neither of them are necessarily permanent, at least not how I saw it.
	**C:** Now I'm even more confused. Is there a point to having two non-permanent MAC addresses?
	**Chair:** I will de-mark requirement 23 as ready to be motioned on Friday. Similarly, requirement 24 seems to be in need of further discussion. Our goal here was to weed out some uncontroversial requirements that we could use as a basis for our future work, and both of these requirements seem to be generating a lot of discussion. We can return to them at a later time.
	2. **Requirements related to issue 2 (cont. from 11-22-665r0 p. 6.2, 11-22-698r0 p. 7.1)

	Chair:** We had agreed that requirement 26 needed more discussion and were about to discuss requirement 27. Because we've now went through requirements 7 and 8 under issue 3, I think we are at a point where we can return to this.  **C:** I checked the spec on scramblers, relating to requirement 27, and it seems like this would already be automatically fulfilled. We already have a requirement in the spec text to reset seeds for scramblers.
	**C:** We had this discussion yesterday - the current spec text defines these things in pre-association, but now we're also talking about post-association resetting of parametres and scrambler seeds. To me that's a difference.
	**C:** Isn't there also an overlap with requirement 9? Then this would again be redundant. I also want to correct a misconception about the .11aq amendment that I hear floated a lot: what the amendment specified is that a STA needs to retain the same MAC address if it wants to refer to state that it established with that MAC address. There is nothing in the .11aq amendment that obliges a STA to use the same MAC address post-association.
	**Chair:** I will mark that it's already encapsulated by requirement 9 and mark requirement 27 ready to be motioned.
	**Chair:** Moving on to requirement 28.
	**C:** I would like to understand a bit more why we separate only sensing and data transmission? I think it's also the same with requirement 29 that covers ranging. So we have three different MAC addresses used for different purposes? And if one MAC address is changed do all of them need to be changed at the same time, and would we deal with timing, synchronisation and how?
	**C:** When I proposed this, the idea was to have different MAC addresses for different purposes to further obfuscate which STA is doing what at what time. It's in general more difficult to track a device if separate device instances are used for different purposes.
	**C:** I would like to understand what "sensing measurements" are.
	**C:** The sensing measurements are currently being defined by task group bf, but it might also be for instance the task group az location measurements.
	**C:** I'd still like to know why only the sensing measurements should be covered. There are many different kinds of measurements that go on so why not extend this?
	**C:** Well, .11ak measurements for instance are not so often repeated. Most other measurements that are available in the tool box are not instantiated very often.
	**C:** Ah, it's a frequency issue then.
	**C:** Yes.
	**C:** The assumption is that these measurements are different from measurements and associated reports that could be encrypted?
	**C:** Correct, we can use management frames and encryption to transfer the reports, but the privacy would be even further improved if we separated the addresses used for the measurement itself.
	**Chair:** I'm hearing requirement 28 might need more discussion?
	**C:** We can run a strawpoll tomorrow and have some offline discussions.
	**Chair:** I will mark requirement 28 to be strawpolled.
	**C:** On requirement 29 I think we can postpone it for later. I want to have more offline discussions with people about this.
	**Chair:** I will mark requirement 29 as postponed for later.
	**Chair:** Now on to requirement 34.
	**C:** I believe the plan here was only encrypted management frames, including beacons and probes, and ensuring that also these types of frames would be encrypted by the BPE.
	**C:** I recall that we already agreed on focusing first on CPEs, but this is a BPE requirement. So how is this for procedure?
	**Chair:** We have already covered the CPE requirement for issue 2, so we're now on BPE requirement. We can work through them and see if we have broad agreement on some of them. If that turns out not to be the case, we can move ahead.
	**C:** On the AP side there would be a lot of complexity involved in encrypting a beacon. Not that it's a bad idea, but the implementation would need to be reflected upon. We need some solution to be considered perhaps, first. The beacons are used for discovery so this really affects a lot of things.
	**C:** If this is approved, would an .11bc device have to encrypt everything or is this for a different use-case?
	**C:** I understand that if it was a BPE AP, that AP would offer a mode where privacy enhanced beacons are possible.
	**C:** Ah, so it's an optional development then.
	**C:** I think it's ok to discuss the CPE requirements first because they might be less controversial. BPE's in general would present more challenges technically. In general, in reference to the last question, some of the features defined here may not be able to be made backwards compatible, in the sense that applying the enhanced privacy functionality would disable some other features.
	**Chair:** I will mark requirement 34 as needing more discussion. I will also mark other BPE related requirements, requirement 36,37,38 and 42, as needing more discussion later. We can hopefully return to them in the upcoming month or two months.
	**Chair:** We can still discuss requirement 35.
	**C:** This is related to the mobile AP use-case. It's intended to protect the privacy of the devices that move along with a mobile AP.
	**C:** I think randomizing beacon transmissions will create legacy device issues and that we're back in the BPE discussion. We should postpone it for later. If a CPE does this unilaterally there will be some backwards compatibility issues, so this has to be, for technical reasons, a BPE issue. But then we again have legacy issues that we will have to deal with.
	**Chair:** I can insert wording in the requirement to clarify that it is the BPE AP that needs to randomize beacon transmission times, and mark requirement 35 as needing further discussion?
	**Chair:** I will mark requirement 35 as needing further discussion.
	**Chair:** We can discuss requirement 43.
	**C:** This is related to requirement 28 that we already discussed earlier. The requirement was intended to introduce PHY level protection for measurement reports, and maybe we can postpone the further discussion until later. I think this is a BPE level issue, and the strawpoll we'll be having on requirement 28 tomorrow, which is CPE related, will give more clarity on how to move ahead with this.
	3. **Requirements related to issue 4

