IEEE P802.11
Wireless LANs

|  |
| --- |
|  TGbi Minutes Electronic **Interim Session 17-25 Jan** 2022 |
| Date: 2022-01-21 |
| 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 17-25 January 2022.

Note: Highlighted text are action items.

Q – proceeds a question

A - proceeds an answer

C - proceeds a comment

Yellow highlight - action point

r1: correction in strawpoll results under 11.3.1

**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 19 January 2022, 11:15 ET.**

Chair calls meeting to order at 11:17 ET.

Agenda slide deck: 11-22-1974r1:

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. Kurt Lumbatis offers to present during the Thursday slot rather than the Friday slot to free up time for procedural discussions on the roadmap ahead. Tentatively accepted.
	2. Clarification that roadmap discussions will run for about 1-1,5 hours on Friday.
	3. Unanimous approval of the agenda as revised in 1974r2.
5. **Administration**
	1. **Motion #7:** Approve previous minutes

Approve the minutes for:

2021 November 802.11 Electronic Plenary: 11-21/1915r0,

TGbi Teleconference: 11-21/2030r0

Moved: Kurt Lumbatis

Seconded: Stephen McCann

Approved by unanimous consent (55 participants).

* 1. **Approving the issue-tracking and use-case document by motion** (11-21/641r6)

		1. **Use-case #8** could use further modification. In the first bullet point in the second Issue list, we should add CSI as an example.
		2. Today CSI is not signalled directly, we have compressed beamforming support, so when we add this to our list of use-cases what do we mean? Are we talking about what is in the first bullet (CSI feedback), or about the CSI that is obtained by the device itself? In my opinion they should be made separate since CSI obtained by the device is not standardised.
		3. The first CSI is about a device measuring the CSI and sending it in a frame and we want to protect those frames. The second CSI is about measuring the channel state directly. In the first list it's about the CSI as a payload to some frame, and in the second list it's the measurement as such that could leak - the mechanisms used to perform those mechanisms and characteristics extracted from frames that are being transmitted.
		4. That is also my understanding.
		5. We could change CSI to channel state measurement in the second list.
		6. There is no basis in **use-case #6** for dealing with the situation that a STA becomes an AP. In our standard an AP is either an AP or not, and for STA too. I would prefer if this feature was not defined in the standard in such a backdoor manner. If it's a STA the privacy requirements should apply as to STAs, and if it's an AP then those privacy requirements should apply.
		7. Because soft or mobile AP are expected to be more common in future I disagree that we can avoid this issue.
		8. I very much agree that this use-case is valid. Maybe we can avoid the words soft/mobile AP, and call it only "AP privacy". But there is definitely an issue of privacy in AP here.
		9. what would be different from a privacy perspective for a mobile AP than a fixed AP?
		10. Not necessarily anything. I also agree that the use-case is valid. I also remind that the PAR does not permit us to introduce new features into the base-line, so it's not clear that we could change the base-line standard to permit this entirely new concept of a soft or mobile AP. Generally we could have AP privacy and this would allow us to work on this.
		11. If we remove the soft/mobile language we're broadening the scope a lot which is an issue to me. I think we should keep what we had before.
		12. I'm now worried that we started by trying to make a motion on this document, but with the revisions to this document we'll have to upload a new version to mentor until we could move ahead with the motion. In the interest of saving enough time for our presentations, maybe we could defer other discussions to offline?
		13. Chair: The current discussion should be wrapped up within 10 minutes.
		14. Soft, hard, etc. are bad terms to describe AP. Mobile AP in the way it's used for this use-case I think it is quite clear that we are specifically targetting the situation where the AP is moving along with a user. I assume this use-case to cover relatively small BSS, maybe a family group that is using shared connectivity from a device, and not for instance large BSS covering hundreds of enterprise users.
		15. A mobile AP is anyway being exposed to the DS so it's always somehow exposed. We are boiling the ocean and we need to be realistic about boundaries here.
		16. Chair: Let's close the discussion here and amend the agenda to postpone this motion. We will do further offline discussions on use-case 6.
		17. Jarkko Knecht volunteers to coordinate offline discussions.
		18. Chair: We will come back to this on Friday and if it is not resolved by then we'll have to revisit the matter later.
	2. **Teleconferences**
		1. Chair: We'll postpone discussions on teleconferences until later in the week.
1. Technical Presentations
	1. **Initial Privacy Enhancements Requirements (11-22/0107r0),** Phil Hawkes (Qualcomm)
	2. Document slightly revised during presentations (editorial changes). See 0107r1 on mentor.