	Chair:** We have two requirements for this issue, 13 and 14.
	**C:** I'm wondering if we don't need to clarify that these are SA and DA fields that are being sent in the clear.
	**C:** I have the question if the DS MAC address mentioned here is the same as the private MAC address we discussed earlier?
	**C:** Yes.
	**C:** So it's different from the OTA MAC address?
	**C:** Yes.
	**C:** There will be a MAC address in the DS that is used for IP address mapping, and that will be in the SA and DA fields as well, so these requirements are made to ensure that this information is protected from external eavesdroppers.
	**C:** I'm against these requirements based on the charter of this group not including the purpose of creating persistent identifiers to compensate for the randomized ones.
	**C:** I have an editorial remark, that SA and DA fields are not always present, so we may want to specify that these requirements only need to be fulfilled if the fields are actually there.
	**C:** I disagree that these requirements would not be within the remit of this group.
	**C:** I don't think these requirements cover the private persistent identifier that was discussed earlier. We have exposure of identifiers in the SA and DA fields specified currently in our standard text, so these requirements are meant to give us the space to deal with that. No matter how much we change the OTA MAC, if we have the SA and DA fields in data frames, we'll always be revealing information unless we make sure that plug this hole.
	**C:** I think we should then clarify that this requirement covers the protection of MAC addresses in the mentioned fields. The way they're currently written it looks like it would only be covering a private MAC in a DS. We could just as easily decouple a PKMID from the MAC-address by which it was generated, and then use that PKMID to roam around in an ESS, and I think that's a neater and more privacy-friendly solution than introducing this alternative permanent identifier that's been discussed here.
	**C:** We should clarify that these requirements cover the DS MAC address, and the SA and DA fields just happen to be the most prominent technical problems to overcome.
	**C:** Maybe we can put SA and DA fields at least as examples, if there are other problems that we need to overcome concurrently?
	**C:** Another approach is that we restrict the inclusion of fields in transmissions that we can't protect. We could drop the SA and DA fields entirely for those transmissions, for instance.
	**C:** "Protect" doesn't equate to "encrypt". We can protect by different mechanisms, including by dropping fields. So this should not have to impact the wording of the requirement in my view.
	**Chair:** I will mark both of these requirements as deferred for further offline discussion.
	4. **Requirements related to issue 5