Discussion:

**C:** You defined the PE. I find the title of the project, EDP, maybe we don't need to use that but it may be better for us to just call the project bi.

**Q:** My question is on slide 4. The assumption on the BSS here is that only in a BSS where all the devices are PE capable there will be PE. I don't think this will be possible, if we consider legacy support and other things. This may be too strict and restrict deployment options. So how are you thinking about that?

**A:** My assumption here is that if an AP is PE capable it would have a PE BSS and a non-PE BSS, so you could have two BSS from the same AP in that case. And we need this for a couple of reasons: if we have an AP that is transitioning between over-the-air MAC addresses, all the devices connected to it will have issues and drop their connection and the UX will be poor. But we could reflect on this changing MAC for AP to be something that is only the case when an AP moves around with the user.
The other case is when we want source and destination addresses not to be sent in the clear. If we have some legacy devices and some new devices, the new devices will be able to hide these data but legacy devices not. These features are not just useful to protect the STA or the AP, but also other STA or devices in the network - more generally the network itself. But we can only guarantee this protection if the entire BSS is PE (or bi) devices.
So that's where we're coming from with these proposals. We're open to having a more detailed discussion on this topic, more presentations, etc. But it's how we're thinking.

**C:** I would want to be more careful on this assumption since it seems like a doubling of BSS and this may severely impede deployment, but yeah some more thought.

**Q:** On slide 8, are you now saying that you want to have a standardised version through the scan iteration requirement of how often a MAC address is changed over-the-air?

**A:** Yes, this is correct. It would standardise the frequency of over-the-air MAC address changes. We could put "may" instead of "shall" if we want it to be configurable.

**Q:** On slide 10 I just want to clarify if the PE AP changing its over-the-air MAC address is actually a specific case where you have a small BSS that moves around with a single user or maybe family, because you already brought up it's very disruptive if the AP changes its MAC address with legacy devices?

**A:** Yes, that's correct.

**Q:** On slide 4, I'd like to return to the assumption of having all devices supporting these features with no legacy devices. Do we need to be this strict?

**A:** Yeah, some features will not be easily accessible otherwise.

**Q:** On slide 5 if I'm reading it correctly, if you already have a requirement that there should be seamless over-the-air MAC address transition do you need to have a shall-requirement for retransmitted frames with respect to over-the-air MAC used for that retransmission? It seems to me that would be in the lower layers, perhaps in PHY protocols.

**A:** We may need to look closer at this, yeah. It's a good point.

**Q:** Regarding the general mention of MLDs and MLOs, it doesn't seem to be too controversial here. But since 11be is not yet an approved amendment, is it not better for us to look at 11bi as an amendment made towards a baseline standard where 11be does not yet exist? It's not a technical comment but procedurally we can adapt our amendment to the 11be features at a later time.

**C:** I think having 11be APs and BSSs covered by our amendment is a good way of achieving good privacy for APs and STAs.

**C:** We're expecting 11be to be rolled in to the standard first so it would then be within scope for 11bi to make modifications to 11be.

**Q:** If you can go to slide 8, you talk about the sequence of authentication. Is each authentication frame here implied to have a different MAC address over-the-air or that you would use the same over-the-air MAC address for the entire sequence?

**A:** One and the same for the entire sequence.

**C:** But why could the PE STA not choose this itself? It could be a may, rather than a shall, no?

**A:** It's a good point. I can't immediately assess the drawbacks here but I take your point.

**Q:** On slide 9, I don't understand why it's a may-requirement that PE AP initiates the post-association OTA MAC changes?

**A:** Basically it's the mobile AP case again.

**Q:** On slide 10, with the PE AP changing the OTA MAC and being in charge of a rotation we have the entire same complexity problem as with key exchanges. It seems to me like we may be able to find some simpler approach?

**A:** Point taken. We could look at this of course.

**Q:** I have a question on both slide 8 and 12, a similar question: if the STA keeps their MAC addresses but the AP changes its MAC addresses you could still track that vehicle, so don't we need to find some other mechanism for privacy enhancement here? Like we would have to make sure rotations are done at the same time, probably, so that you can't do asynchronous monitoring?

C: The APs and STAs could coordinate their changes somehow.

Q: But would this really protect privay? Coordination could also leak data.

1. **Recess 11:16 ET.**

**2nd slot. Thursday 20 January 2022 11:15 ET.**

1. **Meeting called to order at 11:19 ET.**
2. **Reminder of policies and procedures (see para 1-3 above under 1st slot).**
	1. No response to call for essential patents.
	2. Copyright policy was presented.
	3. Reminder to do attendance issued, together with reminder to register for meeting.
3. **Agenda review (11-22-1974r3, slide #17)**
	1. A submission number updated.
	2. Agenda approved by unanimous consent.
4. **Technical presentations**
	1. **Requirements for usecase 1 and 2 (11-22-93r0), Antonio de la Oliva and Joseph Levy (InterDigital)**

Discussion:

**Q:** The privacy setting that you mention in requirement 3, but privacy configuration in requirement 1, is there a difference between these two concepts for what we are developing? Or is the configuration a capability indication, when we communicate the features we are developing?

**A:** We didn't really intend for there to be a strong difference between the concepts. They could be interpreted as interchangeable.

**Q:** But then it might cause confusion, right? Configuration would seem to me that it's an agreement in our group what we will be using here during the association. Setting might be more up to the user?

**A:** Yeah, we can clarify a bit more on this. We were trying to keep this more general at this stage.

**C:** For me it seems like we have some features and a setting chooses you have these features, you have those features, we have these. But we don't need to do the word-smithing at this point.

**Q:** If we look at features we have today for protected frames, MAC headers and other encryption that we use to protect things, I'm wondering how the protection in requirement 5 relates to the protection mechanisms we already have. Is this a new header? Or you want to have protection of the parameters at large?

**A:** To be honest, this is not something we have looked at until now.

**C:** If you want to encrypt the whole MAC header that's a significant change and investment. It would require a completely new encryption mechanism, but we could specify more easily if we have additional fields that we want to have protected by some of the existing mechanisms that we've already defined.
**Q:** Have you considered how to include MLO in these requirements? Would it require additional requirements on top of these ones?
**A:** This is something we also need to discuss based on what was already talked about yesterday.
**Q:** Why are these privacy features being negotiated and agreed upon? If we have privacy features why would you just not take advantage of them?
**A:** It depends on the privacy feature. If you need a feature that requires some data disclosure you need to negotiate on which data to be shared and how. Some mechanisms you can use without there being prior agreements in the BSS but if you need, you need to agree on the terms.
**C:** In my view we should consider the MLO issue, but my understanding of MLO point-to-point association is that they are the same as AP to non-AP STA association, so that doesn't actually impact the privacy features. There's some issues internally to MLOs and component STA but they will have be developed separately. These requirements cover the MLO-to-MLO associations already.
**Q:** There are lots of terms here: privacy feature, privacy setting, privacy configuration, etc. I'm finding it a bit hard to parse all this terminology. On requirement 4 it also says that AP can request STA to change privacy settings, so does that mean that AP can force the STA not to do some privacy things? Or that the AP can reject an association if the STA does not do privacy?
**A:** On your second set of questions, we're exactly aiming at that situation to disassociate if AP and STA are not in agreement on the privacy re-arrangement, especially that AP tries to impose stronger privacy.
**Q:** Why would there have to be a reassociation?
**A:** So far our discussions have mostly been oriented towards privacy contracts negotiated during association so this is a fall-out from that. It's during association, as far as we understood that we'll have these agreements set up.
**C:** I believe this could be solved without re-association but we should look at this of course.
**Q:** If I understand the first four requirements concern association and the requirements on privacy that would apply for the rest of the association. If the STA does not like what is negotiated there it would reassociate with some other terms, is that correct?
**A:** Yes.
**Q:** But like the previous commenter, maybe we don't have to start from scratch with the security association if there is no agreement on the privacy association as in requirement 4?
**Q:** But would that actually be universally applicable for all privacy features?
**A:** Would have to think about this.
**Q:** Something that is not addressed with these requirements, APs which are hiding themselves and where the SSIDs are hidden, have you considered those?
**A:** We are looking at the privacy of STA rather than the privacy of the AP, so I don't understand?
**C:** These requirements assume that all the APs are discoverable.
**A:** I don't think any of these requirements relate to discoverable APs or non-discoverable APs. I'll put in a note to look closer at this though, because I see the point.