	Chair:** We have two requirements related to issue 5. Both of them are already discussed and agreed ready for motion under out discussions related to issue 1, so we can move on. Requirements related to issue 6 are also all BPE related so we move beyond them.
	5. **Requirements related to issue 7

	Chair:** We have some BPE related requirements associated with this issue that we agreed to discuss at a later time, but perhaps we can start with the CPE requirements. Requirement 30 covers proposed CPE functionality.
	**C:** The second mention of "new value" is redundant.
	**C:** I again have the concern that we have to think about timing, synchronization, etc. We already had language on this in requirement 9.
	**C:** In my view this is not linked to a change of a MAC address, it's more general.
	**C:** I'm wondering what obfuscated TID would mean. The TID is a traffic identifier, so if we transmit an uncorrelated value that is obfuscated, what does it mean? How can we identify a traffic stream if we de-correlate values from the traffic?
	**C:** This requirement could be tied to MAC address change. That would make more sense.
	**C:** I think we should be careful about changing the TID when changing the MAC address, but obfuscating it as a different story. I don't have a strong opinion about this, but obfuscation seems to me to leave the opportunity for us to keep, in the background, the TID as it was.
	**C:** I think the difference between change and obfuscate is subtle. It needs some form of scheme to manage the thing anyway. If there would be a difference in that scheme, I am presently failing to identify it.
	**C:** I really want to have the TID not changed, because it's related to how we deal with encryption. Obfuscation is to me a much more acceptable language because it leaves it open for us to deal with what is transmitted over the air. But I would really prefer that we don't change the TID.
	**Chair:** I do not hear a consensus on requirement 30. I will mark requirement 30 as needing further discussion. We are now out of time for this meeting slot. The discussions will be continued tomorrow.
6. **Recess at 13:14 ET.**

**3rd slot. Friday 13 May 2022 11:15 ET**

1. **Call to order 11:19 ET**
2. Reminder of policies and procedures (see also point 1-3, 10 above).
3. **Review of agenda (11-22/0606r2 slide #17)**
	1. Agenda approved by unanimous consent (38 participants).
4. **Administrative**
	1. Teleconferences.
	2. TGbe will continue on Wednesdays and Thursdays at the 10AM ET slot. Mondays at 10AM ET would be possible for the TGbi group.
		1. Request: Avoiding conflicts with TGbf and TGme too? Conflicts noted.
		2. 10AM ET on Fridays proposed.
		3. Strawpoll: Please indicate preference for weekly meeting time:
		 Thursday 9 AM ET: 13
		 Friday 10 AM ET: 7
		 No answer: 25
		4. TGbi will stick with its current schedule of Thursday 9 AM ET for 1 hour, except when there is a conflict with CAC calls.
5. **Motion requirements marked as "ready for motion" by previous discussions

 Motion #13:** Approve the requirements marked as "To be motioned - agreed by unanimous consent" in doc 22/606r2. The requirements were approved at a range of dates.

 Moved: Jarkko Kneckt (Apple Inc)
 Seconded: Po-Kai Huang (Intel)

 Discussion?
 **C:** Would it be possible to have a list of the requirements that are actually now included in this motion?
 **C:** This list would be the one that is included in 22/606r2 - all the requirements marked as "ready for motion" in that document. But there is no self-contained list consisting only of the requirements that are marked ready for motion.
 **C:** Does the list of requirements being motioned include requirement 23?
 **C:** No.
 **Chair:** Do we have any further questions relating to this poll? I hear no further questions on this poll. I remind everybody that this is a motion, so only voting members can vote.