* 1. **Enhanced randomized and changing MAC addresses (11-22-114r0), Stephane Baron (Canon)**Discussion:

	**Q:** I understand there are two parts here, AP change addresses and STA change addresses, and I think they may have to be addressed separately. For legacy devices you have larger problems for APs which change addresses because of dropping associations.
	**A:** Sorry, this could have been more clear but my intention here was saying the AP and the STA jointly compute a new non-AP STA MAC address - so the AP MAC is not impacted at all.
	**Q:** With the beacon proposal, is the idea here that everybody will change their IP address or what is the implication here?
	**A:** Both make sense.
	**Q:** I have a couple of comments. First on slide 5 related to the new key. Personally I would use the design we already have in the current baseline, so that when we construct PTK we can do it following the current mechanisms.
	**A:** I agree that we could use the current mechanisms for deriving keys. We can discuss which key we need to generate the new MAC addresses of course.
	**C:** I mean, I'm just saying that we have an exchange mechanism already but the key can be the same of course. So that's what I mean.
	**Q:** On slide 7 you have a very specific time counter for MAC address changing, is this really intended? What happens if there is another exchange going on at the same time?
	**A:** The original proposal was that we use beacon frames to signal the MAC address change and enable both agents to cooperate on the rotation.
	**Q:** But so then it would be sort of assumed that the non-AP STA would not be initiating before the time of the rotating be initiating a durable exchange that could be disturbed by a MAC rotation?
	**A:** Yes that was the intention.
	**Q:** On MAC headers we also have TID numbers and other sequence numbers that can be used to track devices, and this proposal seems not to address these other identifiers and counters that remain after the MAC is changed? Especially if all listening devices can now also eavesdrop this beacon frame exchange announcing a MAC change, it would seem trivial to track a device anyway - perhaps more demanding, but still possible. I was thinking maybe we could change addresses to unicast and broadcast, and that unicast would be changing with coordination and with broadcast not?
	**A:** I focussed here on the MAC address because it's a known problem and given a lot of attention, and the other information elements we probably need to look at - we'll have a longer and more complicated discussion, I think?
	**C:** It's good that we agree that all these fields should be protected somehow.
	**A:** Now the second part here is that the timing does not need to be synchronous. But then the PHY needs to remember two MAC at the same time, which seems impractical to me, but we can discuss different scenarios of course and see what sort of flexibility we need.
	**C:** I'm wondering if this period of MAC address pairs would create problems for scheduling, we should be looking at that.
	**C:** For group address changes, using beacons to announce I can see the rationale here but for the unicast case I'm still hesitant.
	**Q:** On slide 8, the ERCM change counter is not broadcast, correct? It's just maintained internally? Does it need to be broadcast?
	**A:** Well, the benefit of broadcasting it is that the STA knows even if it misses a beacon or frame what is the counter.
	**C:** As far as I know, the STA keeps track of the TBTT anyway so it will know when the next frame is due to arrive.
	**A:** It is more practical if you have the broadcast ERCM though, a STA which wakes up for instance.
	**Q:** What is the value of doing this though? You already have a security association in this model, as far as I understand, so you could just communicate directly within that association between the AP and the non-AP STA right?
	**A:** The less information we transmit the more security we can guarantee, so the purpose here is to minimize the amount of information that has to be exchanged within the security association. We're trying to minimize in time and scope the information that is exchanged.
	**Q:** In the distribution system what is the address that you use? Like destination address and recipient address?
	**A:** I mean here I only considered the RA. The DA was not considered. I think they're not the same issue. RA is usually wired somewhere on the internet, but we're still not settled on whether DA should be changed or it's enough just to hide it, as far as I understand. My personal opinion is that maybe DA could be hidden rather than changed but I understand it's an open question.
	**Q:** When the counter counts down, does every STA have the same counter or it's different per STA?
	**A:** It could be but it doesn't need to be. For me it's sort of preferable if all the STA change, yeah.
	**C:** That puts a lot of pressure on the AP as far as I understand.
	**A:** The point is that the AP has a lot of time to compute the new addresses. There are cases when this could be practical, but it's possible to do it only for subsets of associated non-AP STA or even individual non-AP STA.
	2. **Association MAC Address Based On AID (A-AMAC) (11-22-1854r3), Kurt Lumbatis (Arris/Commscope)**Discussion:

	**Q:** I'm trying to understand the AID in this case. Is there a real good justification for trying to change it? I mean, I'm not super up to speed with all the places where it's used today but I'm just trying to figure out if it has impact on multi-SSID set-up or similar features. Maybe we could be using a different index to provide the same feature?
	**A:** The purpose here is to divorce the station's MAC with identifiable information of the station. The AID is a simple mechanism for this, it's used internally by the AP to keep information about the STA, and yes, it's also there in power-save but the fact that it's internal to the AP is the reason that it's mentioned here.
	**C:** I'm really against AID being repurposed for this for reasons previously stated.
	**Q:** I'm trying to understand the difference between this presentation and the previous presentation. It's all about changing the MAC addresses and the processes that accomplish that. But the high-level difference between this and what we heard before is that you depend on AID.
	**A:** Yes, I'm trying to use existing mechanisms and identifiers, and the previous presentation was rather relying on cryptographic methods.
	**Q:** So I think there may be more fundamental questions here like what space we're randomizing over here.
	**A:** Okay, thank you for your input.
	**Q:** The previous two questions included my concerns to a large part. If we want to randomize MAC addresses, we need a way to calculate it that can be used, but using this AID would then announce what is happening. We'd need some way to do more obfuscation.
	**Q:** So the AID has been used for more things following its introduction, like in 11ax it's also used for trigger frames and other things. Assigning AIDs at random would then... Having a very fragmented range of AID assigned to station would render trigger frames completely useless. This problem would be exacerbated in the case of multi-BSSID. Did you consider this?
	**A:** That is true and I considered it. This is of course one solution, but we could look at hashing also, if the AID as a base-line is sufficient but then not directly using it later. My original goal was to not add overhead or over-complicate matters, but there are some additional steps and information that could be inserted to protect these use-cases and it wouldn't matter much.
		1. Strawpoll #1: Is there interest within the 802.11bi TG to pursue the idea of defining and specifying the use of post Association over the air MAC address (A1, A2) utilizing the AID?
		Yes: 5
		No: 25
		Need more info: 11
		Abstain: 4
		No answer: 34
1. **Recess at 13:02 ET.**

**3rd slot. Friday 21 January 2022 11:15 ET**

1. **Call to order 11:19 ET**
2. Reminder of policies and procedures (see also point 2-3, 9 above).
3. **Review of agenda (11-21/1974r5 slide #17)**
	1. Agenda approved by unanimous consent.
4. **Administrative**
	1. Teleconferences through-out February and March.
		1. Avoiding meeting collisions with TGbe and TGme is a continued priority.
		2. Weekly, one-hour calls on Thursdays at 9AM ET unless the 10AM ET slot is freed up by TGbe.
5. **Technical presentations**
	1. **Proposed 11bi requirements (11-22-109r1) Po-Kai Huang (Intel)**

Discussion:

**Q:** You're saying you want to use existing encryption mechanisms like UCMP, but where do you find the generation material for these keys?
**A:** We believe there are ways that to find material for PMKID. High-level the PMK can be used
**Q:** SAE uses public-key crypto though.
**A:** Did you look at the 859 presentation from last year?
**Q:** Yes.
**A:** So previously I think there was discussion on encrypting only part of the frame, and we propose to extend it.
**Q:** On slide 4 you say that existing symmetric encryption is sufficient to encrypt the frame body field without significant changes to the hardware and that this is demonstrated.
**A:** I thought this was something you had also said before but we can work together on changing this.
**Q:** This idea of avoiding authentication frames, and doing something like WPA3 enterprise, would lead to two association frames to protect this exchange and then another association frame after that to add the real protection as in .1X?
**A:** Yeah, so in .1X they need something like this for EAPOL. What I'm saying here is that we can do something like that, using the PMK and the PMKID to derive keys and set up encryption for the frame body field in an optimised way. But we're certainly open to further discussion here on how to keep it simple. But I understand basically your comment is that there are multiple authentication schemes and we can ask which one is more appropriate.
**Q:** I have some questions on the scanning part. Let's say we came up with 6GHz scanning rules and those mechanisms require SSID or unicast probe requests, are you addressing that kind of issue at all?
**A:** It's a good point and SSID is specific. It's a bit complicated because you have a lot of legacy interoperation issues. One way would be to fall back to .11aq whenever we have legacy issues with SSID, but personally I think we may even need specific design requirements for this.
**Q:** In .11be we have probe requests for associated devices as well, so do you have any thoughts on extending your proposed mechanisms to that sort of situation as well? Like encrypted action frames?
**A:** It's under discussion as far as I know, but in my opinion it would be good with a post-association action frame and it's easily protected, but I understood that they already are looking at that anyway so it may not be something we need to care about in the end.
**C:** It would be for broadcast data and queries and I agree we need very efficient mechanisms for this.
**Q:** Could you explain more about how the STA deal with the different address fields? Would we need a third address field and what to do with it?
**A:** I think for now it is better if we try to focus on the simpler case where we don't have this soft or mobile AP, for instance. Then we have just two address field in a data frame. The complication of selectively revealing SA or DA is legacy devices, but we will be discussing I'm sure how to minimize the revelation of these addresses. For the legacy devices I don't think there's anything we can do.
**C:** I could add that these suggested requirements are focussed on protecting a client device from revealing itself, not about the client device being revealed. Providing that sort of option.
**Q:** When you talk about STA MAC that means a non-AP STA, correct?
**A:** Yes, that is correct.
**Q:** You also talk about encrypting the frame body at re-association, but do you intend for this to cover also the case of post-association where re-association does not come into play?
**A:** Yes, I guess we see that these suggestions on slide 5 are a pre-requirement for doing that sort of post-association MAC randomization as well. But there are a number of things that we should also be looking at protecting, these information elements - counter numbers, sequences, AID and other elements. And it's fine if we look at this MAC address issue first, and it will also help us when we move on to other things as well.
**Q:** So is it fair to say that this presentation focuses on pre-association and during association, but less on the post-association phase?
A: We try to cover also the issue of roaming between ESS, and mention here the BSS transition, so I would not understand our proposals to be that limited.
**Q:** On slide 4, do you intend for there to be any authentication to apply the frame body field encryption?
**A:** I don't intend to change with this presentation any of the existing authentication mechanisms so you're right there that we're re-using the same authentication mechanisms that are already in the standard.
**Q:** I mean, it seems you could create then a key before association but that temporal key would not be authenticated. It would just be a key.
**A:** There are a number of authentication options so we have some of those already applied, they use PMK or they don't, and we can discuss which specific mechanisms we find more suitable for this purpose as I mentioned before.
**C:** The "authentication" in the state machine can be open, e.g. when 802.1x is used. The key is generated AFTER association so there's nothing to protect the association request.
**Q:** Could you again clarify this encryption? I'm now confused.
**A:** Well, once you have PMK and that's authenticated you can use it to derive other things, that's what I mean. But we can discuss alternative methods for encrypted the frame body field. My main point is that we probably need to get that done to protect against this fingerprinting situation that has been raised before.