 **Results:**
 Yes: 19
 No: 2
 Abstain: 7
 N/A: 23
 Invalid: 3
 (54 people on the call)

 Motion passes.
6. **Review of proposed requirements from document 11-22-1848r7**
	1. **Requirements related to issue 4 (cont. from p. 13.3 above)

	Chair:** We will return to our discussion on requirement 13 and 14. Some revised text has been produced in offline discussions since yesterday.
	**C:** I continue to be unsure why we need to stipulate anything about the distribution system. We should be protecting things which are in the MAC header. That doesn't just go for the MAC address but for any information that goes in the third and fourth fields, and that should be our goal. If we want to refer to them as SA/DA fields, I guess that's fine, but it's not the important part of our mission.
	**C:** I believe this new text would cover both requirements 13 and 14 in one go. So maybe we could drop one.
	**C:** The client will not know anyway if something is "in the DS", so it's redundant.
	**C:** The focus of the requirement should be on what is our goal, that we are protecting client stations from exposing information that can be used to track them.
	**C:** The distribution system addresses are not really obvious to clients, and I think we can't really protect the structure of the MAC address as such. We can protect source address and destination address. I don't understand why we would need to drop the distribution system reference though, because it's something that is difficult for us to protect in any other way.
	**C:** One way to address this is to do MSD where DA is already in the data frame. But now we are talking about the fields themselves, do we need to encrypt them, or completely change the MAC header, or what? Mentioning the DA is fine with me.
	**C:** I thought that these fields can contain the MAC address, and I know that, but they might also contain other information.
	**C:** We need to mention explicitly that we're protecting over-the-air too.
	**C:** Personally I'm not comfortable mentioning fields, but SA/DA is fine.
	**Chair:** We currently have the following proposal: "11bi shall define or reuse a mechanism for CPE Clients and CPE APs to protect the SA/DA values from exposure OTA to 3rd parties". Did I understand that this might also negate the need for requirement 14?
	**C:** I do not believe requirement 14 is necessary anymore.
	**Chair:** I will mark requirement 14 as covered in the reworded requirement 13.
	**Chair:** I will mark requirement 13 as ready to be motioned.
	2. **Requirements related to issue 1 and 5

	 C:** I want to point out that SAE credentials are already protected against passive attacks, so I don't know what these requirements are doing here.
	**C:** My understanding was that this requirement was here to address the issue of protecting passwords identifiers.
	**C:** I thought this was about protecting over the air SAE password identifiers and PKMID. I sort of agree that there could be ambiguities in the specific wording of these requirements but this is what I understood that these requirements were meant to do. If we need to change to this later in I guess we can do that by repeating a motion with improved text, but my understanding was that this is about protecting OTA SAE PW ID and PKMID.
	**Chair:** These requirements are motioned and adopted, but if the wording is confusing or misleading we can accept submissions about reworded text. I would tend to agree that my understanding was also that they covered protecting OTA SAE PW ID and PKMID.
	3. **Requirements related to issue 7 (cont. from p. 13.5 above)**
	**Chair:** Yesterday we dropped the discussion on requirement 30.
	**C:** Will these requirements end up being mandatory? When we say here "shall define", that doesn't mean that the function will end up being mandatory to implement in the end. Some of these things will have a big impact on the station side power usage, and I don't think that these things should be mandatory to implement if only for that reason. That said, I do think it might be reasonable for us to define these mechanisms, even if they will not always be used.
	**C:** I continue to have no problems with the word "obfuscate". Obfuscation of the TID could very well be something that we should legitimately try to do.
	**C:** I think issue 7 is very straight-forward in that it invokes the MAC header field as a way of detecting behaviour, and that we need to make sure that these fields need to be protected. Specific technical implementations I don't think need to be within the scope of our requirements discussions for now - we're dealing with what we need to be doing, not whether they need to later be mandatory or optional. If "encryption" would suggest that we have a huge power consumption increase for end-clients, then maybe we can also use language such as "obfuscation" and see if there are technical solutions that are more power-efficient for that purpose.
	**C:** Are we moving into territory of requirement 31 now, with power-save?
	**C:** I think by analogy it could be argued for both requirement 30 and requirement 31.
	**C:** But what I'm wondering here is that we have this TID field, if it's 0 it's 0, if it's 1 it's 1. What can we do with obfuscation here if there is only one bit? I'm not even sure that this is feasible, but we're saying here that we "shall define", and I'm concerned we end up obliging ourselves to define something that just is not possible.
	**C:** Maybe this mechanism could be described by "encrypt/obfuscate" so that we leave ourselves the room for selection between different proposed mechanisms in the future? If we're doing encryption, I still don't think we can change the MAC headers. We can only add more payload and put these bits there.
	**Chair:** I will mark reworded requirement 30 as ready to be motioned. But I'm also hearing we need more discussion on this encryption and obfuscation issue.
	**Chair:** I will mark requirement 31 as needing further discussion.
	**Chair:** Moving on to requirement 32.
	**C:** I have a similar comment as before, the HTC+ field has this original purpose which seems jeopardized by this requirement.
	**C:** These headers and the payloads are carrying more and more information about what the device is and what it's doing, so it is a concern that we can not currently protect these fields. We should be looking at different ways of modernizing our spec with a view to protecting the security and privacy of clients that will be communicating using frames that have these fields, headers and payloads.
	**Chair:** I will mark requirement 32 as needing further discussion:
	**Chair:** Moving on to requirement 33.
	**C:** So I understand that we have some networks where it's not the AP as such that encrypts but some other, remote entity. If we then encrypt the Retry bit we would force a re-encryption of the transmissions if it needs to be retried. This could potentially introduce a lot of overhead, so I just want to caution about that.
	**C:** We use the Retry bit to inform about decryption so I think this will necessitate an entire redesign of the receiver path. That's a fairly large change. In the previous requirements I saw many more pieces of information that should be encrypted, but for this Retry bit I'm wondering if it's not extremely complicated to solve while the fingerprinting capability of exposing the Retry bit is not, to my mind, sufficiently demonstrated.
	**Chair:** So far only people who are against requirement 33 have spoken. Should it be dropped from our list of requirements or should we mark it as needing further discussion?
	**C:** What is the current requirement for sequence numbers within the context of this discussion?
	**C:** We've said they should be changed rather than encrypted.
	**C:** I agree with the previous concern that the single bit is not a very strong fingerprinting capability. But the Retry bit has an affinity with sequence numbers. So if the sequence number is going to be a block somewhere, protected somewhere, then having the Retry bit in the same block would address the receiver implementation issues. They need both SN and Retry bit.
	**Chair:** I will mark requirement 33 as needing further discussion.
	4. **Requirements relating to BPE**

	**Chair:** We have agreement to leave BPE requirements until a later time.
	5. **Requirements relating to issue 8**

	**Chair:** Currently we have no requirements that directly correspond to issue 8.
	**C:** Some requirements would target PHY/RF related privacy issues and some of the requirements currently under discussion (management frame encryption, sensor and measurement protection, etc) I believe already approach this. But it can be left for a later meeting.
	6. **Requirements relating to issue 2 (cont. from p. 13.2 above)**

	**Chair:** Yesterday we agreed to do a strawpoll on requirement 28 today. This could be a good time to engage with this?
	**C:** We've had some offline discussions on this requirement so it's not clear that the strawpoll is needed anymore.
	**C:** It's true that we've agreed to have further offline discussions. I'd requested this strawpoll yesterday, but I think I will drop this for now.
	**Chair:** I will mark requirement 28 as no action for now, with a view to getting a submission later.
7. **Motion requirements marked as "ready for motion" by discussions under p. 20.

 Motion #14:** Approve requirements 13 and 30 marked as "To be motioned - agreed by unanimous consent" in 22/606r3. The requirements were agreed upon 13 May 2022. **Discussion:
 C:** Document 22/606r3 needs to be uploaded to mentor for the motion to be valid.  **Chair:** I will upload this version of the chair slides deck, 22-606r3, to mentor. I will also remind everyone that this is a motion, and only voting members can vote. The results will be verified later.Moved: Stephen McCann (Huawei)
 Seconded: Stuart Kerry (OK-Brit, Self)

 **Results:**
 Yes: 17
 No: 1
 Abstain: 9
 N/A: 32
 Invalid: 0
 (59 people on the call)

 Motion passes.
8. AoB.
	1. No AoB.
	2. Reminder that participants are welcome to present submissions.
	3. Reminder that BPE requirements will be processed in future sessions.
9. Chair adjourned the meeting at 13:04 ET.