**Q:** So you're assuming there's a PMK here which has been generated during an authenticated association? Would that mean that the .11bi relies on an association to have already occured before you do the actual association that implements .11bi protections or what is it that is happening?
**A:** You need a dataframe to carry for instance EAPOL already so we have a range of various authentication mechanisms that we could be looking at - there are so many of them and we can check which ones give us the type of key management that are appropriate for these requirements but generally I believe we can find the authentication mechanism that allows us to do this encryption.
**C (chat):** But the PTK is already generated in another 4-way-handshake?
**C (chat):** So is the proposal here to move 802.1X into a "private limited connection" phase before the open authentication?
**Q (chat):** With the 802.1X controlled port, isn't there already a "private limited connection"?
**A (chat):** Yes, but .11 provides the .1X link-up after association already succeeds. That's the trigger of the .1X exchange. So I'm confused.
C: I guess the question here is how the protection functionally happens on the association after the first connection?
**A:** Indeed the idea of this proposal was to provide effective change while making fewer changes or new mechanisms.
**Q:** Could you go back to slide 9? The basic scheme is taking a MAC, sending a typical frame of association to get going, you get the PMK, then the next time around when you use a different MAC you re-use the PMK and PMKID to send encrypted stuff in the header? However, when you send that first association request you get your keys, is that using the traditional association request? Aren't you then sending your fingerprintable information in the clear anyway?
**A:** No, let me clarify. I specifically clarified the two situations: if you use SSID you go through that step, but through 1X you don't really need to convey all those capabilities. That's how we're thinking here. For SAE maybe we don't need that but for 1X we for sure do, yes.
**Q:** Then the first sequence I'm sending to the AP to get my keys, and to the authenticators, then I reveal all the elements?
**A:** No you don't have to do that.
**Q:** But those elements are not being used to determine if I'm able to associate? It's more of a blind situation where I say "Hello give me a key?" and then if the network hands out the key, then we can start seeing if I should be associating and what are my capabilities, and so forth?
**A:** We can be discussing this of course. The focus here is to not revealing information in the clear. Obviously not all the elements in a request frame transmitted today are necessary to set up an association, right?
**Q:** Yeah, but the AP may need to know the capabilities to know if it wants to associate?
**Q:** Looking at these requirements they seem to be avoiding some of the bigger questions. At least for me the bigger question with the work we're doing is exactly how the authentication happens. Here we're assuming that authentication can be left entirely intact but this isn't necessarily the case? I'm not happy about using the private limited connection as it's use here - we could make a cleaner design and it should have been done 20 years ago but wasn't. But I think to solve this now we'd have to move away from the .1X design and putting EAPOL and data frames. I would welcome the discussion on whether we should separate authentication and association even more clearly so we don't need to have this discussion on which information elements need to go in which authentication or data or management frames, since they would be in authentication frames period. Currently I can't commit to these requirements as presented.
**A:** Well what we're coming from is that this frame is there and it will be there, and that's where we're coming from and now people ask where do the keys come from. We're suggesting to use what's there today, but we're not trying to specify all the key-deriving mechanisms here. So I don't entirely see where you are going here?
**C:** I agree that, assuming that we get an authentication mechanism that works, I'm very happy with these requirements just to be clear.
**Q:** But then you're not against looking further at some mechanism here that doesn't use EAPOL?
**A:** That is correct.
**C (chat):** Agreement that EAPOL in data frames was a horrible decision!!
**Chair:** Unless I'm mistaken it would be safe for me to close the queue.
**A:** We will work offline to find routes forward based on the feedback.

1. Review the Proposed Issues Document (11-22-641r6)
	1. No objection in principle to the idea that mobile AP could cause privacy issues.
	2. Mobile AP already being looked at by other groups.
	3. Motioning of document postponed.
2. Reviewing TGbh text.
	1. There is no settled TGbh text as of yet, but should we organise a joint teleconference once they have text proposals?
	Discussion:
	**C:** I would suggest TGbi focuses on 11bi. If TGbh makes a decision but feels they have to come to TGbi for a view that will slow things now. The review mechanisms are already there and anyone is able to join there and provide feedback, also through the group comment systems and their open meetings.
	**C:** Other agreement.
3. AoB.
	1. No AoB.
4. Chair adjourned the meeting at 12:46 ET.